jornadas FCCN

Maximizar o Valor da RCTSaai

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

Agenda da Sessão

- RCTSaai 2024
- HPE Clearpass Role and Policy Orchestration (Patrocinador)
- Ponto de Situação do Pacote de Instalação Shib. IdP e Novos Identificadores na federação
- Protocolos de Autenticação a sua evolução (SAML vs Oidc)
- Serviço Invite – Funcionalidade de Gestão Acessos a disponibilizar aos serviços brevemente
- Q&A

Área de Serviços de Redes
Serviço de Identidade Digital e Sistemas (SIDS)

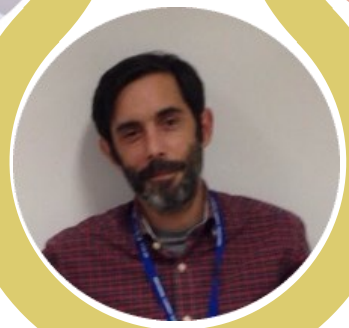
Emanuel Massano

Esmeralda Pires

João Guerreiro

André Leite

António Coucelo



Pedro Simões

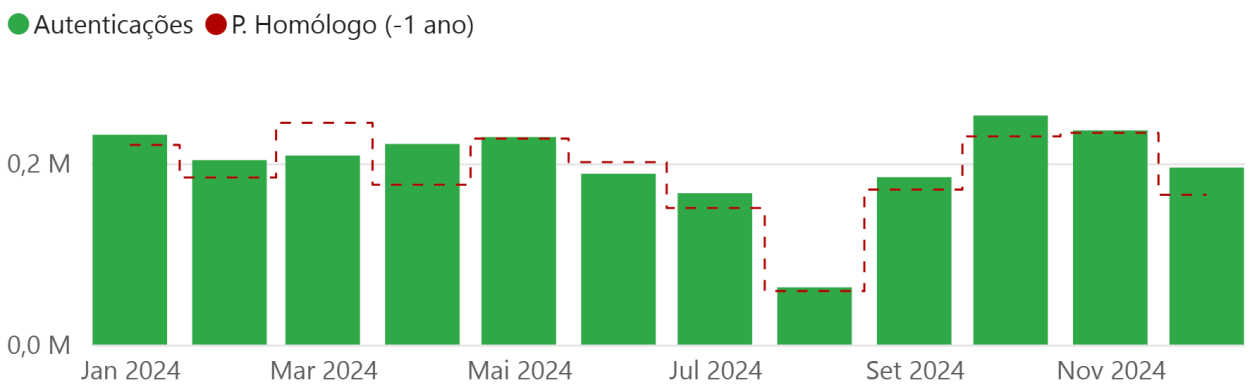
Filipe Santana

RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

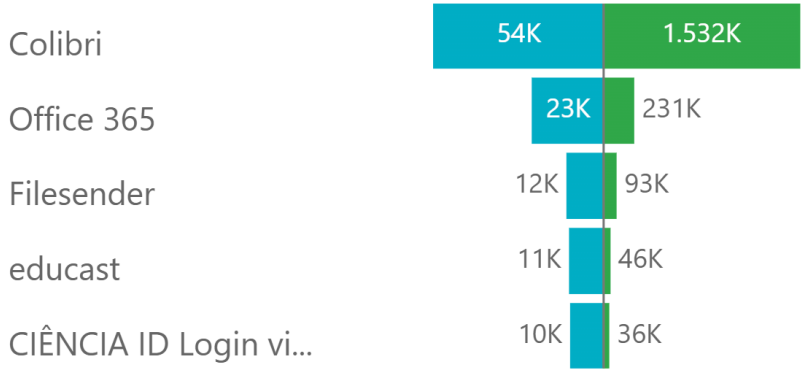
jornadas FCCN

Ano de 2024

Autenticações p/ Mês (+5%)



Top 5 Serviços - Utilizadores e Autenticações



Autenticações

2,4 M

P. Homólogo: 2,3 M (+5%)

Utilizadores Distintos

167,5 K

P. Homólogo: 147,3 K

(+14%)

Entidades Aderentes

82

(+4)

Entidades no eduGAIN

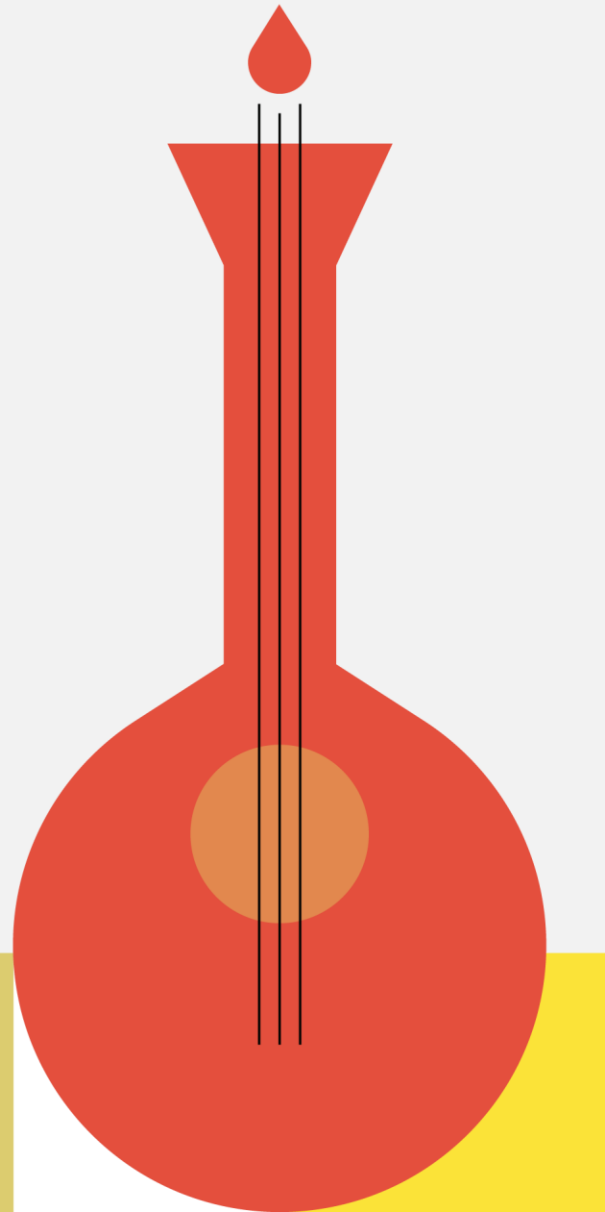
79

(+6)

jornadas FCCN

Patrocinador

HPE aruba, Eng. Pedro Lourenço



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

HPE Clearpass Role and Policy Orchestration

Pedro Lourenço, Systems Engineer

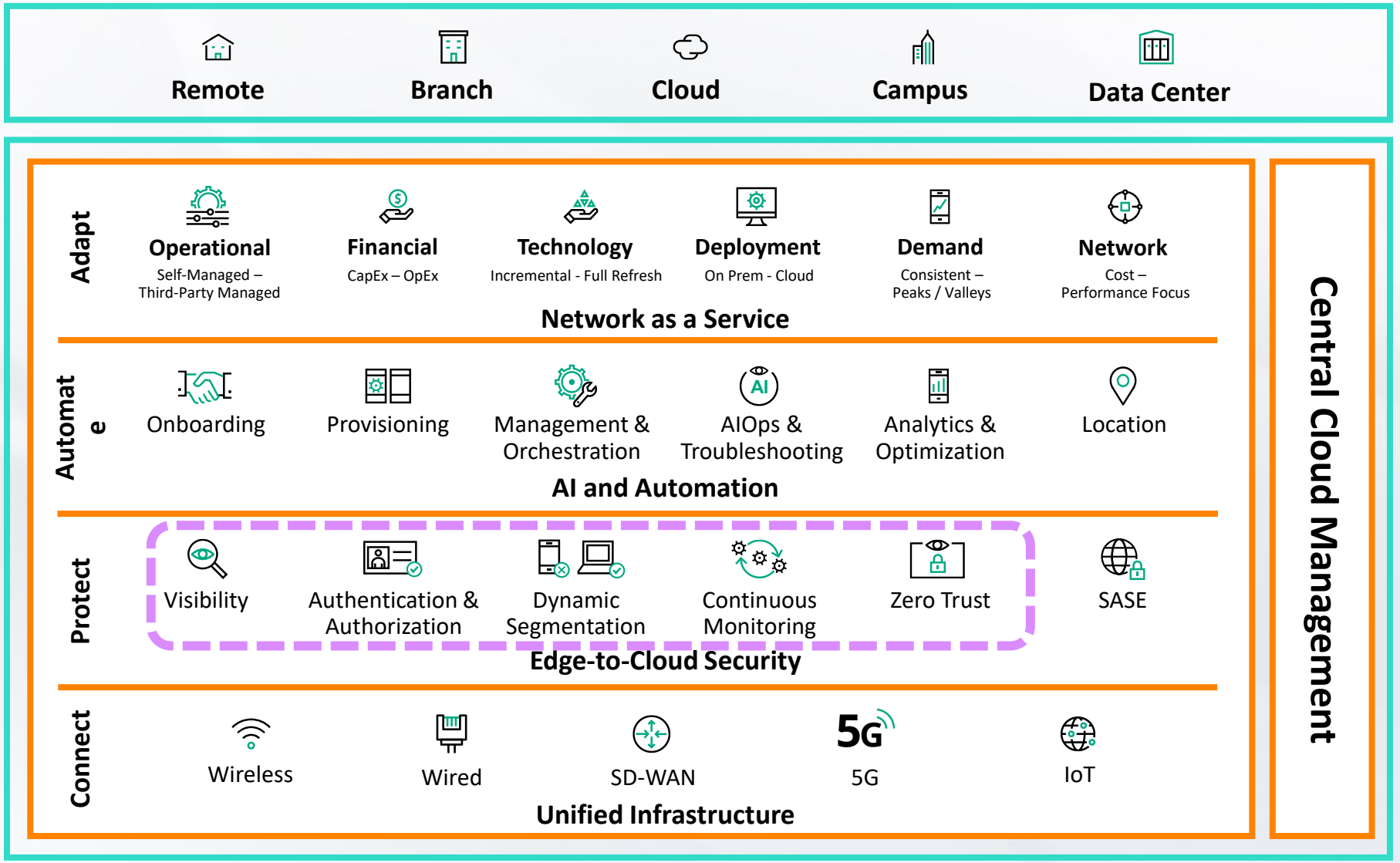
Maio 2025

Orchestrating network services from edge-to-cloud

HPE Aruba Networking

Powered by ESP

(Edge Services Platform)



HPE Aruba ClearPass solutions

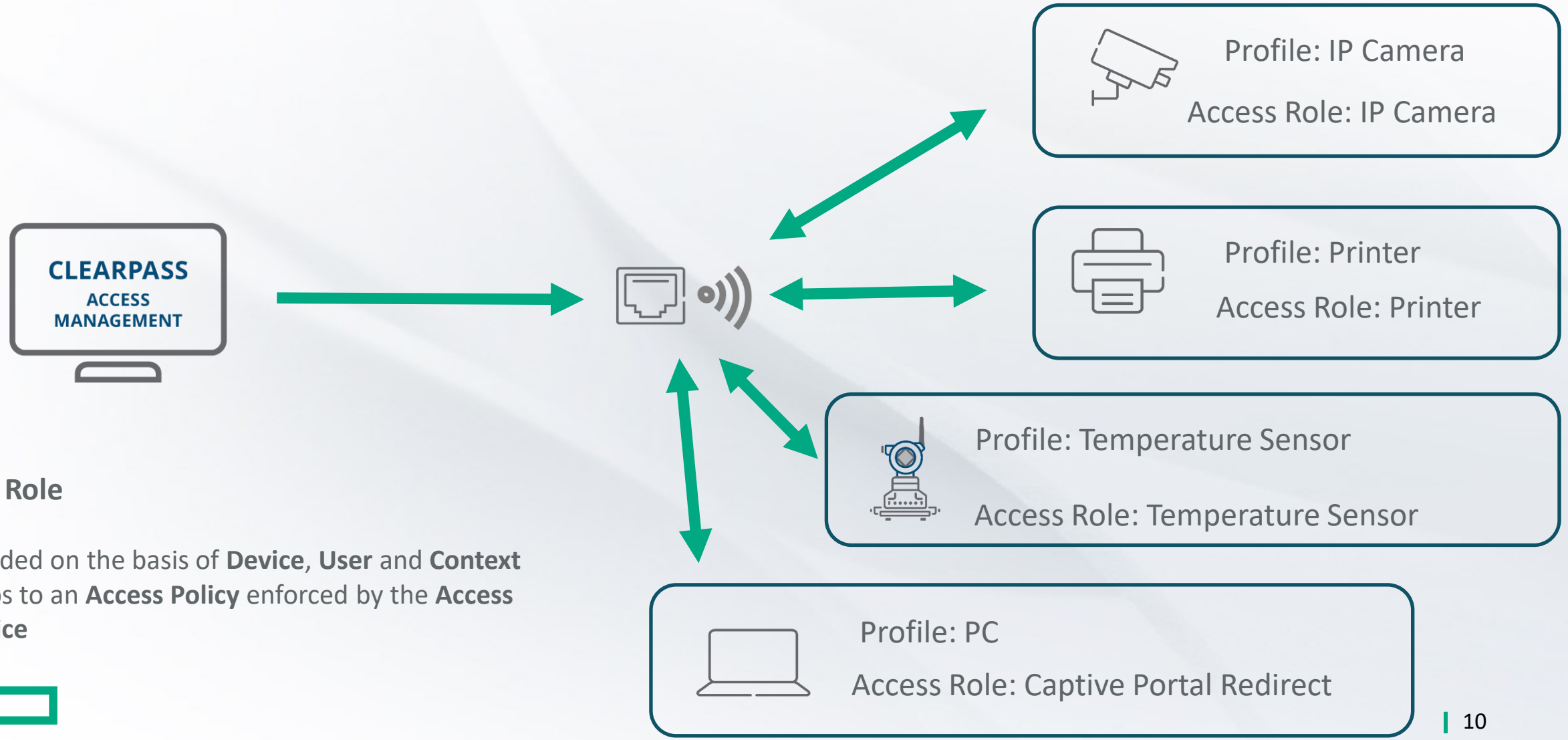
End-to-end user & device visibility, control, and automation

Vendor-neutral—**no lock-in**

Wired and Wireless Acess - Unknown Device Profiling

You can’t protect yourself of what you don’t know !

