Arquiteturas de Federação e o OpenID Federation: Adesão de Provedores e Soberania de Dados

Eduardo Dani Perottoni[1], **Brendon Vicente Rocha Silva**[1], **Frederico Schardong**[1], **Ricardo F. Custódio**[1]

[1]Laboratório de Segurança em Computação (LabSEC)
Universidade Federal de Santa Catarina (UFSC)

Resumo. *Federações de identidade acadêmicas estão iniciando a migração do Security Assertion Markup Language (SAML) para o OpenID Federation. A adoção desse novo protocolo, no entanto, introduz complexidades. Para reduzir o atrito nesse processo, o presente trabalho propõe uma arquitetura de federação que se aproxima do modelo hub-and-spoke, na qual componentes são hospedados pelo seu operador, o que facilita a adesão de provedores em comparação à full-mesh. Discute-se o trade-off entre facilidade de adoção e soberania de dados, abordando os riscos da centralização e como mitigá-los.*

1. Introdução

Uma Federação de Identidade Digital (FID) permite que usuários de uma instituição acessem serviços de outras usando suas credenciais de origem. Esse modelo é difundido no meio acadêmico. As FIDs acadêmicas, incluindo a Comunidade Acadêmica Federada (CAFe), são construídas sobre o protocolo *Security Assertion Markup Language* (SAML).

O sucessor do SAML é o *OpenID Federation* (OIDFed) [Hedberg et al. 2026], que substitui o gerenciamento centralizado de metadados por um modelo de confiança hierárquico, dinâmico e criptograficamente verificável. A adoção do OIDFed está em curso em diversos projetos: no piloto da eduGAIN [van Dijk and Vaghetti 2024], em produção no governo italiano SPID/CIE [Agenzia per l'Italia Digitale (AgID) 2024] e, no Brasil, na CAFe 2.0, reconcepção da CAFe sobre o OIDFed[1]. Assim como no SAML, integrar entidades em uma federação OIDFed exige recursos e capacitação técnica que muitas instituições brasileiras não dispõem [Aldosary and Alqahtani 2021].

Embora SAML e OIDFed não imponham uma arquitetura centralizada, concentrar componentes operacionais sob o operador reduz a complexidade de integrar novas entidades, ao custo de lhe transferir fluxos de autenticação, atributos dos usuários e custódia de chaves de federação. O presente trabalho discute esse *trade-off* entre facilidade de adoção para instituições com equipes de Tecnologia da Informação (TI) reduzidas e privacidade e soberania de dados, uma vez que o operador passa a ter acesso a atributos do usuário em uma arquitetura centralizada, na qual o próprio operador gerencia componentes participantes dos fluxos de autenticação.

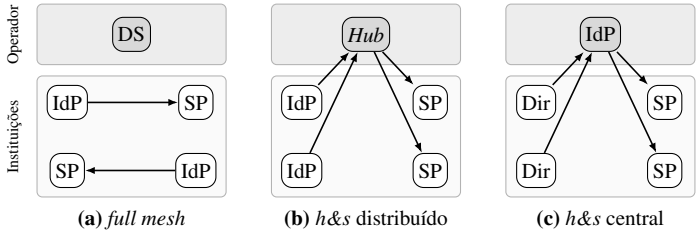
2. Arquiteturas de Federações de Identidade

A GÉANT classifica as arquiteturas de federação, mostradas na Figura 1, conforme a centralização de execução de seus componentes [GÉANT 2025]. Na ***full mesh*** (Figura 1a), arquitetura da eduGAIN e da CAFe, cada organização executa seus provedores e

[1]O presente trabalho foi realizado com o apoio da Rede Nacional de Ensino e Pesquisa (RNP), por meio do GT-BAITA, grupo de trabalho do Programa de Serviços Avançados.

o operador apenas distribui metadados assinados e mantém o serviço de descoberta (DS), que auxilia o usuário a localizar seu Provedor de Identidade (IdP). O fluxo de atributos, ilustrado pelas setas, ocorre diretamente entre IdP e Provedor de Serviço (SP).

Na ***hub-and-spoke* com login distribuído** (Figura 1b), o operador interpõe um *hub*, um *proxy* IdP-SP que atua como SP perante os IdPs e como IdP perante os SPs. Nesse caso, as credenciais permanecem na instituição, mas o *hub* processa as asserções e acessa os atributos das autenticações. No ***hub-and-spoke* com login central** (Figura 1c), um único IdP do operador autentica os usuários a partir das bases (*Dir*) que as organizações conectam a ele. Embora quatro em cada cinco federações adotem o *full mesh* [Hämmerle 2018], o *hub-and-spoke* aparece em federações nacionais como a SURFconext (Países Baixos) e a WAYF.dk (Dinamarca) [Hämmerle 2018, SURF 2024].



