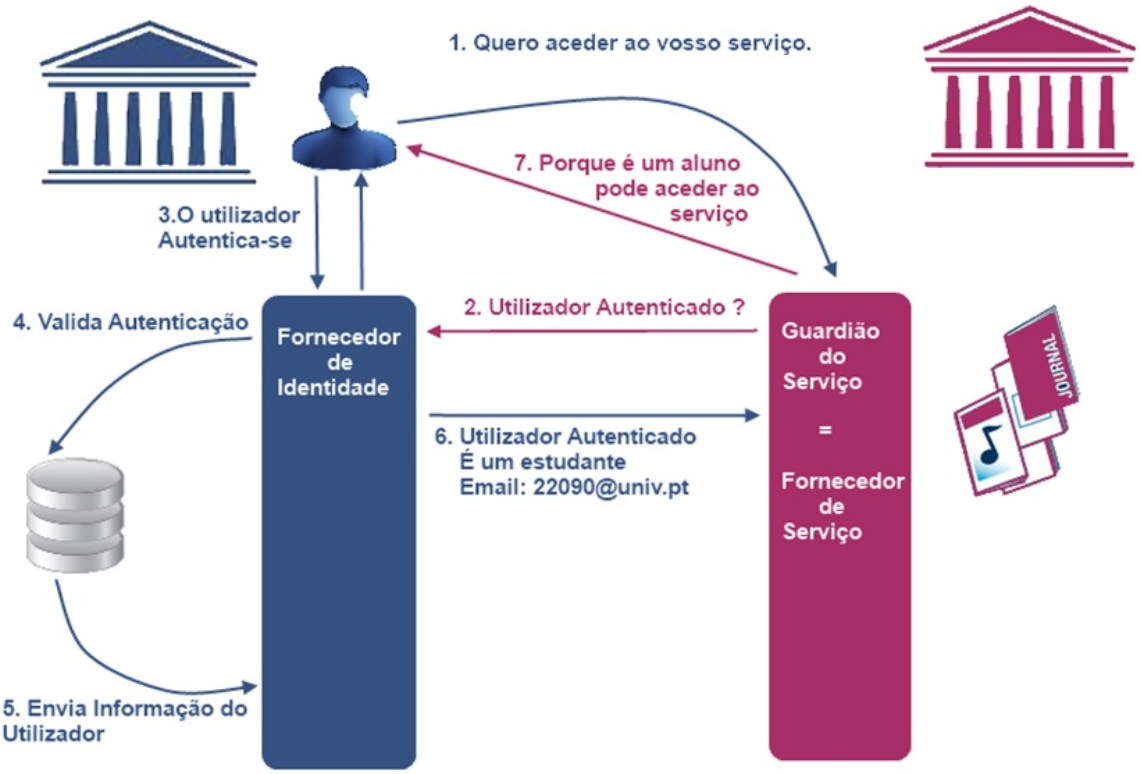
Atributos para que servem ?

Atributos

A informação que é trocada entre um Fornecedor de Identidade e um Fornecedor de Serviço assenta na sua maioria em dados do utilizador, que este autorizou que fossem transmitidos. É com base nesta informação que os serviços autorizam o acesso do utilizador e que podem criar os perfis de acesso.

Para que um utilizador possa aceder a um serviço RCTSaai ou eduGAIN é necessário que o Fornecedor de Identidade da instituição a que o utilizador pertence, envie atributos/informação de identidade para o serviço (Passo 6). Os serviços utilizam esta atributos/informação de identidade para controlar a autorização e/ou personalizar o serviço (Passo 7).

⚠ É fundamental que os Fornecedores de identidade forneçam informação de identidade precisa e autêntica, assim como, quem recebe esta informação garanta a privacidade e respeite restrições de privacidade colocadas pela federação ou fonte de informação.