Wired and Wireless Acess - Unknown Device Profiling



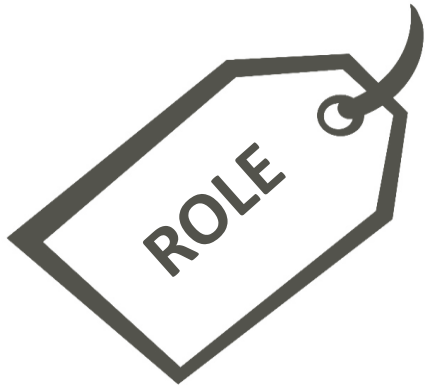
Access Role

- Decided on the basis of **Device**, **User** and **Context**
- Maps to an **Access Policy** enforced by the **Access Device**

Zero Trust: Who/What Are You? – Access Context

Access Request Context

- Client Credentials
- Access Request Timestamp
- Authentication Type
- Device Authentication
- Device Type/Fingerprinting
- Location
- Access Type
- Posture
- 3rd Party Context
- Other



ClearPass Comprehensive Profiler Methods

Helps ensure accurate fingerprints

Passive Profiling

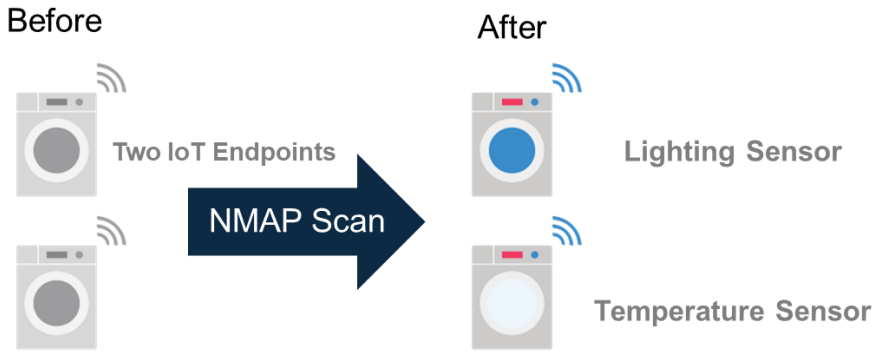
- DHCP Fingerprinting (MAC OUI & Certain Options)
  - DHCP Relay or SPAN
- HTTP User-Agent
  - AOS IF-MAP Interface, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Cisco Device Sensor
- Netflow/IPFIX
  - Identifies open ports

Active Profiling

- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP

Example with NMAP Port-based Scanner

- On-demand or pre-scheduled scans
- Granular visibility for like devices

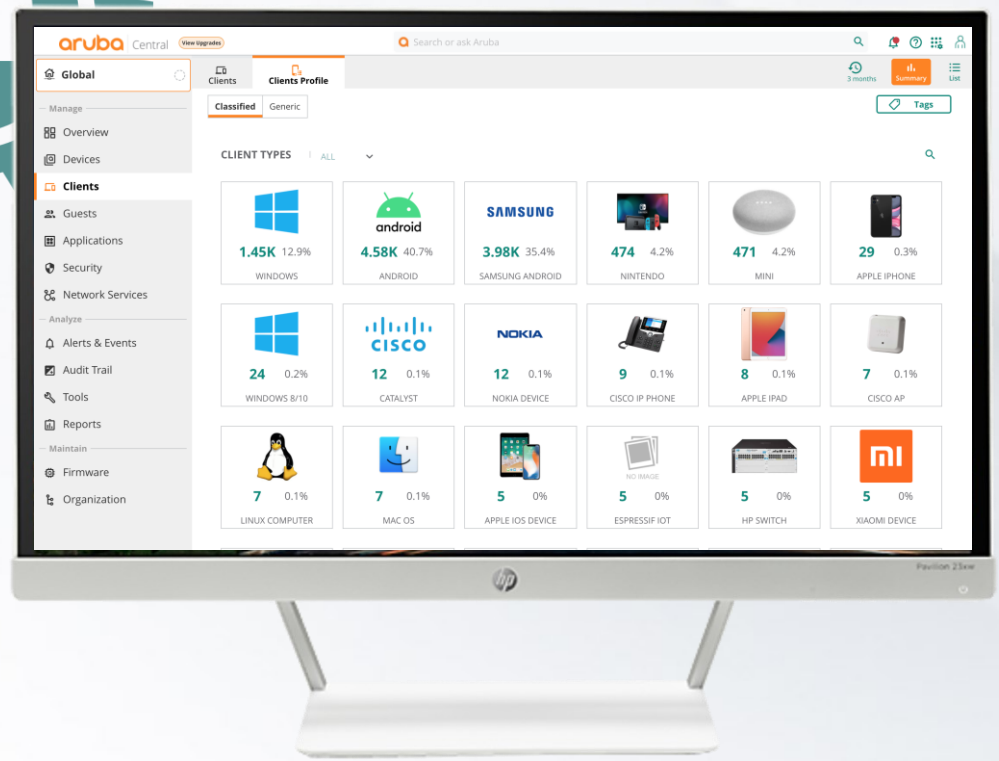






Client Insights – Understanding Traffic Flows

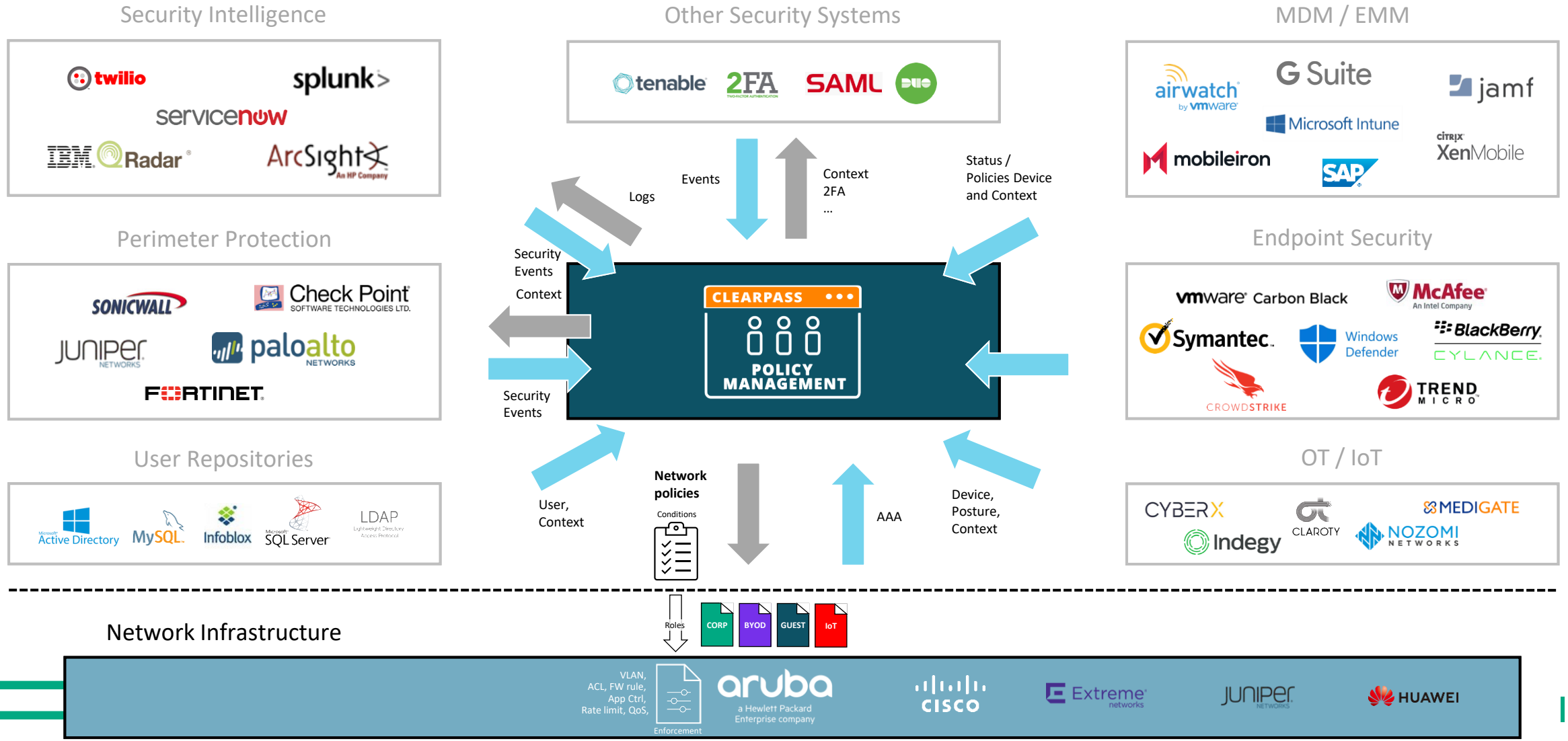
Complete endpoint inventory solution built into Aruba Central



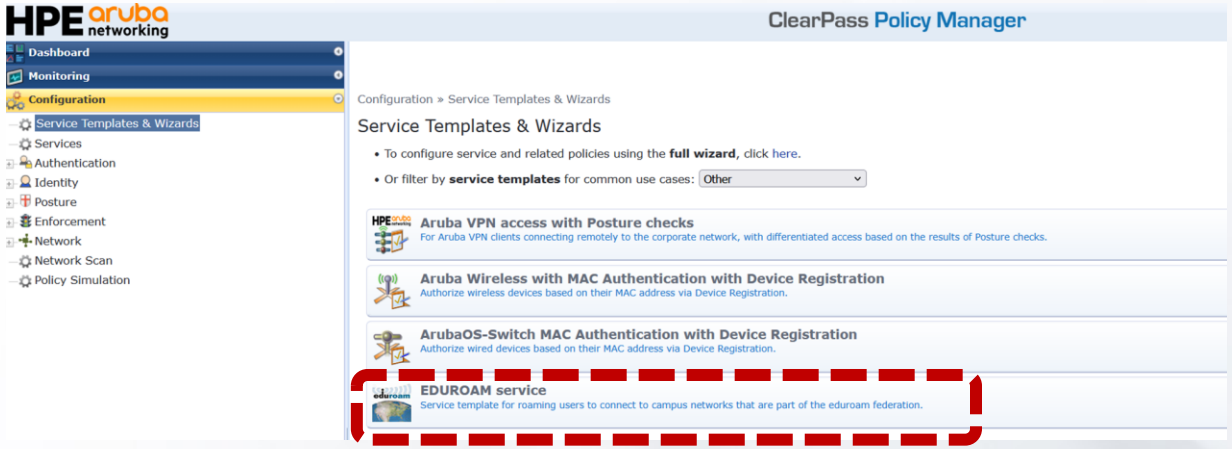
- Accurate AI/ML profiling with **~99% accuracy**
- No additional hardware—reduces complexity and **CAPEX**
- Immediate ROI with **IT efficiency gains**
- Always-on AI/ML monitoring **protects against security breaches**

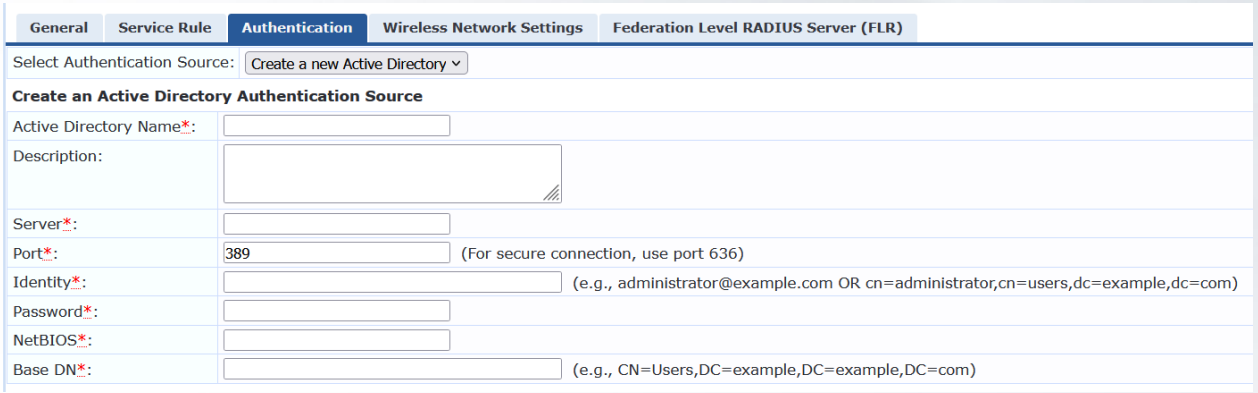
AAA, Role assignment Automation and Security Orchestration

