Agregação de Metadados vs. Cadeia de Confiança: Comparando CAFe SAML e CAFe OpenID Federation

Eduardo Dani Perottoni[1], Brendon Vicente[1], Frederico Schardong[1]
Ricardo F. Custódio[1], Laerte F. Belotto[2], Reinaldo Matushima[2], Jean C. Faustino[2]

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

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

Resumo. *A Comunidade Acadêmica Federada (CAFe), operada pela Rede Nacional de Ensino e Pesquisa (RNP), é construída sobre o protocolo Security Assertion Markup Language (SAML). Este artigo compara a CAFe atual com a CAFe 2.0, uma reconcepção da federação sobre o protocolo OpenID Federation. A comparação é organizada em relação à topologia da federação, que evolui de uma estrutura em dois níveis para o formato multinível, e ao modelo de confiança, que migra de uma agregação estática de metadados para uma cadeia de confiança dinâmica e criptograficamente verificável.*

1. Introdução

A identidade eletrônica federada permite que usuários de uma instituição acessem serviços de outras utilizando suas credenciais de origem, sem a criação de novas contas. O cerne de uma Federação de Identidade Digital (FID) é o estabelecimento de confiança entre suas partes, o que possibilita a troca segura de informações sobre uma identidade [Kylau et al. 2009]. A Comunidade Acadêmica Federada (CAFe), gerenciada pela Rede Nacional de Ensino e Pesquisa (RNP) desde 2009, é a principal implementação desse modelo no Brasil, agregando atualmente 334 instituições de ensino e pesquisa.

Assim como a maioria das FIDs acadêmicas, a CAFe é construída sobre o protocolo *Security Assertion Markup Language* (SAML) [OASIS 2005]. Entretanto, discussões no grupo *Research and Education FEDerations* (REFEDS) apontam o SAML como um protocolo legado, sem funcionalidades para apoiar a evolução das FIDs acadêmicas [Flanagan 2024]. Embora consolidado, foi concebido em um contexto que não antecipava requisitos atuais de conectividade e alta disponibilidade [Vaghetti 2024].

Nesse ínterim, a *OpenID Foundation* desenvolveu o protocolo *OpenID Federation* (OIDFed) [Hedberg et al. 2026], que substitui o gerenciamento centralizado de entidades por um modelo de confiança hierárquico, dinâmico e criptograficamente verificável. O GT-BAITA[1] propõe a CAFe 2.0, uma reestruturação da federação com base no OIDFed. Este artigo compara a CAFe SAML e a CAFe 2.0: a Seção 2 trata da topologia da federação; a Seção 3 trata do modelo de confiança, contrastando a agregação estática de metadados do SAML com a cadeia de confiança dinâmica do OIDFed; e a Seção 4 conclui o artigo e discute a formação de federações aninhadas usando o OIDFed.

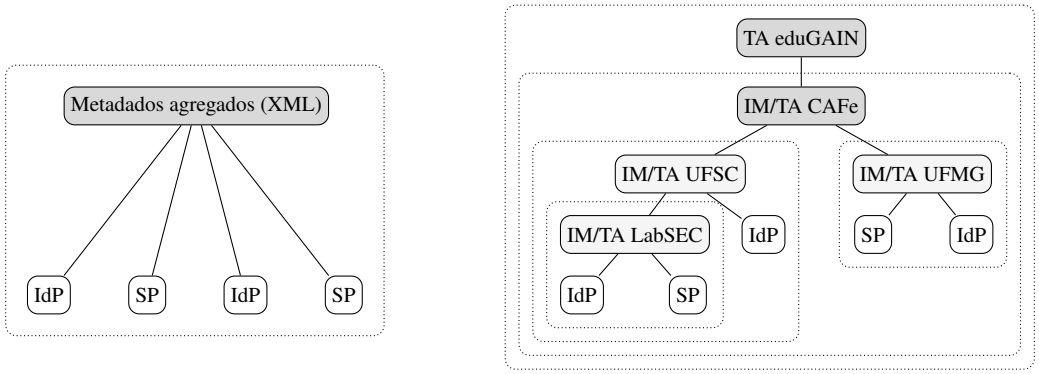
[1]O presente trabalho foi realizado com o apoio da Rede Nacional de Ensino e Pesquisa (RNP), por meio do GT-BAITA, grupo de trabalho do Programa de Serviços Avançados.

2. Topologia da Federação

O modelo de confiança centralizado da CAFe SAML resulta em uma topologia plana, ilustrada na Figura 1(a). Não há níveis intermediários de administração nem soberania das instituições sobre seus provedores. Todos baseiam sua confiança no mesmo arquivo central. A formação de subfederações com conjuntos de provedores de acesso restrito é possível por meio da publicação e checagem de metadados adicionais. Entretanto, essa implementação dificulta a integração de serviços, pois a delimitação de quem pode acessá-los depende de configurações manuais em cada provedor [Kantara Initiative 2019].

