



Educação, Pesquisa
e Inovação em Rede

Gld no contexto de E-Ciência

Fiterlinge Sousa

Agenda

- Introdução
- Contexto do Provedor de serviços
- Contexto do Provedor de Identidades
- CiLogon como núcleo de interoperabilidade global
- Conclusões

Introdução

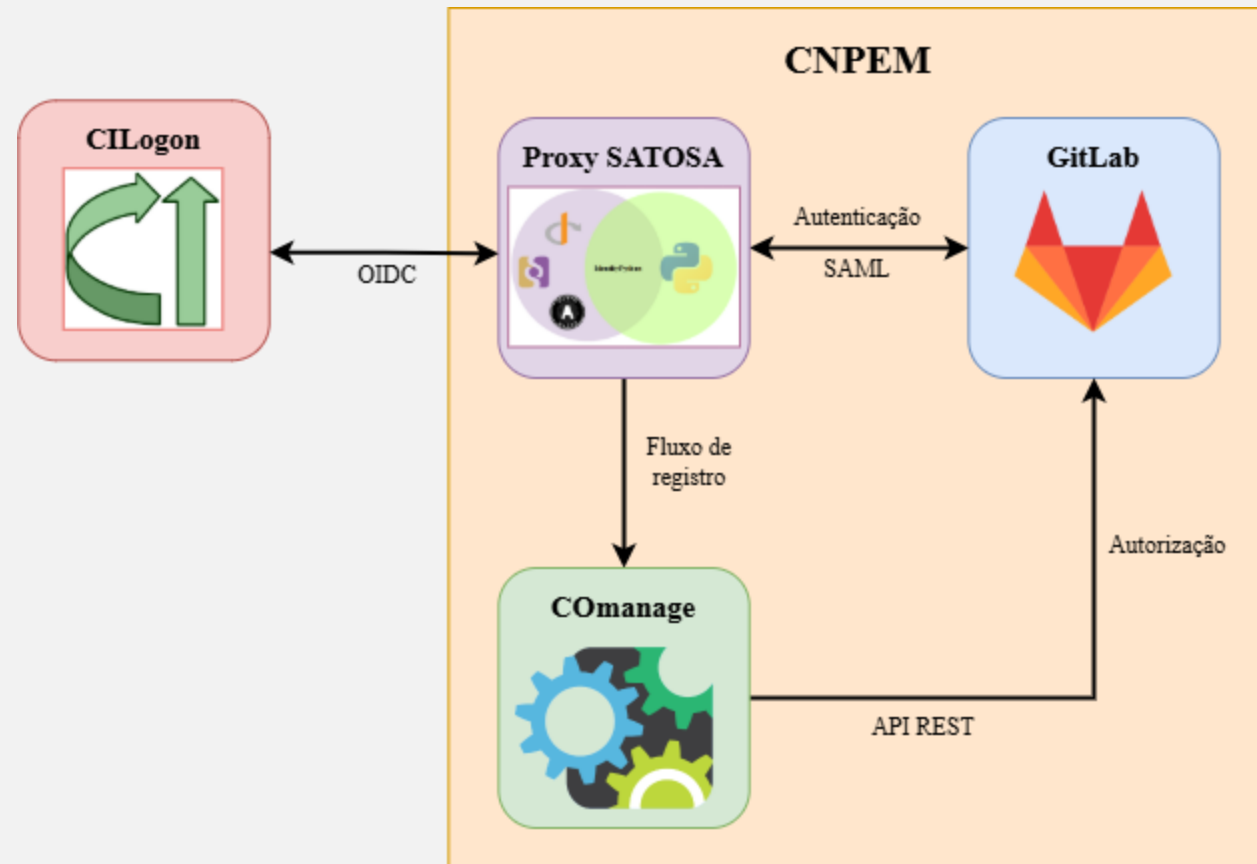
- **Cenário atual:**
 - Múltiplas instituições
 - Múltiplas federações
- **Desafios:**
 - Escalabilidade
 - Interoperabilidade
 - Confiança
 - Segurança