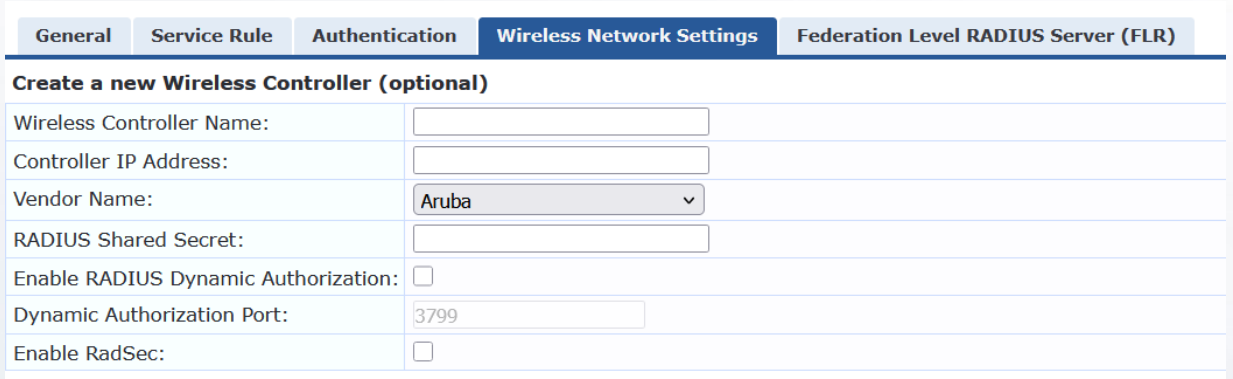
HPE Aruba ClearPass Policy Manager

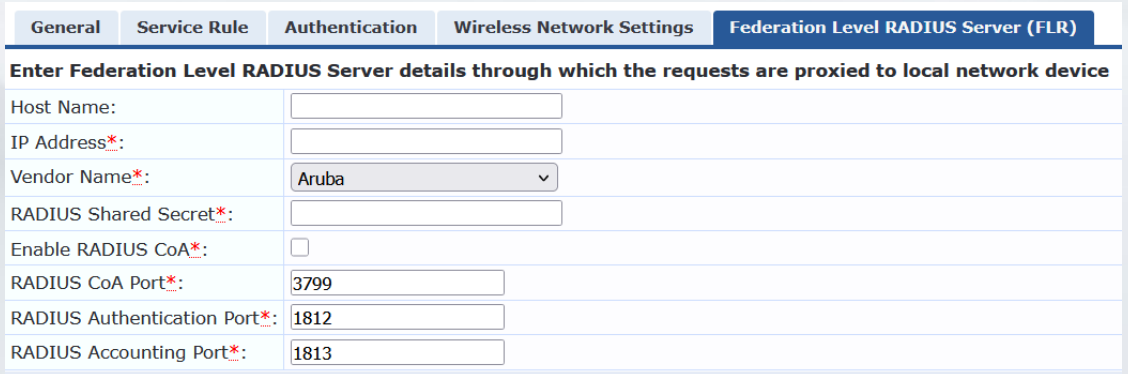


ClearPass EDUROAM Template Wizard Integrated



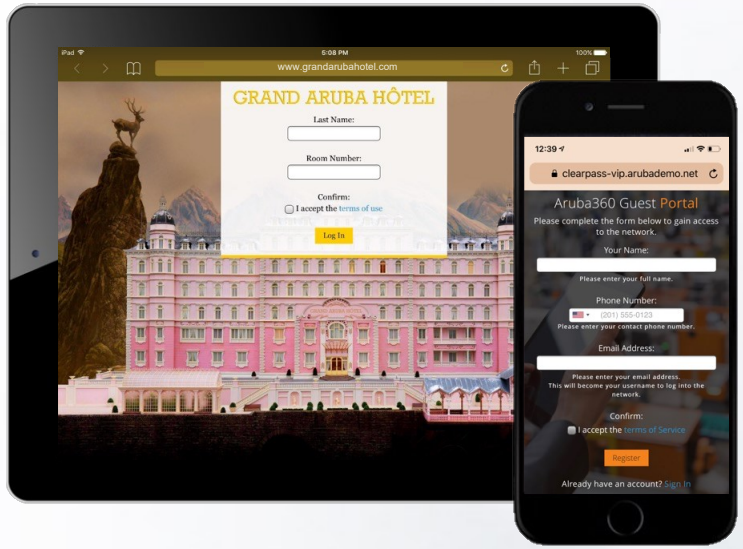


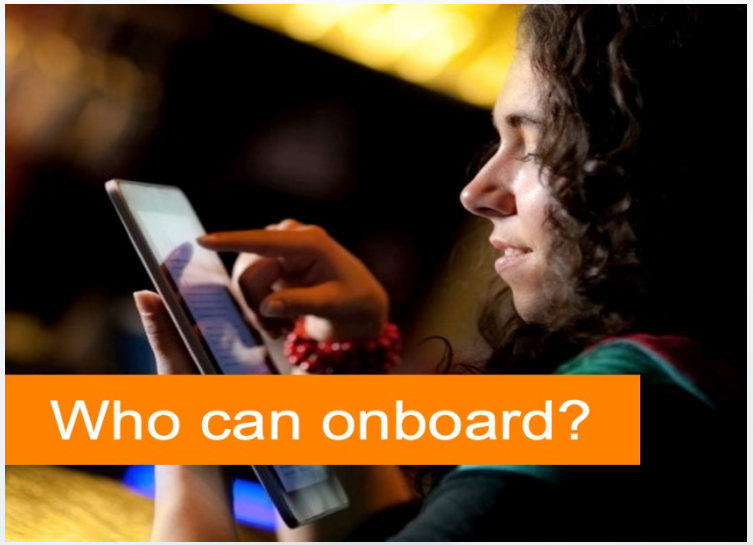


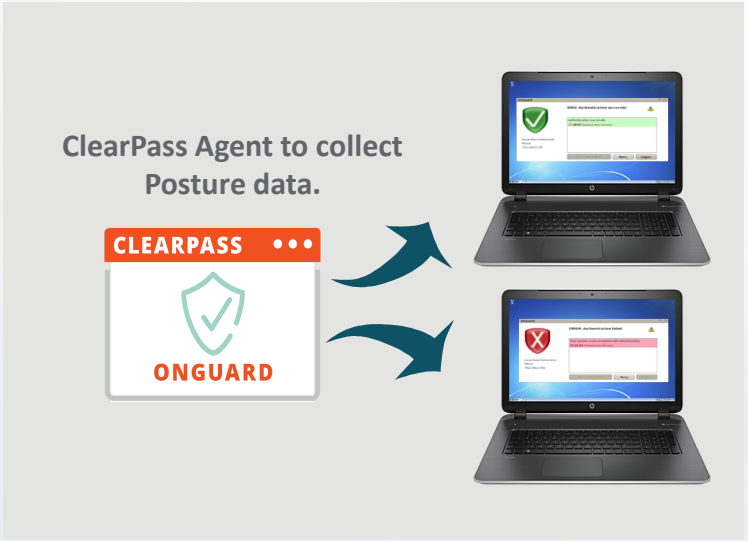


Designed to integrate with multiple diferente services including **EDUROAM**

Additional Embeded Services







Captive portal

- Easy process to manage guests.
- Custom Look & Feel
- +30 social network integratios.
- Self-registration, Login, alerts…

Certificate Authority

- ClearPass includes a CA.
- Tool to manage certificates.
- Wizard to deploy certificates.
- Management, renew & revocation.

Posture Analysis

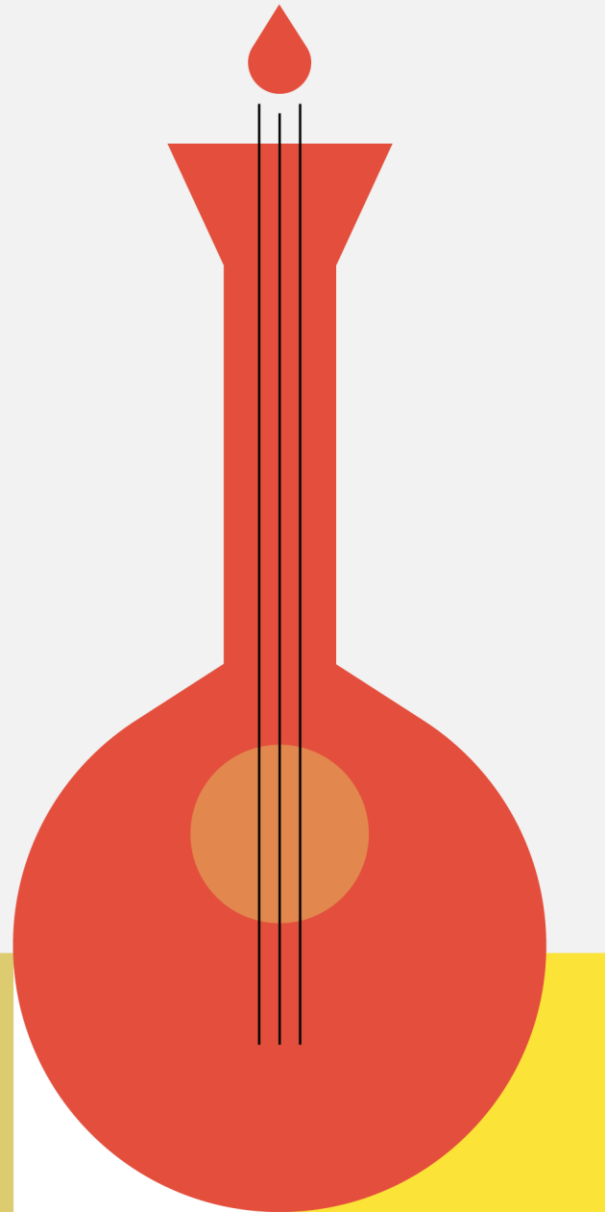
- Constant monitoring
- Device Posture
- Remediation
- Windows, Mac, Linux laptops

Obrigado

jornadas FCCN

Shibboleth IdP Actualizações & Transição para Novos Identificadores

Esmeralda Pires



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

jornadas FCCN

Shibboleth IdP & Pacote de Instalação

Atualizações

Shibboleth IdP – Versões em Fim de vida (EOL)

- ***Security Advisories***
  - ✓ *Shibboleht IdP V4*
  - ✓ *Shibboleth IdP V5*

IdP 4.3.3: Última versão da série 4.x sem vulnerabilidades conhecidas. No entanto, todas as versões da série 4.x já atingiram o fim do suporte (EOL).

Versão	5.1.4	5.1.3	5.1.2	5.1.1	5.1.0	5.0.0	4.3.3	4.3.2	4.3.1	4.3.0	4.2.1
EOL		mar/25	Jul/24	abr/24	mar/24	mar/24		set/24	mar/24	mar/23	jan/23

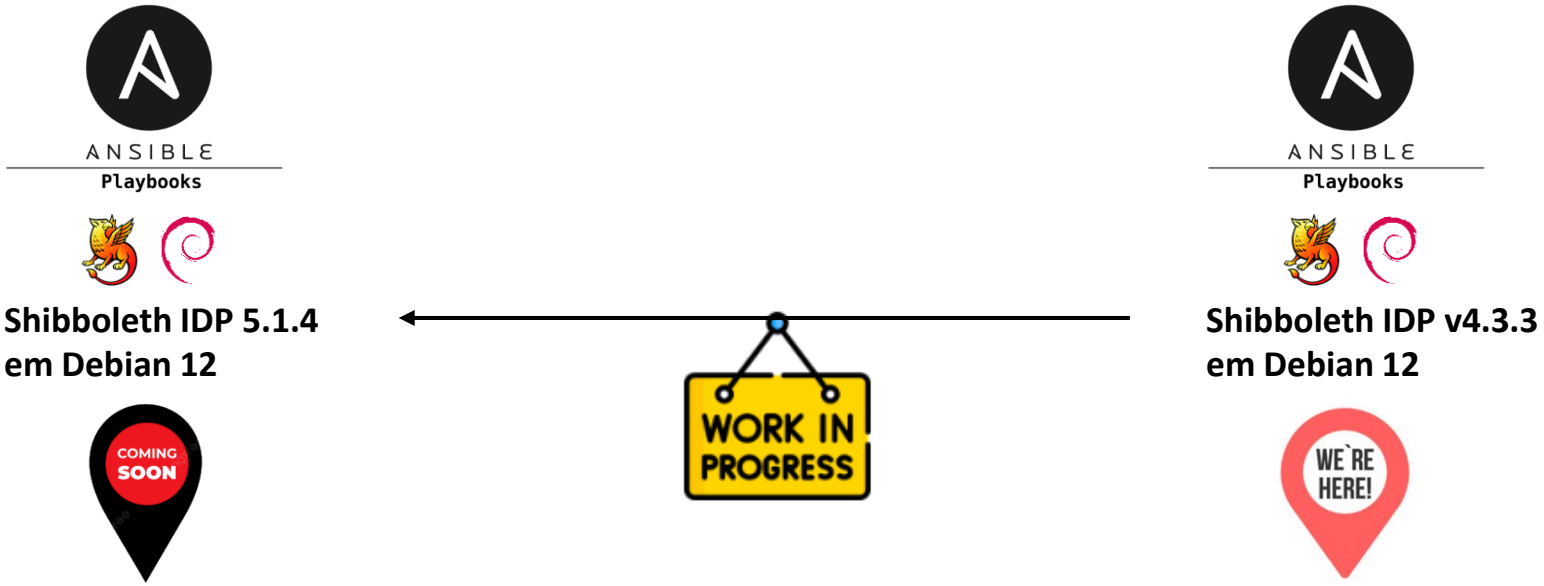
IdP 5.1.4: Esta é a versão mais recente e estável da série 5.x, sem vulnerabilidades conhecidas até o momento.