A **especificação de atributos** é crucial para a troca de atributos dentro da federação. Esta especificação fornece uma base comum às organizações envolvidas no sentido em que a informação que partilham entre si é interpretada de forma idêntica. A RCTSaai e eduGAIN permite que sejam utilizados os atributos dos seguintes esquemas:

Schema eduPerson

Esquema LDAP desenhado pela Internet2 para incluir atributos bem conhecidos de elementos e organizações do ensino superior.

http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-200806.html

Schema SCHAC

Esquema desenhado pela TF-EMC2 da Terena com o objectivo de definir e promover um especificação na área do ensino superior para facilitar a troca de dados inter-instituicional.

http://www.terena.org/activities/tf-emc2/schac.html

Atributos

Atributos RCTSaai e eduGAIN

Configuração de Atributos

Saiba como configurar os atributos no Fornecedor de Identidade na página de Configuração de Serviços.

Atributos RCTSaai

Informação de Nomes

- givenName
- sn
- cn
- displayName

Atributos de Autorização

- eduPersonPrimaryAffiliation
- eduPersonScopedAffiliation
- eduPersonEntitlement

Identificadores

- email
- eduPersonPrincipalName

Organização

- o
- ou

Atributos eduGAIN

Atributos recomendados pelo *eduGAIN attribute Profile* aos Fornecedores de Identidade que participam no eduGAIN

Informação de Nomes

- givenName
- sn
- displayName
- commonName

Atributos de Autorização

- eduPersonAffiliation
- eduPersonScopedAffiliation
- eduPersonEntitlement

Identificadores

- email
- eduPersonPrincipalName
- eduPersonTargetID / persistentID

Organização

- o
- ou
- schacHomeOrganization
- schacHomeOrganizationType

Syntax e Valores

Informação de Nome

givenName *OID:* 2.5.4.42 (RCTSaai | eduGAIN)

Este atributo contém um ou vários valores que correspondem ao nome próprio do utilizador.

Exemplo: *João Pedro*

sn *OID:* 2.5.4.4 (RCTSaai | eduGAIN)

Este atributo contém um ou vários valores que correspondem ao(s) sobrenome(s) do utilizador.

Exemplo: *Melo Silva*

cn (commonName) *OID:* 2.5.4.3 (RCTSaai | eduGAIN)

Este atributo contém um ou vários valores que correspondem ao nome completo do utilizador.

Exemplo: João Pedro Melo Silva

displayName *OID:* 2.16.840.1.113730.3.1.241 (RCTSaai | eduGAIN)

Este atributo é de valor único e corresponde aos nomes que o utilizador prefere para visualização (ex.: Nome do utilizador quando realiza o login)

Exemplo: João Pedro Silva

Atributos de Autorização

eduPersonAffiliation *OID:* 1.3.6.1.4.1.5923.1.1.1.1 (eduGAIN)

Este atributo é de múltiplo valor e representa o(s) vínculo(s) entre o utilizador e a instituição.

Obrigatório

Os Fornecedores de Identidade que participam no eduGAIN tem de assegurar que os atributos relativos à filiação do utilizador à instituição (eduPersonPrimaryAffiliation, eduPersonScopedAffiliation, eduPersonAffiliation) utilizam a semântica definida a negrito no documento *"REFEDs ePSA usage comparison"*.

Termos Consistentes

- **member (Membro)**

  Inclui professores, funcionários, alunos e outros benificiários aos quais foram atribuídos um conjunto básico de privilégios que se enquadram na adesão à comunidade universitária (ex.: privilégios da biblioteca).

- **faculty (Professor)**

  Inclui os utilizadores em que a principal função é o ensino ou a investigação (ex.: professores e investigadores).

- **student (Estudante)**

Inclui os utilizadores que se encontra a estudar ao nível da licenciatura ou pós-graduação.

- **alum**

Inclui utilizadores que foram antigos estudantes da organização.

- **library-walk-in**

Inicialmente este valor representava um utilizador que se encontrava fisicamente na biblioteca para acesso a recursos licenciados. Nos últimos anos foi alargado a utilizadores que frequentam a biblioteca e utilizam a rede do campus, ou que utilizam estações de trabalho do campus.

Termos Inconsistentes

Os seguintes valores não são confiáveis e não devem ser utilizados pelos Fornecedores de Serviço, a menos que sua semântica tenha sido verificada a nível bilateral com a Federação da Instituição ou Instituição de Origem:

- **staff**

Funcionários que não são professores nem investigadores.