—● Arquitetura de Autenticação Federada

- Componentes principais:
 - Provedor de Identidade (IdP)
 - Provedor de Serviço (SP)
 - Atributos, metadados e regras de confiança
- PAPEL da RNP / CAFe no Brasil
- PAPEL global da EduGAIN e InCommon

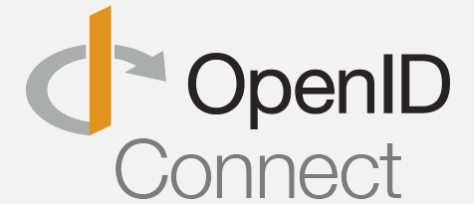
Contexto do Provedor de Serviços para e-Ciência

- Objetivo: permitir acesso de pesquisadores de diferentes instituições
- Necessidade de interoperar com múltiplas federações
- Exemplos de casos de uso:
 - Repositórios científicos
 - Plataformas de HPC, clusters e supercomputadores
 - Sistemas de gestão de dados experimentais
 - Instrumentação remota



—● Requisitos para o SP em um Ambiente Federado

- Suporte a SAML ou OIDC (conforme a federação)
- Requisitos de segurança (HTTPS, certificados confiáveis, TLS atualizado)
- Necessidade de metadados atualizados e assinados
- Adequação aos padrões globalmente aceitos