Risco de utilização de versões em Fim de Vida

- Potencial exposição a vulnerabilidades futuras que não serão corrigidas
- Incompatibilidades futuras com bibliotecas externas, como o Java, o OpenSAML, entre outras

Shibboleth IdP – Pacote de Instalação

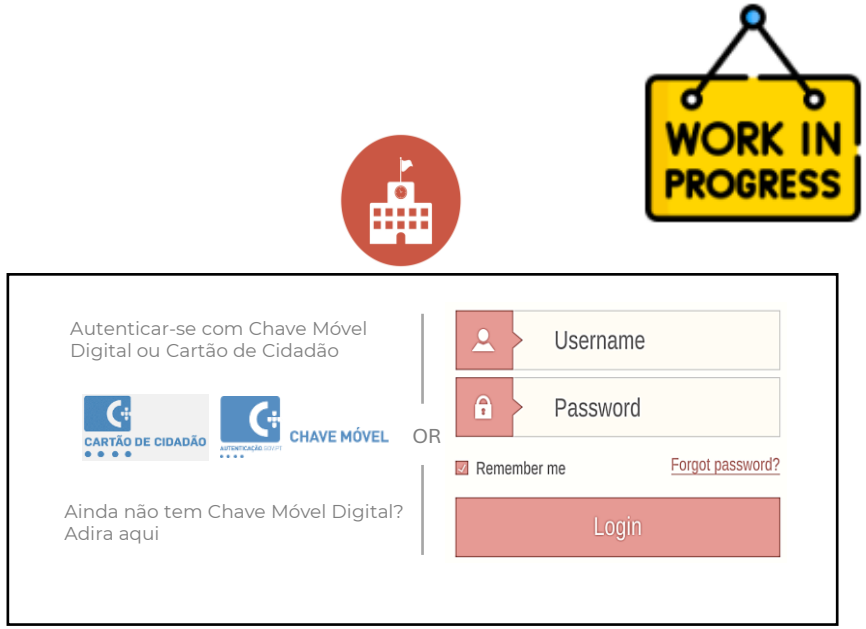
- **Disponível no Espaço RCTSaai / Área Técnica**
  https://share.fccn.pt/sites/rctsaai/



Versão	5.1.4	5.1.3	5.1.2	5.1.1	5.1.0	5.0.0	4.3.3	4.3.2
EOL		mar/25	Jul/24	abr/24	mar/24	mar/24		set/24

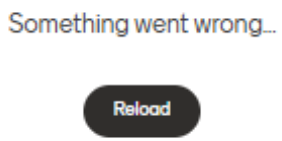
Shibboleth IdP – Plugin de Autenticação.Gov

- **Plugin Autenticação.Gov - Atualização em curso para garantir compatibilidade com versão Shibboleth IdP v5.1.4**



Shibboleth IdP – Pacote de Instalação

Evolução do pacote de instalação: manter Ansible ou migrar p/ Container?



jornadas FCCN

Próximo Pacote de Instalação

Configurações +Simples

Shibboleth IdP – Configurações +Simples

- **Attribute Registry**

  Sistema de regras que define como os atributos são codificados e decodificados para os vários esquemas (localizados na pasta conf/attributes/)

```
drwxr-xr-x 2 tomcat tomcat  4096 Apr 23 19:15 custom
-rw-r--r-- 1 tomcat tomcat  1430 Apr 22 13:11 default-rules.xml
-rw-r--r-- 1 tomcat tomcat  3218 Apr 22 13:11 eduCourse.xml
-rw-r--r-- 1 tomcat tomcat 21214 Apr 22 13:11 eduPerson.xml
-rw-r--r-- 1 tomcat tomcat 31170 Apr 22 13:11 inetOrgPerson.xml
-rw-r--r-- 1 tomcat tomcat  4498 Apr 22 13:11 samlSubject.xml
-rw-r--r-- 1 tomcat tomcat 26704 Apr 22 13:11 schac.xml
```

Ativo por omissão na versão 5 (conf/services.xml)

```
<!--
This is suitable for new installs but will usually produce duplicate Attribute
output if a legacy resolver file is used that contains AttributeEncoders.
-->
<util:list id ="shibboleth.AttributeRegistryResources">
    <value>%{idp.home}/conf/attribute-registry.xml</value>
    <value>%{idp.home}/conf/attributes/default-rules.xml</value>
    <value>%{idp.home}/conf/attribute-resolver.xml</value>
</util:list>
```

Shibboleth IdP – Configurações +Simples

- **Attribute Registry**

  - Oferece uma maneira mais eficiente de organizar e processar atributos

  - O mapeamento do atributo é feito automaticamente, desde que o identificador seja igual ao definido no esquema localizado em /conf/attributes.

/conf/attributes/schac.xml

```
<bean parent="shibboleth.TranscodingProperties">
    <property name="properties">
        <props merge="true">
            <prop key="id">schacHomeOrganization</prop>
            <prop key="transcoder">SAML2StringTranscoder SAML1StringTranscoder</prop>
            <prop key="saml2.name">urn:oid:1.3.6.1.4.1.25178.1.2.9</prop>
            <prop key="saml1.name">urn:oid:1.3.6.1.4.1.25178.1.2.9</prop>
            <prop key="displayName.en">Home Organization</prop>
            <prop key="displayName.de">Heimatorganisation</prop>
            <prop key="displayName.de-ch">Heimorganisation</prop>
            <prop key="displayName.fi">Kotiorganisaatio</prop>
            <prop key="displayName.fr">Organisme</prop>
            <prop key="displayName.it">Dominio dell'istituzione</prop>
            <prop key="description.en">The domain name of the subject's home organisation</pr
            <prop key="description.de">Domänenname der Heimatorganisation der Person</prop>
            <prop key="description.de-ch">Domainname der Heimorganisation der Person</prop>
            <prop key="description.fi">Henkilön kotiorganisaation domain-nimi</prop>
            <prop key="description.fr">Nom de domaine DNS de l'organisme d'origine d'une pers
            <prop key="description.it">Dominio dell'istituzione</prop>
        </props>
    </property>
</bean>
```

exportAttributes: Mapeamento automático do atributo

```
<DataConnector  id = "staticAttributes"  xsi:type = "Static"  exportAttributes = "o schacHomeOrganization ou eduPersonEntitlement" >

        <!-- The name of your institution is set statically here for all accounts. -->
        <Attribute id = "o" > <Value >Fundação para a Computação Científica Nacional</Value > </Attribute >

        <!-- The domain of your institution is set statically here and usually corresponds to the scope -->
        <Attribute id = "schacHomeOrganization" > <Value>%{idp.scope}</Value> </Attribute >

        <Attribute id = "ou" > <Value >FCCN, Serviços Digitais FCT </Value> </Attribute >

        <Attribute id = "eduPersonEntitlement">
                <Value>urn:mace:terena.org:tcs:escience-user</Value>
                <Value>urn:mace:terena.org:tcs:personal-user</Value>
                <Value>urn:mace:dir:entitlement:common-lib-terms</Value>
```

Shibboleth IdP – Configurações +Simples

- **Attribute Registry**

  - Caso o identificador do atributo não corresponda ao nome definido no esquema do registry, serão utilizadas as configurações personalizadas

/conf/atribute-resolver.xml

```
<AttributeDefinition id="eduPersonScopedAffiliation2" xsi:type="Scoped" scope="%{idp.scope}">
  <InputDataConnector ref="staticAttributes" attributeNames="eduPersonAffiliation2" />
</AttributeDefinition>
```

/conf/attributes/custom/custom.txt

```
id=eduPersonPrimaryAffiliation2
transcoder=SAML2ScopedStringTranscoder
saml2.name=urn:oid:1.3.6.1.4.1.5923.1.1.1.5

id=eduPersonAffiliation2
transcoder=SAML2ScopedStringTranscoder
saml2.name=urn:oid:1.3.6.1.4.1.5923.1.1.1.1


id=eduPersonScopedAffiliation2
transcoder=SAML2ScopedStringTranscoder
saml2.name=urn:oid:1.3.6.1.4.1.5923.1.1.1.9
```

Shibboleth IdP – Configurações +Simples

- **Metadata Providers**

- Consolidámos a configuração dos metadados, eliminando os ficheiros separados e centralizando tudo num único ficheiro (conf/metadata-providers.xml)

- **failFastInitialization=false**
Define se a inicialização do serviço MetadataResolverService deve falhar caso a inicialização de um provedor de metadados não seja bem-sucedida. Quando configurado como 'false', a IdP poderá iniciar e continuará tentando recarregar metadados válidos.

```
<MetadataProvider id="EngineRCTSaaiQUA" xsi:type="FileBackedHTTPMetadataProvider"
                  backingFile="%{idp.home}/metadata/metadata.rctsaai.qua.engine-key-20250210.xml"
                  metadataURL="https://engine.qua.rctsaai.pt/authentication/sp/metadata/key:20250210"
                  requireValidMetadata="true"
                  maxRefreshDelay="PT1H" failFastInitialization="false">

    <MetadataFilter xsi:type="SignatureValidation" certificateFile="%{idp.home}/credentials/engine-qua-rctsaai-key-20250210.pem" />
    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P7D"/>
    <MetadataFilter xsi:type="EntityRole">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>
 </MetadataProvider>
```

jornadas FCCN

RCTSaai Novos Identificadores

Integração e Fase de Transição

SAML Name IDs - Utilizados Atualmente na Federação

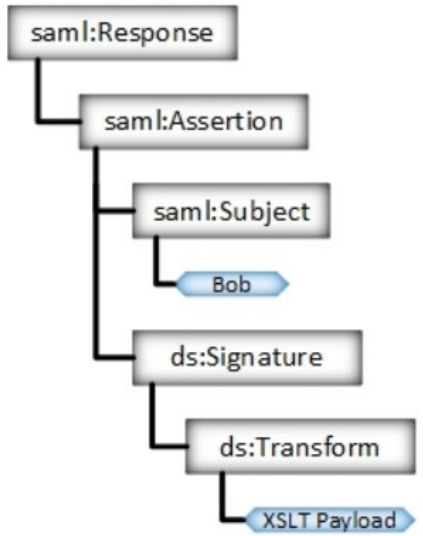
OLD

- **Transient SAML Name Identifier**
  urn:oasis:names:tc:SAML:2.0:nameid-format:transient

  ✓ Identificador **temporário**, **opaco** e único para um utilizador durante uma sessão SAML.
  ✓ Não permite identificar o utilizador em visitas posteriores.

Onde é utilizado ?

✓ Incluído no Saml:Response / Saml:Assertion enviada pelo Fornecedor de Identidade ao Serviço




```
<saml2:Subject>
    <saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                  NameQualifier="https://idp.fccn.pt/idp/shibboleth"
                  SPNameQualifier="https://engine.rctsaai.pt/authentication/sp/metadata"
                  >
                  AAdzZWNyZXQxN1NEqa+0U5wg8auFTnQFAP6fRy9W13lwlyyvcxp0jo/uqaFjaUcAd+xttdwKLruBElenZ6X0zluC4sRhT5UzyAFepVCYdnHhL3411
                  H1VCtYT2Cy7A7lftpKp9NZ9XKxjeR/g8qv9XYQltQKJ+VP0NhyRkKp6PNyQ</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData Address="172.16.10.31"
                                       InResponseTo="CORTO36cddf80a4aa01335dd601bfc3bb3748c32ecdaa"
                                       NotOnOrAfter="2025-05-02T08:50:09.166Z"
                                       Recipient="https://engine.rctsaai.pt/authentication/sp/consume-assertion"
                                       />
    </saml2:SubjectConfirmation>
</saml2:Subject>
```

SAML Name IDs - Utilizados Atualmente na Federação

- **Persistent SAML Name Identifier**
  urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

  ✓ Identificador **persistente**, **opaco** e único por serviço
  ✓ Evita correlação de dados entre serviços
  ✓ Pode ser usado sem outros atributos para proteger a identidade

Onde é utilizado ?

✓ Enviado através do atributo **eduPersonTargetID**

DEPRECATED

```
<saml2:Attribute FriendlyName="eduPersonTargetedID"
                 Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                 >
    <saml2:AttributeValue>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                      NameQualifier="https://idp.fccn.pt/idp/shibboleth"
                      SPNameQualifier="https://authmonit.fccn.pt"
                      >W4BZmK4ZpX4T0l+NgwS2swOkZNk=</saml2:NameID>
    </saml2:AttributeValue>
</saml2:Attribute>
```

SAML Name IDs - Utilizados Atualmente na Federação

- **eduPersonTargetID - Porque foi descontinuado ?**

  ✓ ***eduPersonTargetID*** *- "Case-sensitive vs case-insensitive string comparisons"*

  Atributo case-sensitive, diferentes implementação deste atributo e erros no seu armazenamento levam a dificuldades na correspondência correta dos valores/utilizadores.

  ✓ ***Necessidade de um identificador amplamente reconhecido*** *- "We need an identifier that is adopted across industries"*

  Um identificador que permita a correlação é fundamental numa transação SAML SSO, não apenas em contextos de colaboração académica ou científica.

- **Próximos Passos?**

  ✓ ***Transição para SAML Subject Identifiers (New Standart) – Definido num perfil oficial da norma SAML***

  samlPairwiseID e samlSubjectID

  https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.html

SAML Subject IDs – samlPairwiseID

NEW

- **pairwise-id**
  urn:oasis:names:tc:SAML:2.0:attribute:pairwise-id

  <Identificador Único> "@" <scope>

Vai substituir o *eduPersonTargetID* bem como o *SAML Persistent Name ID*

<Identificador Único> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")

✓ *Identificador Único pode ter entre 1 a 127 caracteres no total*
- *Caracteres Permitidos:*
  - *Alfanumérico ASCII:*
    - *Letras: A–Z, a–z*
    - *Dígitos: 0–9*
  - *O sinal de igual = (código ASCII 61)*
  - *O hífen - (código ASCII 45)*

O primeiro carácter DEVE ser alfanumérico.

```
<saml2:Attribute FriendlyName="samlPairwiseID"
                 Name="urn:oasis:names:tc:SAML:attribute:pairwise-id"
                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                 >
    <saml2:AttributeValue>LOAFTGFODGSX4E6SL6GYGBFWWMB2IZGZ@fccn.pt</saml2:AttributeValue>
</saml2:Attribute>
```

Encode BASE 32 *Scoped*

<scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")

SAML Subject IDs – samlSubjectID

NEW

- **subject-id**
  urn:oasis:names:tc:SAML:2.0:attribute:subject-id

  <Identificador Único> "@" <scope>

Destina-se a substituir o atributo *eduPersonUniqueID* e possivelmente o próprio *eduPersonPrincipalName*

<Identificador Único> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")

- ✓ *Identificador Único pode ter entre 1 a 127 caracteres no total*
  - *Caracteres Permitidos:*
    - *Alfanumérico ASCII:*
      - *Letras: A–Z, a–z*
      - *Dígitos: 0–9*
    - *O sinal de igual = (código ASCII 61)*
    - *O hífen - (código ASCII 45)*

  O primeiro carácter DEVE ser alfanumérico.

```
<saml2:Attribute FriendlyName="samlSubjectID"
                 Name="urn:oasis:names:tc:SAML:attribute:subject-id"
                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                 >
    <saml2:AttributeValue>epires@fccn.pt</saml2:AttributeValue>
</saml2:Attribute>
```

<scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")

SAML Subject IDs – samlSubjectID

- **subject-id**
  urn:oasis:names:tc:SAML:2.0:attribute:subject-id

  <Identificador Único> "@" <scope>

```
<!-- Novos Identificadores - samlSubjectID  -->
<AttributeDefinition id="samlSubjectID" xsi:type="Scoped" scope="%{idp.scope}">
     <InputAttributeDefinition ref="uid" />
</AttributeDefinition>
```

Este atributo pode ser definido com base no *uid ou sAMAccountName,* desde que respeite as regras de sintaxe definidas, bem como as regras da federação RCTSaai referentes aos Identificadores.