- **employee**

Alguém contratado pela organização (tendo em consideração que algumas federações podem incluir empregados não remunerados ou sem contrato).

eduPersonPrimaryAffiliation *OID:* 1.3.6.1.4.1.5923.1.1.1.5 (RCTSaai | eduGAIN)

Este atributo é de valor único e define a relação considerada principal entre o utilizador e a instituição. O valor permitido corresponde a um dos termos consistentes referidos acima para o atributo eduPersonAffiliation.

eduPersonScopedAffiliation *OID:* 1.3.6.1.4.1.5923.1.1.1.9 (RCTSaai | eduGAIN)

Este atributo é de múltiplo valor e representado da seguinte forma: **affiliation@dominio (corresponde a afiliação do utilizador no respectivo domínio de segurança)**

O domínio (scoped) utilizado nos atributos corresponde ao domínio da instituição que gere o fornecedor de identidade. Caso a instituição possua mais do que um domínio que identifique a instituição, devem escolher apenas o domínio que considera como principal. Este domínio deve ser único na federação, mesmo quando realizam registo com outras federações.

O domínio utilizado no eduPersonScopedAffiliation corresponde ao valor do domínio utilizado no atributo eduPersonPrincipalName.

⚠ Para os fornecedores de serviço que utilizam atributos “Scoped” (eduPersonScopedAffiliation, eduPersonPrincipalName - valor@***dominio***) é recomendado que utilizem os mecanismos disponíveis que permitem a validação do domínio associado corresponde ao fornecedor e validar que o **domínio** associado é da responsabilidade do fornecedor de Identidade que fornece o atributo.

eduPersonEntitlement *OID:* 1.3.6.1.4.1.5923.1.1.1.7 (RCTSaai | eduGAIN)

Este atributo pode ter múltiplos valores associados e permite a uma instituição indicar que um determinado utilizador satisfaz um conjunto de condições adicionais que se aplicam para acesso a um determinado serviço.

Os fornecedores de serviços definem os valores do atributo, compete aos fornecedores de identidade atualizarem os utilizadores que satisfazem as definições. Desta forma o fornecedor de serviço delega parcialmente ou na totalidade a responsabilidade de autorização a determinados recursos no fornecedor de identidade.

Exemplos:

- Serviço Elsevier

Para os utilizadores autorizados a aceder ao serviço Elsevier deve associar-se ao atributo eduPersonEntitlement o valor: **urn:mace:dir:entitlement:common-lib-terms.**

Os valores deste atributo podem eventualmente representar informação pessoal ou sensível, recomenda-se que o fornecedor de identidade controle que os valores libertados são elegíveis para fornecedor de serviço em questão. Este controlo é facilmente configurado através da configuração de filtros.

Identificadores

eduPersonPrincipalName *OID:* 1.3.6.1.4.1.5923.1.1.1.6 (RCTSaai | eduGAIN)

Este atributo corresponde ao identificador único e permanente do utilizador na instituição para todos os serviços.

Sintaxe do Atributo: local-name (valor único)

O “local-name” corresponder ao identificador utilizado no login do utilizador (ex.: uid, SamAccountName, etc.).

email *OID:* 0.9.2342.19200300.100.1.3 (RCTSaai | eduGAIN)

Este atributo corresponde ao endereço de correio do utilizador.

Para os serviços da federação o mail associado ao utilizador tem de corresponder ao mail institucional.

eduPersonTargetedID (a.k.a. SAML2 persistent NameID) *OID:* 1.3.6.1.4.1.5923.1.1.1.10 (eduGAIN)

Este atributo é de valor único e define um identificador único e persistente associado ao utilizador, por serviço.

Exemplo:

Organização

o *OID:* 2.5.4.10 (RCTSaai)

Este atributo define a organização de topo a que o utilizador está associado.

No caso de instituições em cenário distribuído (ex.: um fornecedor de identidade por faculdade) este atributo deve ser preenchido com o mesmo valor.

Exemplo: Para um aluno da Faculdade de Ciência o valor que o fornecedor de identidade deve libertar para o atributo “o” é “Universidade de Lisboa”.

ou *OID:* 2.5.4.11 (RCTSaai)

Este atributo define a unidade orgânica a que o utilizador pertence.