(a) *full mesh* **(b)** *h&s* distribuído **(c)** *h&s* central

Figura 1. Arquiteturas de federações [GÉANT 2025].

3. CAFe 2.0

A CAFe 2.0 apoia-se sobre o OIDFed, que permite a implementação de um modelo hierárquico de confiança, com múltiplos níveis [van Dijk and Vaghetti 2024]: uma *Trust Anchor* (TA) ancora a federação e cada instituição membra é uma entidade intermediária (IM), que pode ter como subordinadas outras IMs, IdPs ou SPs.

A CAFe 2.0 oferece um arranjo híbrido em dois aspectos: (i) representação das entidades OIDFed e (ii) fluxo de autenticação. Sobre (i), instituições com equipes de TI reduzidas podem delegar a custódia de suas entidades ao operador, enquanto as de corpo técnico maduro podem hospedá-las autonomamente. A Figura 2 ilustra a arquitetura com duas instituições (Inst): Inst A delega suas entidades ao operador e Inst B as executa autonomamente. Na Figura, as linhas contínuas representam o fluxo de atributos do usuário e as tracejadas, a emissão das declarações de subordinação (*Subordinate Statements*), que partem da entidade superior para a subordinada, constituindo a hierarquia de confiança.

Na CAFe 2.0, o WAYF (*Where Are You From*) conserva o nome herdado do DS da Figura 1(a), mas acumula duas funções. Além da descoberta, atua como *proxy* de identidade, assegurando a autenticação multifator (MFA) quando o IdP de origem não a oferece. Por isso aparece, nos fluxos a seguir, no caminho dos atributos.

Os provedores da Inst A implementam apenas o protocolo OpenID Connect (OIDC) e são representados por um *proxy* do operador, que assume por eles as funções do OIDFed (geração de artefatos, guarda de chaves e resolução de cadeias de confiança), assim como a TA Inst A, configurada pelo gestor de TI de forma facilitada, via interface *web*. Já a Inst B executa sua TA e seus provedores em infraestrutura própria e comunica-se ponta a ponta, salvo quando o WAYF é acionado. Um usuário da Inst B que acessa o SP OIDC da Inst A é autenticado por seu próprio IdP, e o fluxo de atributos é IdP OIDFed $\rightarrow$ *WAYF* (opcional) $\rightarrow$ *Proxy* $\rightarrow$ SP OIDC. No sentido inverso, quando um usuário da

Inst A acessa o SP OIDFed da Inst B, este resolve a cadeia de confiança do *proxy* até a TA CAFe e o fluxo é IdP OIDC → *Proxy* → *WAYF* (opcional) → SP OIDFed. Nota-se que, mesmo autônoma, a Inst B tem os atributos de seus usuários expostos ao operador sempre que a contraparte é delegada. A proposta aproxima-se do *hub-and-spoke* à medida que as instituições delegam a custódia das entidades ou usam os *proxies* mantidos pelo operador no fluxo de autenticação.

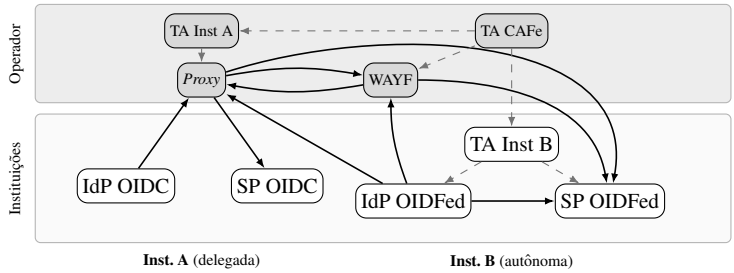


Figura 2. Arquitetura híbrida proposta para a CAFe 2.0

O uso do MFA é sinalizado antes do redirecionamento. O SP declara em `acr_values` o nível exigido e o WAYF, que conhece pelos metadados os níveis suportados por cada IdP, encaminha o usuário ao IdP de origem e, se a asserção recebida não o satisfaz, conduz ele próprio o fator adicional, cadastrado pelo usuário no primeiro uso. Os atributos não são coletados pelo WAYF. Como *proxy*, ele já está no caminho da asserção e apenas a repassa ao SP, retendo somente o identificador necessário para vincular o usuário a seus fatores. A base com os dados de identidade permanece na instituição.