Exemplos valores válidos:

- *johndoe@fccn.pt*
- *john-doe@fccn.pt*
- *jonhdoe53@fccn.pt*

Exemplos de valores inválidos:

- *john.doe@fccn.pt (uso de . não é permitido no Id. Único)*
- *john_doe@fccn.pt (uso de _ não é permitido no Id. Único)*
- *53johndoe@fccn.pt (início com número não permitido)*

SAML Subject Ids – Perfis de Confiabilidade

= P0 P1 P2 P3

- Cada utilizador tem de ter um identificador único
- O identificador tem de representar uma pessoa física afiliada à organização
- A organização tem de ser capaz de entrar em contacto com a pessoa.
- O identificador atribuído nunca é reatribuído.

O identificador transmitido pelo Fornecedor de Identidade deve ser pelo menos um dos seguintes:

- SAML 2.0 persistent Name Identifier [OASIS SAML]
- SAML 2.0 subject-id ou pairwise-id [OASIS SIA]
- OIDC sub ou pairwise [OpenID.Core]
- eduPersonUniqueId [eduPerson]
- eduPersonPrincipalName [eduPerson]

<u>Caso estas regras não estejam a ser seguidas, agora é o momento ideal para corrigir e alterar!</u>

SAML Subject IDs – Integração e Fase de Transição

- *Adicionar os novos Identificadores*

```
<!-- ========================================== -->
<!--       Novos Identificadores                -->
<!--    samlSubjectID e samlPairwiseID          -->
<!-- ========================================== -->
<DataConnector id="StoredId"
    xsi:type="StoredId"
    generatedAttributeID="persistentID"
    salt="%{idp.persistentId.salt}"
    encoding="BASE32"
    queryTimeout="0">
    <InputAttributeDefinition ref="%{idp.persistentId.sourceAttribute}" />
    <BeanManagedConnection>shibboleth.PostgreSQLDataSource</BeanManagedConnection>
</DataConnector>

<!-- Novos Identificadores - samlPairwiseID  -->
<AttributeDefinition id="samlPairwiseID" xsi:type="Scoped" scope="%{idp.scope}">
   <InputDataConnector ref="StoredId" attributeNames="persistentID" />
</AttributeDefinition>


<!-- Novos Identificadores - samlSubjectID  -->
<AttributeDefinition id="samlSubjectID" xsi:type="Scoped" scope="%{idp.scope}">
     <InputAttributeDefinition ref="uid" />
</AttributeDefinition>
```

SAML Subject IDs – Integração e Fase de Transição

- **Temporariamente continuar a definir o eduPersonTargetID**
  - Serviços que permitam o mapeamento eduPersonTargetID / samlPairwaiseID – Enviar ambos os atributos

```
<!-- ========================================== -->
<!--      Identificadores Antigos               -->
<!-- ========================================== -->
<DataConnector id="ComputedIDConnector" xsi:type="ComputedId" generatedAttributeID="ComputedId" salt="%{idp.persistentId.salt}" >
     <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}" />
</DataConnector>

 <!-- Targeted ID/Persistent ID  - Descontinuado  manter apenas em fase de transição  -->
 <AttributeDefinition id="eduPersonTargetedID" xsi:type="SAML2NameID" nameIdFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
 <InputDataConnector ref="ComputedIDConnector" attributeNames="ComputedId" />
     <DisplayName xml:lang="en">Targeted ID</DisplayName>
     <DisplayName xml:lang="de">Targeted ID</DisplayName>
     <DisplayName xml:lang="fr">Targeted ID</DisplayName>
     <DisplayName xml:lang="it">Targeted ID</DisplayName>

     <DisplayDescription xml:lang="en">Targeted ID: A unique identifier for a person, different for each service provider.</DisplayDescription>
     <DisplayDescription xml:lang="de">Targeted ID: Eindeutige Benützeridentifikation, unterschiedlich pro Service Provider.</DisplayDescription>
     <DisplayDescription xml:lang="fr">Targeted ID: Un identifiant unique de l'utilisateur, différent pour chaque fournisseur de service.</DisplayDescription>
     <DisplayDescription xml:lang="it">Targeted ID: identificativo unico della persona, differente per ogni fornitore di servizio.</DisplayDescription>
     <AttributeEncoder xsi:type="SAML1XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" encodeType="false" />
     <AttributeEncoder xsi:type="SAML2XMLObject" name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" friendlyName="eduPersonTargetedID" encodeType="false" />
 </AttributeDefinition>
```

SAML Subject IDs – Integração e Fase de Transição

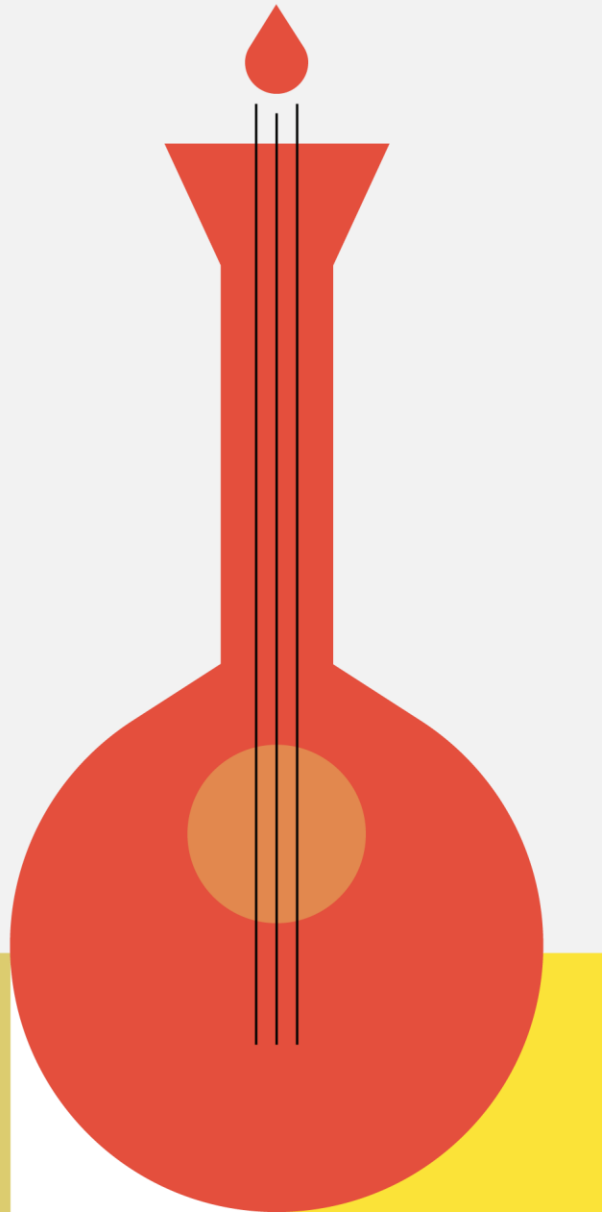
- Adotar novo filtro para a categoria https://refeds.org/category/code-of-conduct/v2"

```
<!-- ================================================================================================================== -->
<!--  GÉANT EU/EEA Data Protection Code of Conduct for Service Providers                                                 -->
<!--  https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home                                          -->
<!--  Envio automatico de um conjunto de atributos para os servicos marcados na                                         -->
<!--  metadatada data-protection-Code-of-Conduct                                                                        -->
<!-- ================================================================================================================== -->
<AttributeFilterPolicy  id = "releaseSubjectId2coco" >
  <PolicyRequirementRule  xsi:type = "AND" >
            <Rule  xsi:type = "EntityAttributeExactMatch"
                    attributeName = "urn:oasis:names:tc:SAML:profiles:subject-id:req" attributeValue = "subject-id" />
            <Rule xsi:type = "EntityAttributeExactMatch" attributeName = "http://macedir.org/entity-category"
                   attributeValue = "https://refeds.org/category/code-of-conduct/v2" />
   </PolicyRequirementRule >
   <AttributeRule attributeID = "samlSubjectID" permitAny = "true" />
</AttributeFilterPolicy >

<AttributeFilterPolicy  id = "releasePairwiseId2coco" >
   <PolicyRequirementRule  xsi:type = "AND" >
            <Rule  xsi:type = "OR" >
                  <Rule  xsi:type = "EntityAttributeExactMatch"
                     attributeName = "urn:oasis:names:tc:SAML:profiles:subject-id:req"
                     attributeValue = "pairwise-id" />
                  <Rule xsi:type = "EntityAttributeExactMatch" attributeName = "urn:oasis:names:tc:SAML:profiles:subject-id:req"
                     attributeValue = "any" />
            </Rule>
            <Rule xsi:type = "EntityAttributeExactMatch" attributeName = "http://macedir.org/entity-category"
                  attributeValue = "https://refeds.org/category/code-of-conduct/v2" />
    </PolicyRequirementRule >
    <AttributeRule attributeID = "samlPairwiseID" permitAny = "true" />
</AttributeFilterPolicy >

<AttributeFilterPolicy id="GeantEEADataProtectionCodeOfConduct">
```

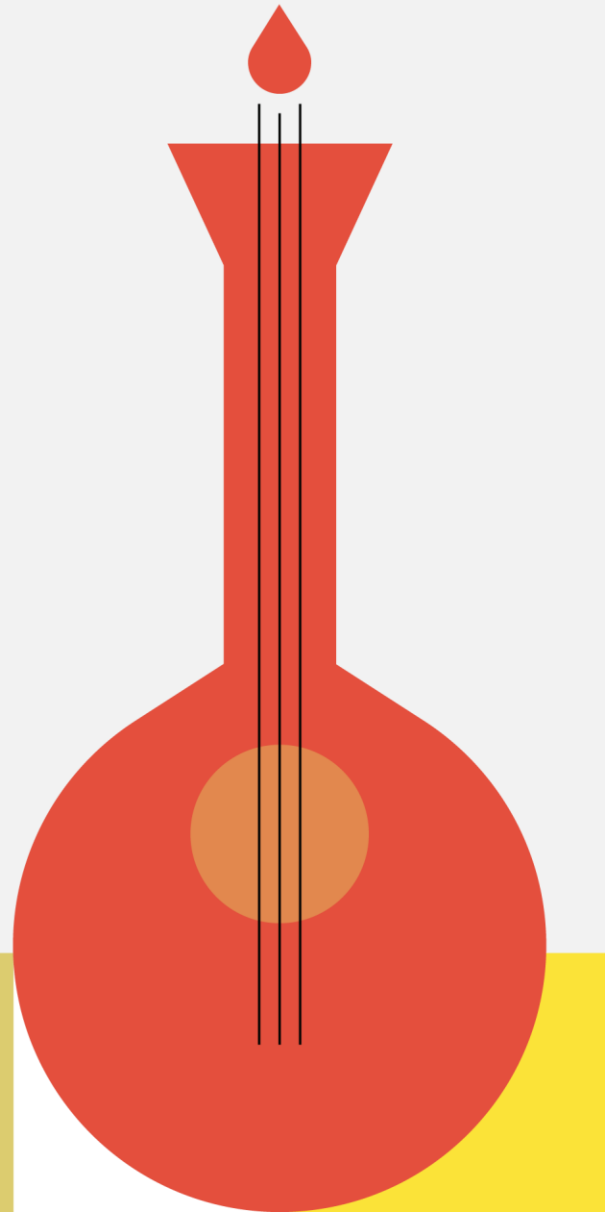
jornadas FCCN



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

jornadas FCCN

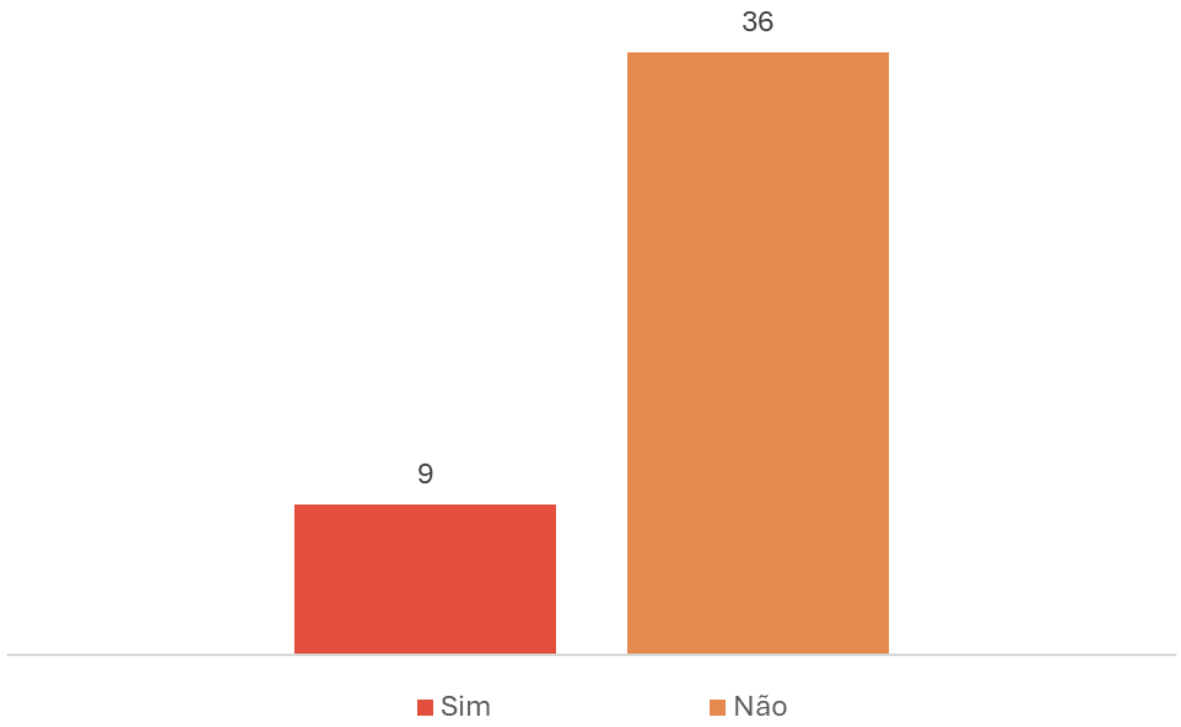
OpenID Connect



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

Em 2024

Sabiam que podem integrar serviços que apenas falam OpenID Connect dentro da Federação RCTSaai?