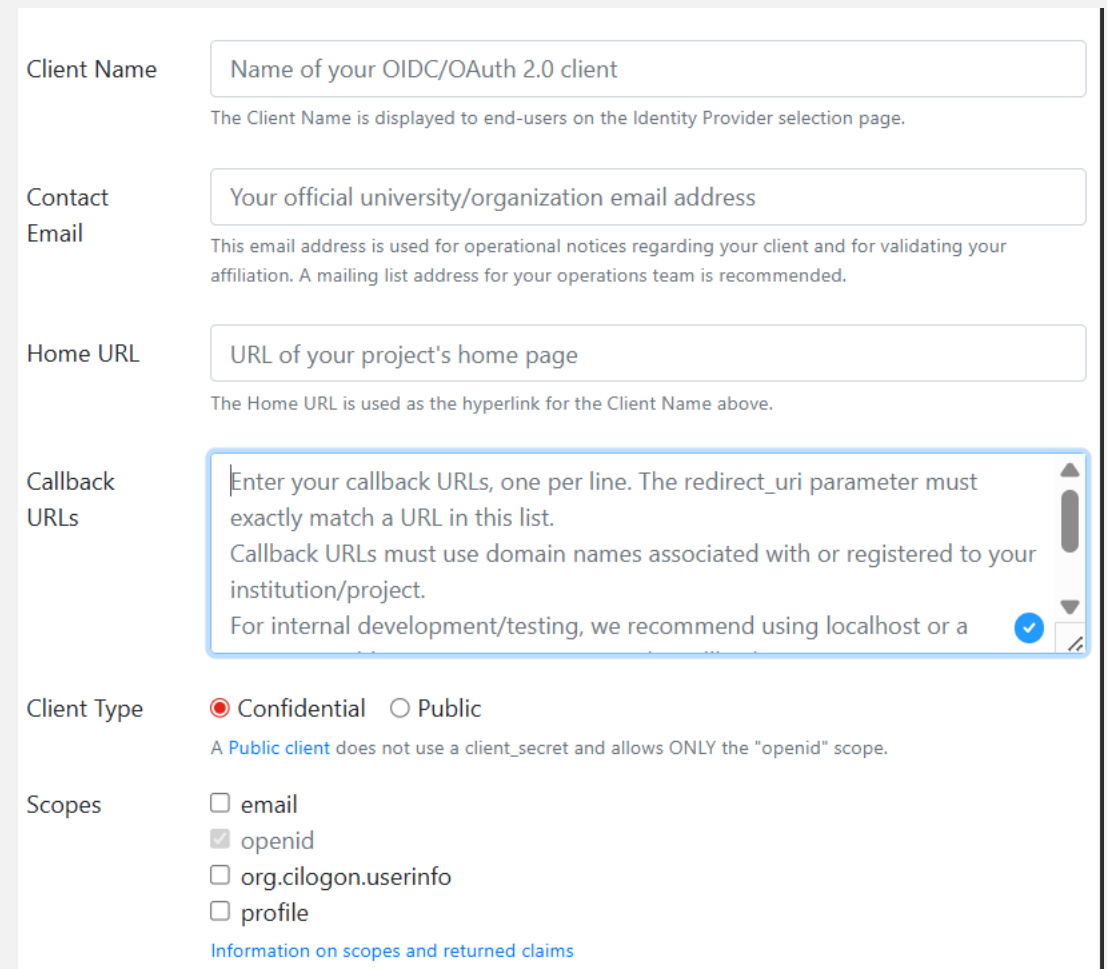


●—● Gestão de Usuários no SP

- Mapeamento e interpretação de atributos vindos dos IdPs
- Estrutura mínima de atributos esperados:
 - eduPersonPrincipalName(ePPN)
 - eduPersonUniqueId(ePUID)
 - Mail
 - displayName
 - affiliation(student, faculty, staff, member...)
- Como lidar com ausência de atributos ou inconsistências

— Boas Práticas para SPs em e-Ciência

- Suporte a múltiplos IdPs simultaneamente
 - Padrões de autorização baseados em atributos
 - Registro de logs compatíveis com auditoria federada
 - Como oferecer níveis de confiança diferenciados (LoA)
- O que o CILogon espera de um SP



The screenshot shows the CILogon client registration form. The 'Callback URLs' field is highlighted with a blue border. The form includes fields for Client Name, Contact Email, Home URL, and a list of Scopes. The Client Type is set to Confidential. The Scopes section shows 'openid' selected, with 'email', 'org.cilogon.userinfo', and 'profile' as options. A link for 'Information on scopes and returned claims' is at the bottom.

Client Name	Name of your OIDC/OAuth 2.0 client The Client Name is displayed to end-users on the Identity Provider selection page.
Contact Email	Your official university/organization email address This email address is used for operational notices regarding your client and for validating your affiliation. A mailing list address for your operations team is recommended.
Home URL	URL of your project's home page The Home URL is used as the hyperlink for the Client Name above.
Callback URLs	Enter your callback URLs, one per line. The redirect_uri parameter must exactly match a URL in this list. Callback URLs must use domain names associated with or registered to your institution/project. For internal development/testing, we recommend using localhost or a
Client Type	☒ Confidential ☐ Public A Public client does not use a client_secret and allows ONLY the "openid" scope.
Scopes	☐ email ☒ openid ☐ org.cilogon.userinfo ☐ profile Information on scopes and returned claims

— Contexto do IdP: Papel crítico do IdP

- O IdP como fonte de verdade sobre usuários
- Necessidade de atender requisitos nacionais e internacionais
- Responsabilidade:
 - Segurança (Sirtfi)
 - Precisão
 - Consistência dos atributos (R&S)



—● Requisitos para um IdP participar da CAFe

- Conformidade com CAFe Metadata Profile
- Teste de interoperabilidade
- Política de liberação de atributos
- Segurança institucional (gestão de senhas, MFA opcional etc.)