O OIDFed, por sua vez, organiza as entidades em uma topologia hierárquica em formato de árvore. O protocolo define papéis estruturais para as entidades. A *Trust Anchor* (TA) é a raiz da árvore e atua como âncora de confiança comum aos provedores abaixo dela; as *Intermediate Entities* (IMs) ocupam os níveis intermediários e opcionalmente organizam administrativamente a hierarquia, conforme as suborganizações da instituição federada; e as *Leaf Entities* (LEs) são as folhas da árvore, Provedores de Serviço (SP) e Provedores de Identidade (IdP), participantes dos fluxos de autenticação.

A *eduGAIN* adota em seu piloto de federação OIDFed[2] uma topologia na qual a própria *eduGAIN* atua como TA e as Redes Nacionais de Ensino e Pesquisa (NRENs) como entidades híbridas (TAs em relação à FID nacional ou IMs em relação à *eduGAIN*) [Vaghetti 2024]. Logo, a CAFe 2.0 propõe o seguinte mapeamento, ilustrado na Figura 1(b): a IM/TA CAFe, operada pela RNP, ancora a federação. Subordinada a ela, está a entidade híbrida da instituição (TAs em relação à FID do escopo da instituição ou IMs em relação à CAFe). Ainda, pode haver IMs (podendo ser TAs) representando laboratórios ou departamentos. Finalmente, as LEs concluem a topologia.



(a) CAFe SAML
confiança plana e agregada

(b) CAFe 2.0 (OIDFed)
cadeia de confiança hierárquica

Figura 1. Comparação entre topologias da CAFe SAML e da CAFe 2.0. Contornos pontilhados delimitam domínios de confiança: único na CAFe SAML; domínios aninhados na CAFe 2.0 em que cada TA/IM pode ancorar a sua subfederação.

Além de permitir a representação da estrutura administrativa das instituições, a topologia do OIDFed habilita a delegação de responsabilidades. Cada entidade não-folha registra e governa diretamente apenas suas subordinadas imediatas, de modo que cada instituição passa a ter soberania sobre os provedores de seu próprio escopo, sem depender do operador central da FID, reduzindo a carga operacional de manutenção da federação.

[2] `https://github.com/GEANT/edugain-oidf-pilot`

3. Modelo de Confiança

Na CAFe SAML, a troca de mensagens entre entidades depende de relação de confiança previamente estabelecida [Ferdous and Poet 2013], construída pela troca de metadados. Esse modelo implica a agregação dos metadados em uma lista de provedores que concordam em seguir regras pré-estabelecidas. A governança adotada nesse modelo exige que cada operador de uma NREN controle os provedores participantes e adicione seus metadados em um único e extenso arquivo XML[3], distribuído a todos os membros. Uma entidade é considerada parte da federação se constar nesse XML. O operador aceita o conjunto completo de metadados de uma entidade, sem uma forma granular e verificável de impor requisitos de segurança. Trata-se, portanto, de um modelo estático no qual a inclusão de um provedor exige um processo manual de aprovação do operador da FID [Jones 2020].

O OIDFed estabelece a confiança entre duas entidades por meio da confiança de ambas em uma terceira parte, a TA. O componente básico do protocolo é o *Entity Statement* (ES), um *JSON Web Token* (JWT) com metadados sobre uma entidade. Toda entidade publica um ES autoassinado sobre si mesma, a *Entity Configuration* (EC). Entidades superiores publicam um ES para cada subordinada imediata, o *Subordinate Statement* (SS), que atesta a confiança na chave da subordinada. A confiança passa a ser dinâmica pela resolução de uma *Trust Chain* (TC), sequência de ECs e SSs, que conecta uma entidade a uma TA. Esse protocolo facilita a operação da federação, visto que o operador registra apenas as entidades diretamente subordinadas à TA da federação, e não cada IdP e SP subordinado a instituições [Jones and Bradley 2024]. Entretanto, ainda não há um modelo de governança para o OIDFed definido pela eduGAIN.