Protocolos SSO

Característica	SAML	OIDC
Formato	XML	JSON
Base	Proprietária	OAuth 2.0
Usabilidade	Web	Mobile/API
Complexidade	Mais complexo	Mais simples
Suporte	Menor em apps novas	Amplo suporte atual

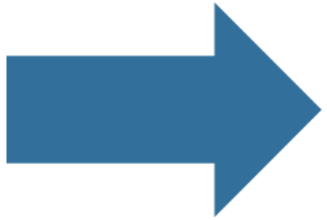
Benefícios de OIDC

- **Existem mais implementações disponíveis** e para mais linguagens de programação do que SAML
- **A configuração técnica é mais direta**
- Orientado para **apps mobile e APIs**
- **Maior facilidade de troubleshooting** devido ao formato ser em json e gerar menos logs

Serviços - OpenID Connect

RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

75 Serviços



61 SAML

SAML

14 OIDC

OpenID

Exemplos: CIÊNCIA ID, *share.fccn.pt*, Grafana, etc.

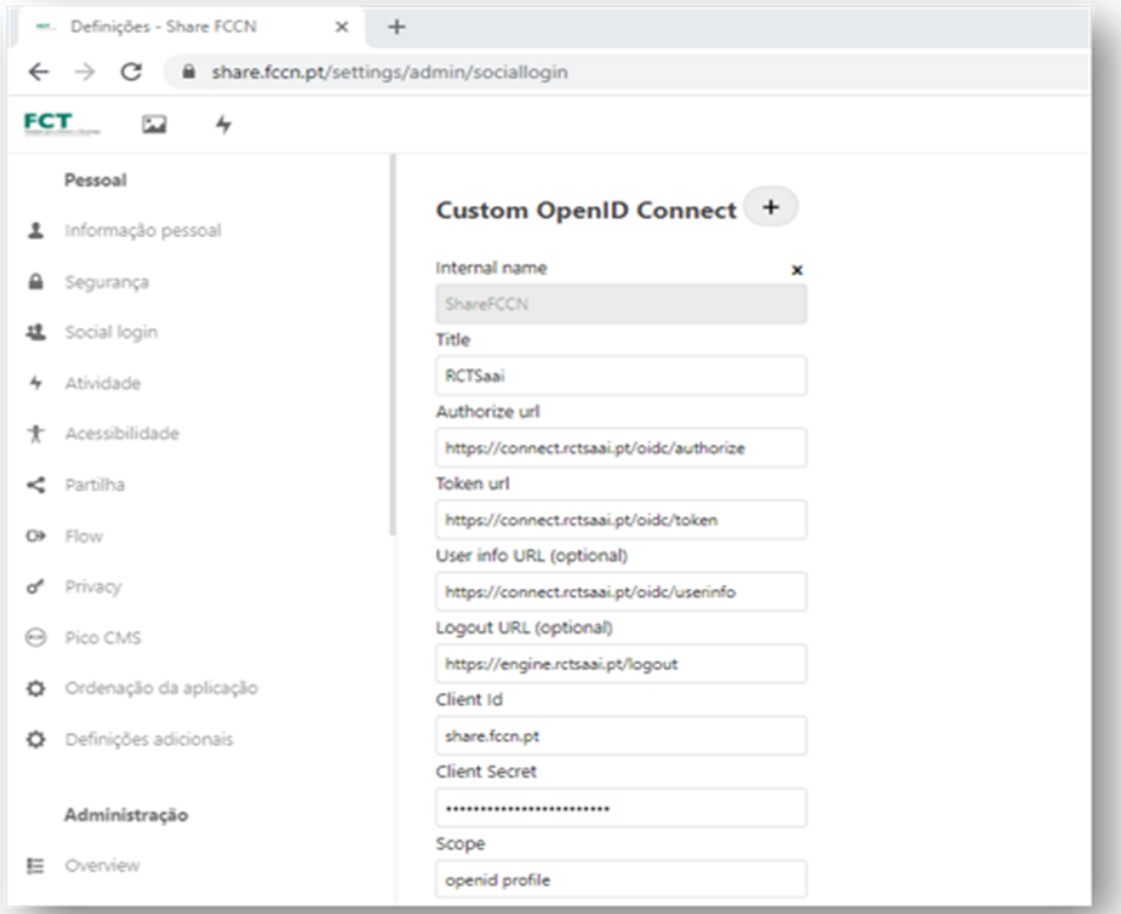
Serviços com OIDC - Exemplos

- Grafana
- Kibana / Elasticsearch
- Jenkins / GitLab / GitHub Enterprise
- Nextcloud / OwnCloud
- Zabbix / Prometheus

Configuração OIDC

share.fccn.pt

oidc.rctsaai.pt

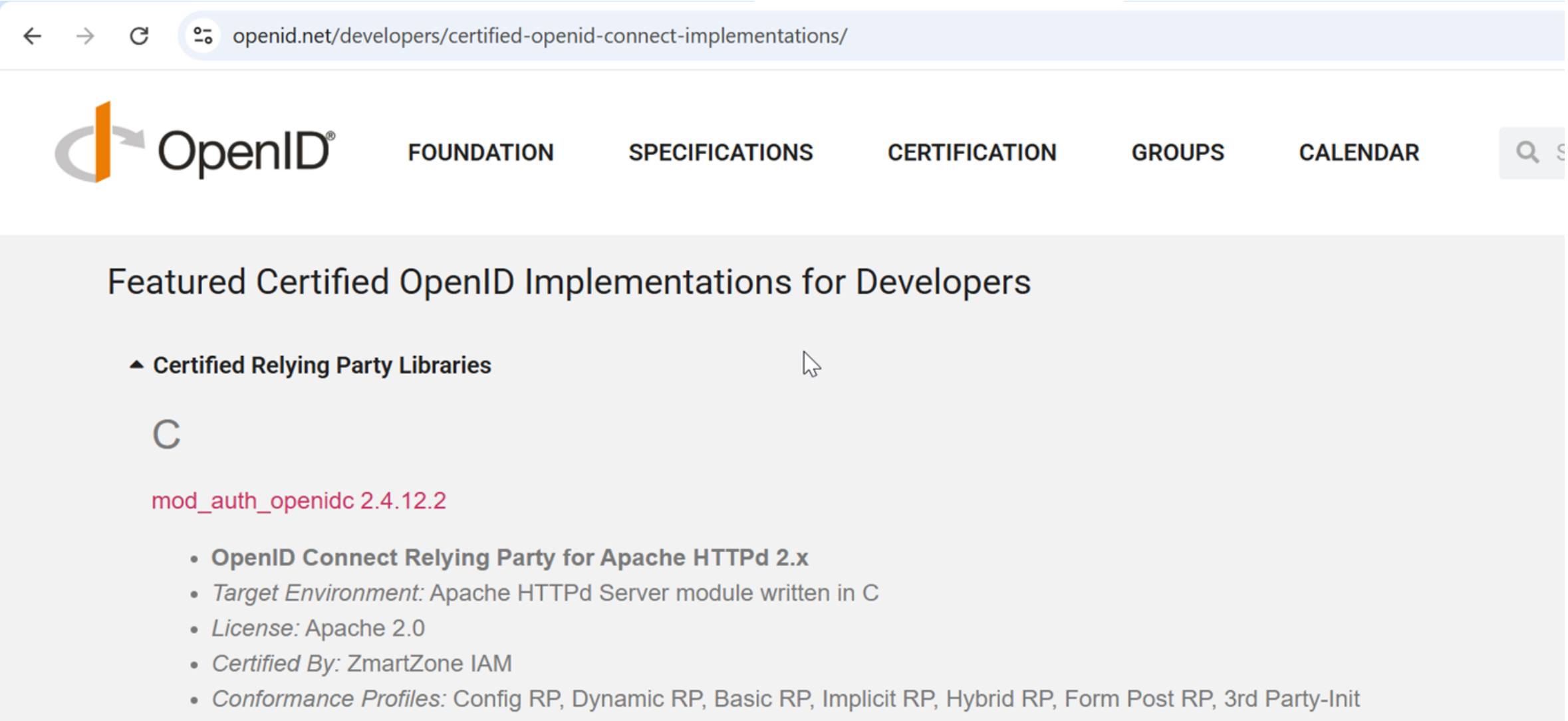


Tipos de *Grants*

Site: https://connect.rctsaai.pt/.well-known/openid-configuration

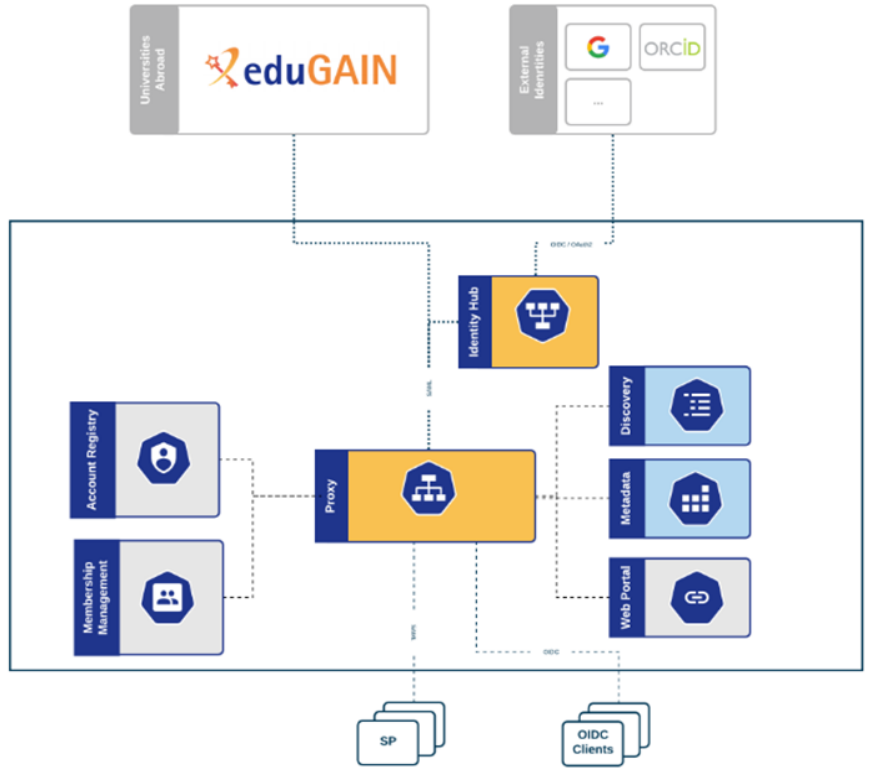
- authorization_code
- implicit (legacy)
- refresh_token
- client_credentials
- device_code

Bibliotecas suportadas por OIDC



GÉANT AAI Service

- Única forma de ligar serviços via OIDC **eduGAIN**
- Serviço fornecido pela GÉANT



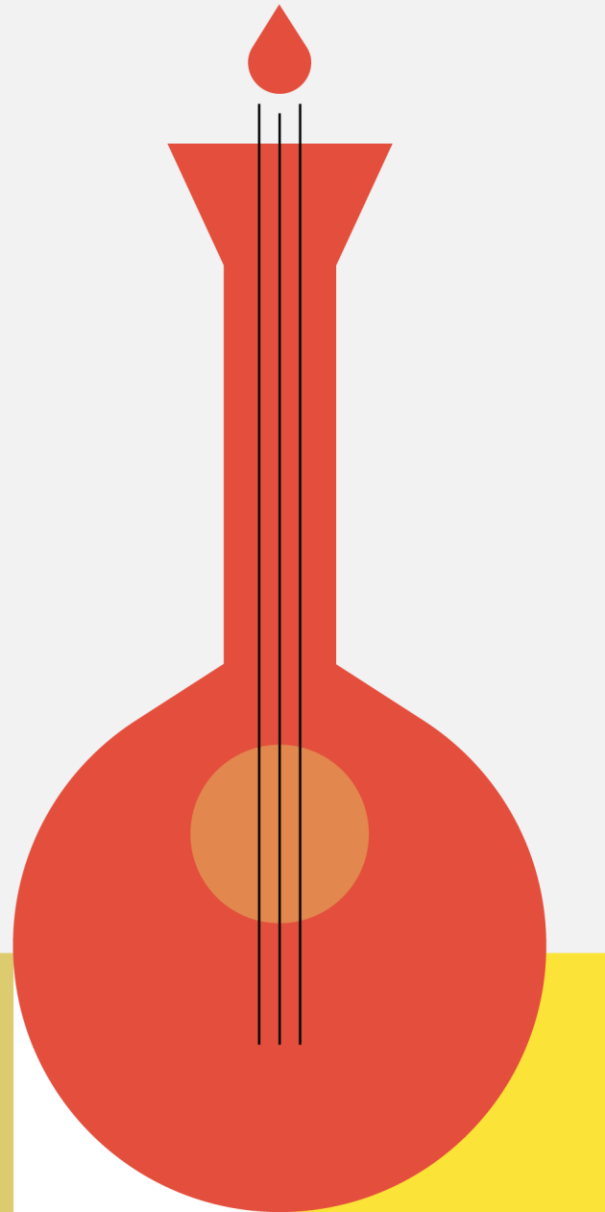
Fonte: https://wiki.geant.org/display/GSPP/GEANT+AAI+Service

jornadas FCCN

Protocolos de Autenticação

SAML

OAuth 2.0 e OpenID Connect



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

SAML – Limitações

- **SAML é um protocolo *legacy***
- **Funcionalidades que nunca serão suportadas no SAML:**
  - Aplicações *Mobile*
  - Autenticações baseadas em REST – APIs
  - FedCM (*Federated Credential Manager*)
  - *Verifiable Credentials* (*Wallets*)
  - Criptografia *pós-quantum*

OAuth2 e OpenID Connect

O framework de autorização OAuth 2.0 permite que uma aplicação de terceiros obtenha acesso limitado a um serviço HTTP em nome de um proprietário de recursos [RFC 6749].