Exemplo: Faculdade de Letras

schacHomeOrganization *OID:* 1.3.6.1.4.1.25178.1.2.9 (eduGAIN)

Este atributo é de valor único e define a Organização de origem do utilizador, utilizando o nome DNS dessa mesma organização.

No caso de instituições em cenário distribuído (ex.: um fornecedor de identidade por faculdade) este atributo deve ser preenchido com o valor referente à Unidade Orgânica.

Exemplo: Para um aluno da Faculdade de Ciência da Universidade de Lisboa, o valor que o fornecedor de identidade deve libertar para o atributo “schacHomeOrganization” é “fc.ul.pt”.

Exemplo: fc.ul.pt

Configurar Atributos

A informação necessária para a configuração de atributos de um Fornecedor de Identidade está disponível nos documentos de configuração.

Libertar Atributos

Com o crescente número de Fornecedores de Serviço a integrar as federações e a necessidade de identificar os utilizadores de ensino superior e investigação através do envio de atributos (nome, email, afiliação institucional, etc.) **verifica-se que o processo de configuração Serviço a Serviço nos Fornecedores de Identidade não escala.**

Com o objectivo de agilizar o processo de envio de atributos e assegurar a confiança no envio dos mesmos, foi criado o atributo ***Categoria*** na definição SAML da Entidade (SAML V2.0 Metadata Extension for Entity Attributes). O valor deste atributo na entidade SAML (Fornecedor de Identidade ou Fornecedor de Serviço) representa uma alegação de que a entidade cumpre os requisitos da categoria, e a garantia de ser membro da mesma. As alegações de membro de uma categoria podem ser utilizadas para definir a forma como são libertados os atributos de um fornecedor de identidade, influenciar decisões a nível da interface do serviço de descoberta ou para outra finalidade. Em geral, a utilização prevista de qualquer participação numa determinada categoria dependerá das definições e requisitos da própria categoria.

Tipos de Categorias

Categorias de Serviço

Uma categoria de serviço é um grupo de Fornecedores de Serviço com um propósito comum. Por exemplo, a categoria “Research&Scholarship” é uma categoria de serviço que tem como objetivo tornar o processo de envio de atributos escalável.

Info. para o Fornecedor de Serviço

Para que um Fornecedor de Serviço seja registado na metadata RCTSaai e eduGAIN com *a categoria "Research&Scholarship"* é necessário declarar a sua intenção de adesão e cumprir os requisitos associados à categoria.

```
<!-- Fornecedor de Serviço educonf -->
<md:EntityDescriptor entityID="https://educonf-directory.geant.net/simplesaml/module.php/saml/sp/metadata.php
/eduCONF">
    <md:Extensions>
                ....

         <mdattr:EntityAttributes>
        <saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
          <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:
AttributeValue>
        </saml:Attribute>
      </mdattr:EntityAttributes>

         </md:Extensions>
....
</md:EntityDescriptor>
```

Categorias de Suporte

Uma categoria de suporte corresponde a um conjunto de entidades que suportam uma determinada categoria. Caso se trate de uma categoria de serviço, então corresponde a um conjunto de Fornecedores de Identidade que suportam a categoria de serviço.

Info. para o Fornecedor de Identidade

Um fornecedor de identidade ao suportar uma categoria (ex.: configurar o filtro que liberta um conjunto de atributos a todos os serviços marcados com a categoria "Research&Scholarship") deve refletir na metadata as categorias que suporta .

```
<md:EntityDescriptor entityID="https://idp.aco.net/idp/shibboleth">
 <md:Extensions>
                ....

        <mdattr:EntityAttributes>
                <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:
names:tc:SAML:2.0:attrname-format:uri">
                <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:
AttributeValue>
                 <saml:AttributeValue>http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:
AttributeValue></saml:Attribute>
        </mdattr:EntityAttributes>
 </md:Extensions>
 <md:IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:1.1:
protocol urn:oasis:names:tc:SAML:2.0:protocol">
...
</md:EntityDescriptor>
```

Categorias Recomendadas

REFEDS Research & Scholarship

A categoria “Research&Scholarship” foi criada pela **"REFEDS** – The Voice of Research and Education Identity Federations” com o objetivo de apoiar as federações na adoção de envio de atributos por categoria.