—● Requisitos adicionais para exportação para EduGAIN

- Aderência ao EduGAIN SAML Profile
- Conformidade com R&S (Research & Scholarship)
- Requisitos de privacidade dos atributos
- Sincronização e assinatura de metadados
- Transparência do IdP (página institucional, suporte, informações técnicas)



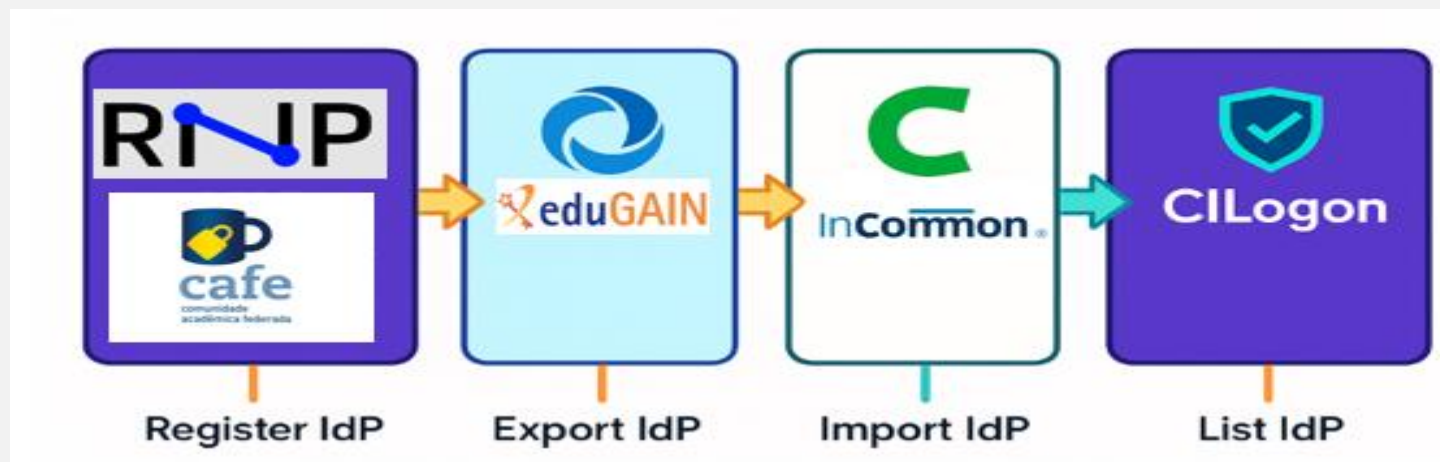
●—● Requisitos para integração com InCommon

- Padrões InCommon Federation Service Provider/Identity Provider
- Requisitos de segurança mais rígidos (InCommon Baseline Expectations)
- Obrigações de suporte e governança
- Conformidade com práticas de identidade norte-americanas



—● CiLogon como núcleo de interoperabilidade global

- O que é o CiLogon:
 - Autoridade de autenticação para e-Ciência
 - Ponte entre várias federações mundiais
- Permite que um pesquisador use seu IdP local em serviços internacionais
- Como o CiLogon faz a integração:



●—● Motivos para o IdP pode não está listado no CILogon

Um IdP pode estar ausente da lista pelos seguintes motivos:

- O IdP não está registrado na InCommon ou não é exportado para o eduGAIN. Os locais para verificar são: <https://technical.edugain.org/entities> e <https://www.incommon.org/federation/incommon-federation-entities/>.
- O IdP está marcado como hide-from-discovery (oculto na descoberta). Ver: <https://spaces.at.internet2.edu/x/DQjvCQ>
- **A InCommon pode descartar o IdP durante o processo de importação da eduGAIN porque ele falhou em alguma verificação de política.** Ver: <https://spaces.at.internet2.edu/x/YwfvCQ>
- O CILogon bloqueou (temporariamente) o IdP (muito raro). Nesse caso, o IdP ficará ausente de: <https://cilogon.org/include/idplist.xml>

●—● Conclusões

- A importância da gestão de identidade federada para e-Ciência (Institutos de pesquisa não devem gerenciar identidades externas)
- Benefícios para colaboração global e mobilidade de pesquisadores
- O papel do CILogon como “hub” de confiança internacional
- Próximos passos para instituições brasileiras

Obrigado!



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