OpenID Connect 1.0 é uma camada de identidade simples sobre o protocolo OAuth 2.0. Permite que os Clientes verifiquem a identidade do Utilizador Final de uma maneira interoperável e semelhante ao REST [openid-connect-core-1_0].

OAuth2 e OpenID Connect - Vantagens

jornadas FCCN

- São o *standard* actual da indústria para **Autorização** e **Autenticação**
- Suportam aplicações ***Mobile*** e **APIs** *(REST-like)*
- São desenvolvidos de forma activa pela comunidade
- Suporte para ***Decentralized Identifiers*** *(DIDs)* e ***Verifiable Credentials***

jornadas FCCN

Estado da Arte e Projectos Piloto

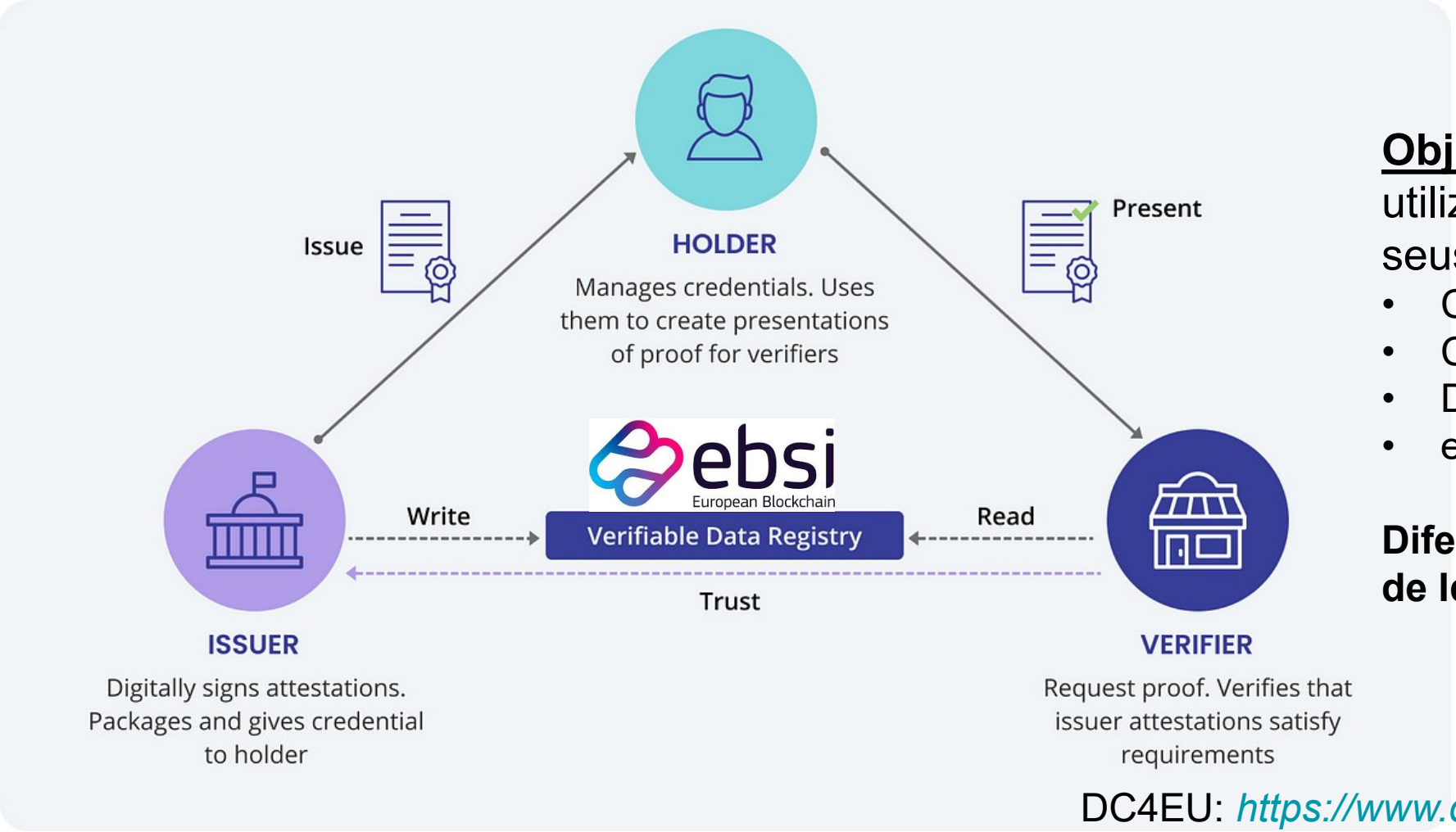
Verifiable Credentials

Digital Credentials for Europe (DC4EU) – **Wallet de referência EU** (EUDI Wallet)

OpenID Federation

eduGAIN OpenID Federation Pilot

Verifiable Credentials + Wallets



Objectivo: Colocar os utilizadores em controlo dos seus dados:

- Cartões nacionais
- Carta de condução
- Diplomas académicos
- etc.

Difere do habitual ambiente de Identidade Federada

DC4EU: *https://www.dc4eu.eu/project/wp6/*

OpenID for Verifiable Credentials: *https://openid.net/sg/openid4vc/*

Federação OpenID – OID Fed
O que é?

jornadas FCCN

- Uma **especificação técnica** *da OpenID Foundation* que define de forma abrangente*:*
  - **Como avaliar a Confiança** – de uma perspectiva técnica
  - Como construir **infraestruturas de confiança**
  - Como **estabelecer de forma segura a interoperabilidade** dos participantes

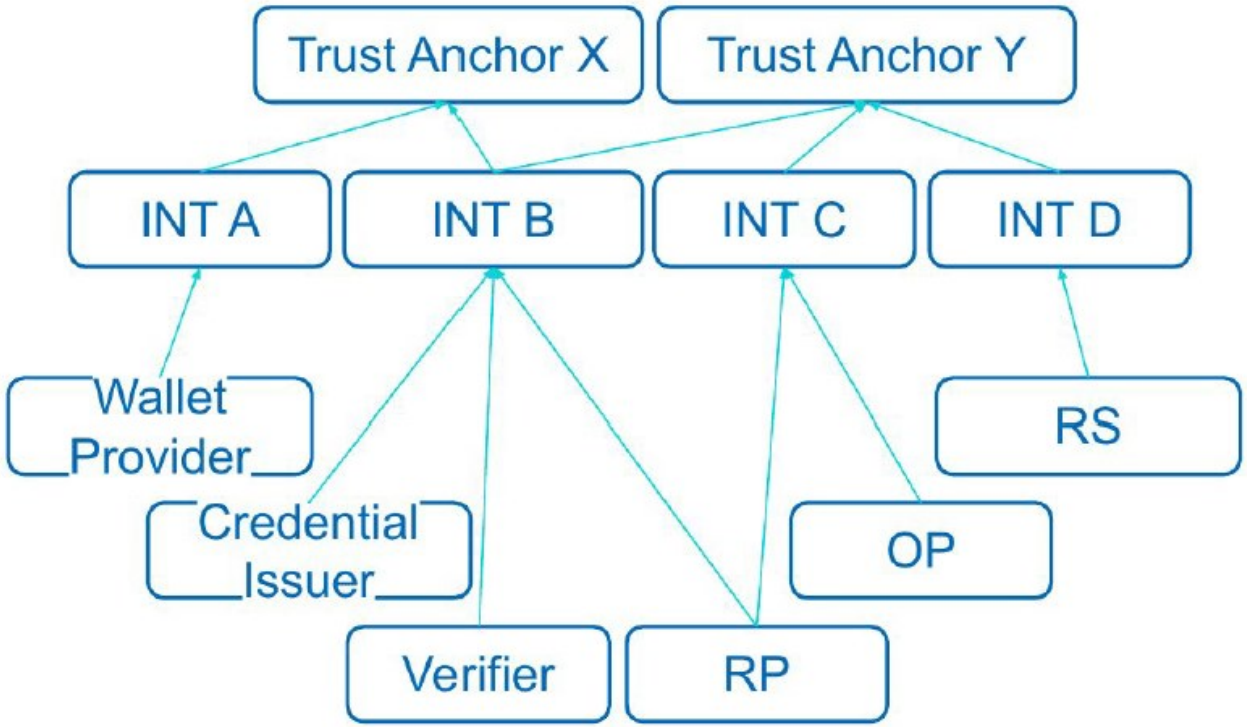
https://openid.net/specs/openid-federation-1_0.html

OpenID

Federação OpenID – Infraestrutura

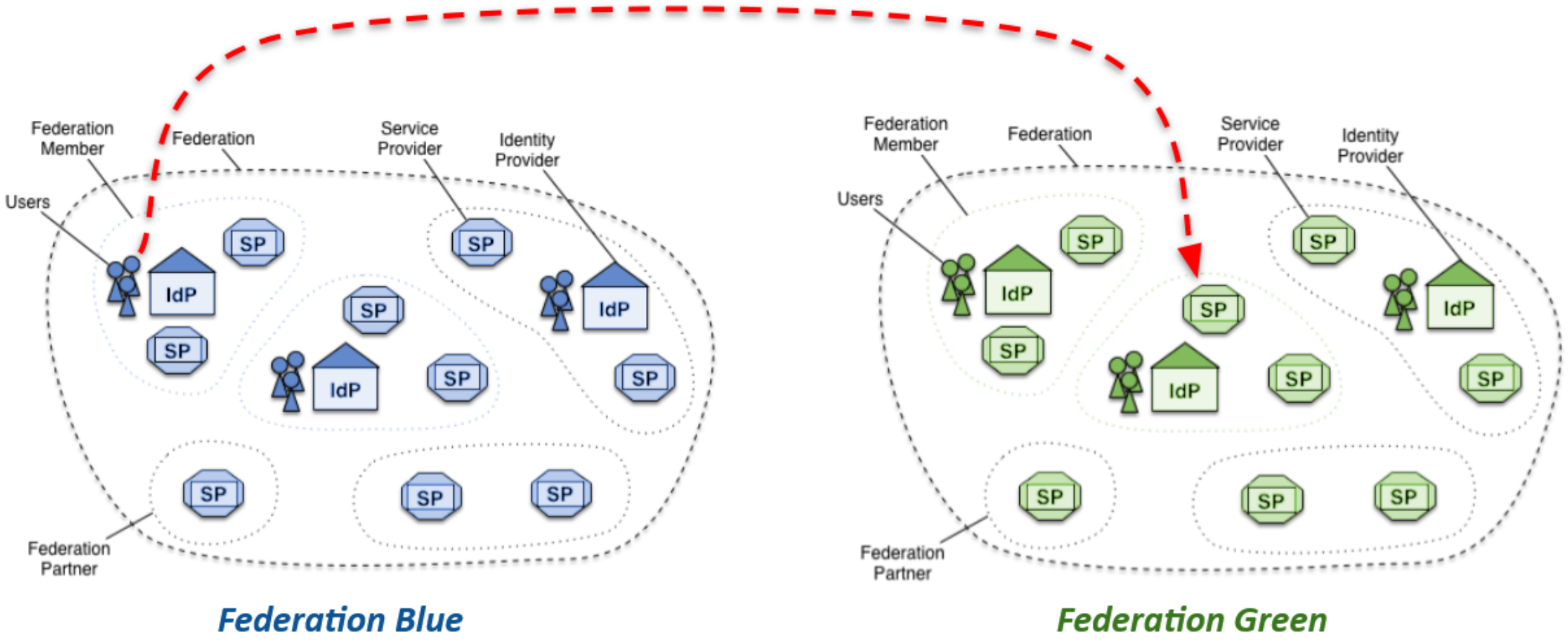
Infraestrutura de confiança que escala de forma:

- **Distribuída** por múltiplos participantes
- **Hierárquica**
- **Descentralizada**
  - Autoridade da Federação tem Intermediários
  - Participantes podem juntar-se a múltiplas federações sem alterações de configuração