- REFEDS Research and Scholarship Entity Category Versão 1.2

Os candidatos à categoria “Research and Scholarship (R&S)” são os Fornecedores de Serviço que suportam atividades de investigação ou ensino, tais como, serviços de colaboração que implicam a interação de utilizadores de várias instituições/campus ou organizações virtuais (ex.: projetos que envolvem várias instituições de ensino/investigação).

Informação para Fornecedores de Serviço

Enquadram-se nesta categoria: Plataformas e serviços utilizados por investigadores ou alunos onde é necessário a colaboração, discussão ou outra interação entre os utilizadores, sendo que o envio de atributos com informação de identificação pessoal seja necessário para o correto funcionamento da plataforma ou serviço.

Não se enquadram nesta categoria:

- e-Journal, ebook ou outro acesso, onde o acesso aos conteúdos é realizado com base na afiliação do utilizador, sem a necessidade de informações pessoais.
- Serviços de venda de produtos ou que oferecem descontos aos funcionários ou alunos com base na filiação.

Informação para Fornecedores de Identidade

É recomendado que todos os Fornecedores de Identidade libertem o seguinte conjunto de atributos para Fornecedores de Serviço da categoria "R&S":

- **Identificadores Pessoais**: e-mail, Nome do Utilizador (displayName, e opcionalmente givenName e surname) e eduPersonPrincipalName
- **Identificador pseudónimo**: eduPersonTargetedID
- **Afiliação**: eduPersonScopedAffiliation

Um Fornecedor de Identidade suporta a categoria "Research&Scholarship" se:

Para um conjunto dos utilizadores enviar um subconjunto mínimo de atributos para Fornecedores de Serviço "R&S" sem o envolvimento administrativo, de forma automática ou sujeito ao consentimento do utilizador.

Subconjunto Mínimo de Atributos "R&S" : eduPersonPrincipalName, mail e displayName ou (givenName e sn)

Para aderir/configurar a categoria no seu Fornecedor de Serviço/Identidade consulte a página "Configuração de Categoria".

GEANT EU/EEA Data Protection Code of Conduct

A categoria "***EU/EEA Data Protection Code of Conduct***" criada pela **GEANT**, tem como objetivo garantir que os requisitos da ***Directiva de Protecção de Dados da EU*** são respeitados, relativamente ao envio de atributos pessoais por parte dos Fornecedores de Identidade para os Fornecedores de Serviço.

Esta categoria permite dar aos Fornecedores de Identidade e Fornecedores de Serviço terem a garantia que os parceiros funcionam em conformidade com a protecção de dados da EU.

Informação para Fornecedores de Serviço

Enquadram-se nesta categoria: Plataformas e serviços utilizados por investigadores ou alunos que operem dentro do espaço da União Europeia e onde é necessário a colaboração, discussão ou outra interação entre os utilizadores, sendo que o envio de atributos com informação de identificação pessoal seja necessário para o correto funcionamento da plataforma ou serviço.

Informação para Fornecedores de Identidade

É recomendado que todos os Fornecedores de Identidade libertem o seguinte conjunto de atributos para Fornecedores de Serviço da categoria "CoCo":

- **Identificadores Pessoais:** mail, cn, eduPersonPrincipalName
- **Identificador pseudónimo:** eduPersonTargetedID, SAML2 Persistent NameID (eduPersonTargetedID),
- **Afiliação:** schacHomeOrganization, schacHomeOrganizationType, eduPersonScopedAffiliation, eduPersonAffiliation

Um Fornecedor de Identidade suporta a categoria "EU/EEA Data Protection Code of Conduct" se:

Para um conjunto dos utilizadores enviar um subconjunto mínimo de atributos para Fornecedores de Serviço "CoCo" sem o envolvimento administrativo, de forma automática ou sujeito ao consentimento do utilizador.

Subconjunto Mínimo de Atributos "CoCo" :

- Atributo que indique a permissão para usar o serviço: eduPersonAffiliation, eduPersonEntitlement ou schacHomeOrganization
- Atributo que identifique o utilizador no serviço: SAML2 PersistentId ou eduPersonTargetedID, cn ou DisplayName
- Atributo para contacto do utilizador: email