O OIDFed oferece mecanismos, ausentes no SAML, para controle granular de confiança. As *Metadata Policies* (MPs) permitem a imposição de restrições propagadas da raiz para as folhas e aplicadas automaticamente na resolução da TC. Uma TA pode, por exemplo, restringir algoritmos de assinatura utilizados pelas entidades da sua federação. Uma IM pode tornar a mesma política mais restritiva. As *Constraints* (CTs) permitem uma entidade restringir quais identificadores, tipos de entidade e profundidade hierárquica a partir dela. Uma IM, por exemplo, pode apenas aceitar subordinadas com o sufixo `.ufsc.br`. Por fim, as *Trust Marks* (TMs) são declarações de conformidade verificáveis, *i.e.*, JWTs assinados por uma autoridade de acreditação (um emissor declarado pela TA), usadas para atestar uma semântica definida pelo perfil da federação. Um SP, por exemplo, pode ter um TM indicando pertencimento à federação ou atestando conformidade com o *Security Incident Response Trust Framework* (SIRTFI). O uso desses mecanismos está em discussão no grupo de *Profiles* da *eduGAIN* [Harris and Vaghetti 2025]. A Tabela 1 resume as diferenças supracitadas entre os modelos.

Tabela 1. Modelo de confiança: CAFe SAML *versus* CAFe OIDFed.

Característica	CAFe SAML	CAFe 2.0 (OIDFed)
Estabelecimento	Pré-provisionado, periódico	Dinâmico, em tempo real
Artefato de confiança	Arquivo XML agregado	Cadeia de ESs assinados
Granularidade	Agregado inteiro	Por entidade, ao longo da TC
Âncora de confiança	Lista central	*Trust Anchor* comum
Imposição de requisitos	Manual	*Metadata Policy*
Conformidade verificável	*Entity attributes*	*Trust Marks*

[3]Por exemplo, o XML da CAFe.

4. Conclusão

Este artigo comparou a CAFe SAML à CAFe 2.0 em duas dimensões. Na topologia, a estrutura de dois níveis e sem soberania institucional dá lugar à hierarquia em árvore, capaz de refletir a organização administrativa das instituições. No modelo de confiança, evolui-se da agregação estática de metadados em um arquivo central para a TC dinâmica, ancorada em TAs e verificada a cada resolução, enriquecida por MPs, CTs e TMs.

A articulação entre as duas dimensões apresentadas é o que viabiliza nativamente a noção de subfederação. A topologia hierárquica fornece a estrutura e os mecanismos de confiança fornecem a garantia de verificabilidade. Uma IM pode atuar como TA para um subconjunto de provedores que, ao adotarem-na como TA, passam a aceitar apenas TCs ancoradas nela, constituindo uma subfederação. Nela, a composição é restringida por CTs, a postura de segurança fixada pelas MPs e o ingresso pode ser condicionado à posse de TMs que atestem conformidade. Desse modo, SPs destinados a um público restrito podem participar da federação em um domínio de confiança delimitado, em vez de permanecerem fora dela ou dependerem da liberação de atributos configurada manualmente, par a par, em cada provedor. Permanecem em aberto as questões de governança sobre gestão de TMs, MPs e CTs, e de migração do SAML para o OIDFed. Esses pontos, em discussão na eduGAIN [Harris and Vaghetti 2025], constituem trabalhos futuros.

Referências

[Ferdous and Poet 2013] Ferdous, M. S. and Poet, R. (2013). Dynamic identity federation using security assertion markup language (saml). In *IFIP Working Conference on Policies and Research in Identity Management*, pages 131–146. Springer.

[Flanagan 2024] Flanagan, H. (2024). Is there a future for refeds and r&e federations? Disponível em: https://refeds.org/a/2984. Acesso em: 17 jun. 2026.

[Harris and Vaghetti 2025] Harris, N. and Vaghetti, D. (2025). edugain technical profiles working group. Disponível em: `https://wiki.geant.org/display/eduGAIN/eduGAIN+Technical+Profiles+Working+Group`. Accesso em 17 jun. 2026.

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

[Jones and Bradley 2024] Jones, M. and Bradley, J. (2024). Trust establishment with openid federation. PDF presentation. Internet Identity Workshop (IIW), Mountain View, CA.

[Jones 2020] Jones, M. B. (2020). OpenID Connect federation 1.0: Enabling trust at scale. Presentation at the OpenID Summit Tokyo 2020. Accessed: 2025-06-11.

[Kantara Initiative 2019] Kantara Initiative (2019). *SAML V2.0 Implementation Profile for Federation Interoperability*. Kantara Initiative, version 1.1 edition.

[Kylau et al. 2009] Kylau, U., Thomas, I., Menzel, M., and Meinel, C. (2009). Trust requirements in identity federation topologies. In *2009 International Conference on Advanced Information Networking and Applications*, pages 137–145.

[OASIS 2005] OASIS (2005). Saml core specification version 2.0.

[Vaghetti 2024] Vaghetti, D. (2024). eduGAIN: OpenID Federation Pilot. GARR Workshop 24.