A aplicação dessa política, contudo, não precisa ser centralizada. Ela pode ser distribuída logicamente, como um módulo de MFA acoplado ao *proxy* pelo qual cada IdP se integra à federação. A verificação do nível exigido ocorre junto à ponta, com os fatores registrados sob a instituição de origem. Nessa variante, a garantia de MFA deixa de justificar a posição de *proxy* do WAYF, que retoma seu papel tradicional de descoberta. Dada a distribuição lógica, o custo de manutenção continua fixo e não cresce com o número de IdPs.

4. O *Trade-off*: Facilidade *versus* Privacidade e Soberania

Na proposta, um provedor ingressa sem implementar o OIDFed ou manter *proxy* próprio, mitigando a "cauda longa" de instituições sem corpo técnico para integrar-se a uma federação *full-mesh* [Barton 2018]. A garantia de MFA pelo WAYF centralizado ou distribuído logicamente corrige em um único ponto o que exigiria atualizar centenas de IdPs.

Para comparação, a SURFconext (*hub-and-spoke*) conecta mais de 2000 SPs a 200 IdPs [SURF 2023] e a WAYF.dk, mais de 400 SPs a 75 IdPs [WAYF 2026], enquanto a CAFe, *full mesh*, tem atualmente 51 SPs para 335 IdPs. No *full mesh*, cada provedor precisa de uma equipe capaz de implantar e manter sua própria entidade, restringindo a federação às instituições com capacidade técnica para isso; os demais serviços permanecem com autenticação local, fora dela. No *hub-and-spoke*, o provedor mantém uma única conexão e as complexidades concentram-se no operador [SURF 2023].

Por outro lado, a centralização traz riscos. Quanto à privacidade, os *proxies* processam os atributos de cada autenticação e o operador sabe quem acessou o quê e quando, violando a *observabilidade* e a *vinculabilidade limitadas* [Hoerbe 2014]. Perante

a LGPD[2], o operador da federação torna-se agente de tratamento em escala federativa, com mais responsabilidade comparado ao *full-mesh*. Ademais, o fluxo de autenticação fica sujeito a um ponto único de falha.

5. Conclusão

A proposta de arquitetura da CAFe 2.0 combina um plano de confiança hierárquico e descentralizado, herdado do OIDFed, com um plano de autenticação que converge para o operador. O ganho aparece na adesão, pois as federações *hub-and-spoke* conectam SPs em ordem de grandeza superior à da CAFe e, na proposta, um provedor ingressa sem implementar o OIDFed nem manter *proxy* próprio. O custo recai sobre o operador, que passa a observar quem acessou o quê e quando, a responder como agente de tratamento em escala federativa e a concentrar o risco de indisponibilidade da federação.

O arranjo híbrido proposto não impõe uma arquitetura única a toda a federação. Cada instituição escolhe quanto delegar. Quem não tem equipe técnica para operar as entidades OIDFed ou possui IdP que não implementa o OIDFed, entrega ao operador a custódia de suas entidades e o fluxo de autenticação, e com isso passa a integrar a federação. Quem tem corpo técnico mantém ambos sob controle próprio. Assim, a adesão deixa de exigir capacidade técnica uniforme e a centralização torna-se escolha de cada participante, revista conforme sua capacidade evolui.

Referências

Agenzia per l'Italia Digitale (AgID) (2024). Spid - sistema pubblico di identità digitale.

Aldosary, M. and Alqahtani, N. (2021). A survey on federated identity management systems limitation and solutions. *International Journal of Network Security & Its Applications (IJNSA) Vol*, 13.

Barton, T. (2018). The future of federations – part two. REFEDS.

GÉANT (2025). Federation architectures. eduGAIN Wiki. Acesso em: 7 jul. 2026.

Hämmerle, L. (2018). The future of federations – part one. REFEDS.

Hedberg, R., Jones, M. B., Solberg, A. Å., Bradley, J., De Marco, G., and Dzhuvinov, V. (2026). OpenID Federation 1.0.

Hoerbe, R. (2014). A model for privacy-enhanced federated identity management. arXiv:1401.4726 [cs.CR].

SURF (2023). SURFconext: REFEDS and eduGAIN webinars on H&S federations. GÉANT. Acesso em: 15 jul. 2026.

SURF (2024). Federation architecture: hub-and-spoke vs. mesh. SURF User Knowledge Base. Acesso em: 7 jul. 2026.

van Dijk, N. and Vaghetti, D. (2024). edugain oid federation pilot.

WAYF (2026). About WAYF. WAYF — Where Are You From. Acesso em: 15 jul. 2026.

[2]Lei nº 13.709/2018.