OpenID

eduGAIN

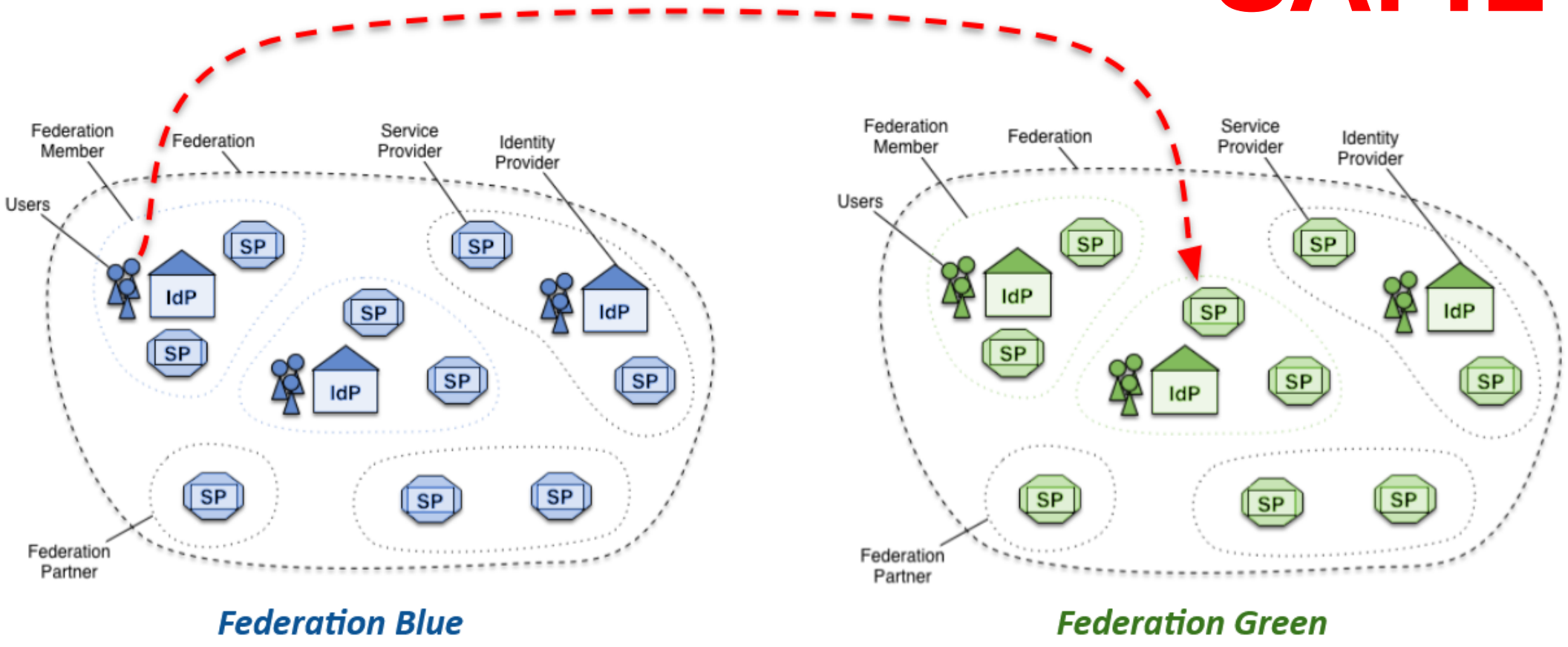


Fonte: *eduGAIN OpenID Fedederation Pilot - FIM4R*

jornadas FCCN

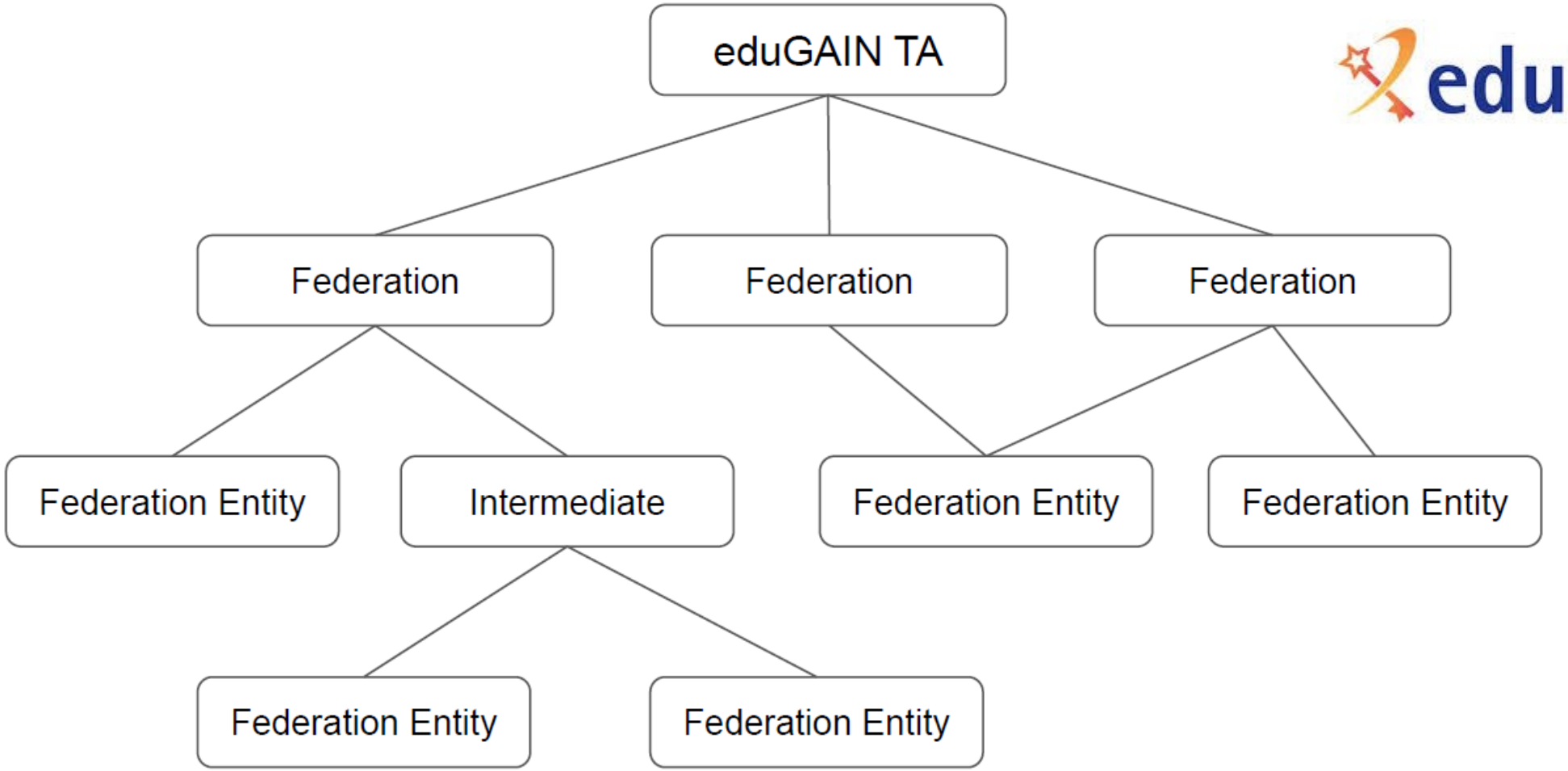
eduGAIN

SAML



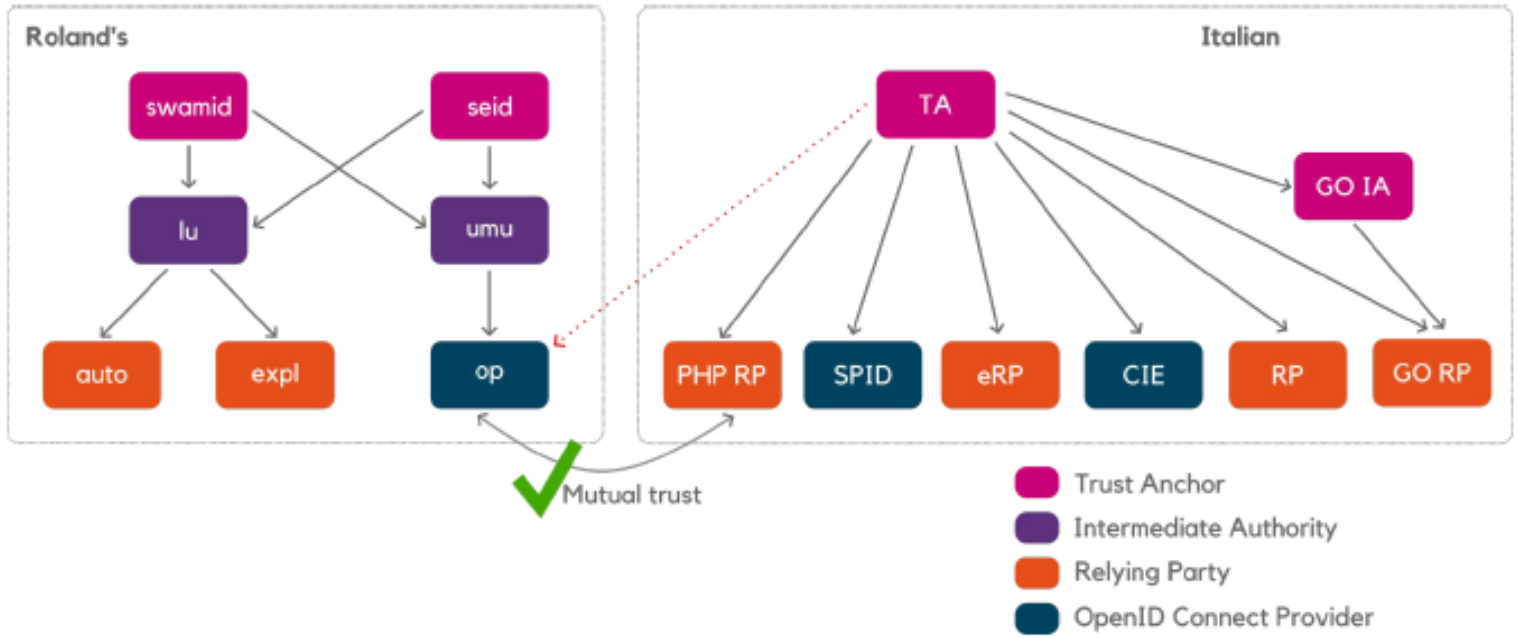
Fonte: *eduGAIN OpenID Fedederation Pilot - FIM4R*

Federação eduGAIN OpenID – Piloto



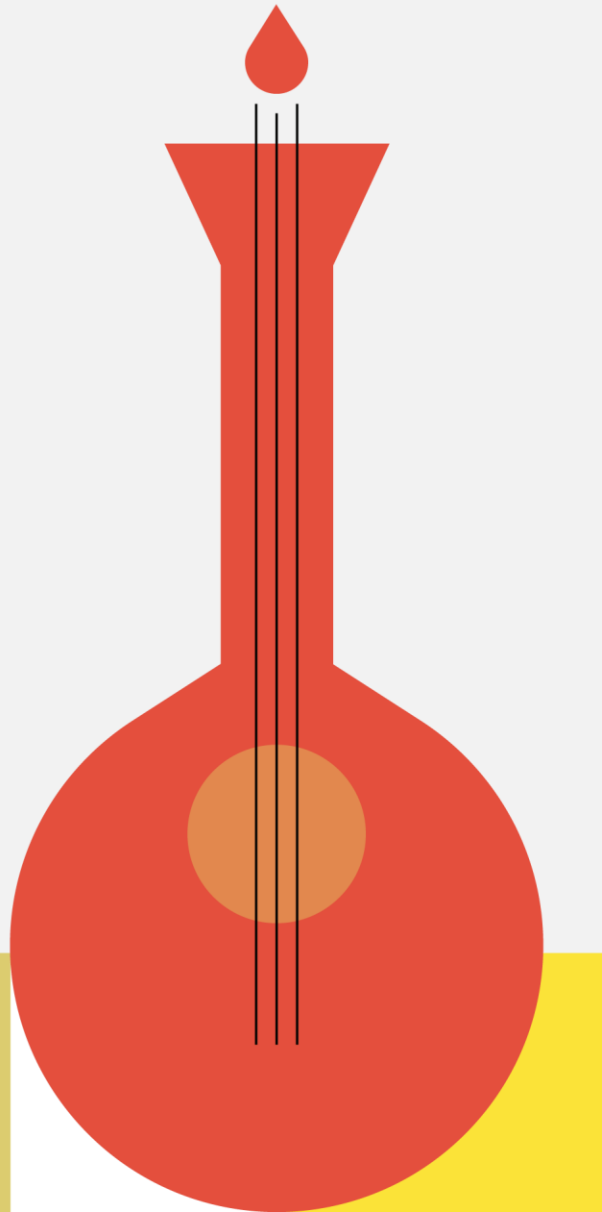
Federação eduGAIN OpenID – Piloto

- **Projecto GEANT GN5-1 WP5**
- Implementações OpenID Federation
  - IDPs Shibboleth
  - SimpleSAMLphp



https://wiki.geant.org/display/GWP5/OIDCfed+support+on+SimpleSAMLphp
https://wiki.geant.org/x/ZIEDLQ

jornadas FCCN

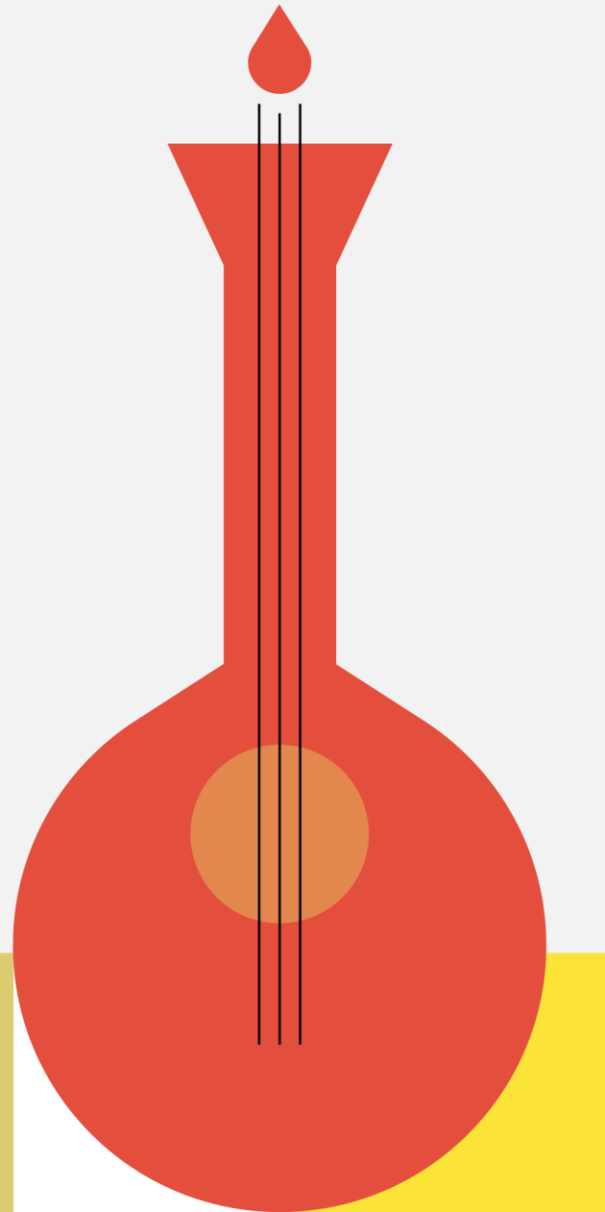


FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

IPLNet

IdP

Desafios de confiabilidade e novos requisitos de cibersegurança

Vasco Mendonça – DSIC/IPLNet
vmendonca@net.ipl.pt

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

IdP

Tecnologia

- SimpleSAMLphp

Motivação para métodos complementares de verificação de identidade:

- Segurança, conseguir identificar e garantir acessos legítimos;
- NIS2 e os seus requisitos;
- Perfis de confiabilidade, como já apresentados pela RCTSaai.

NIS2

- NIS2[1] Artigo 27.º, Medidas de cibersegurança, ponto i)

« i) Utilização de autenticação multifator ou de autenticação contínua, comunicações seguras e sistemas seguros de comunicações de emergência no seio da entidade. »

Sendo uma autenticação contínua um método que analisa o comportamento do utilizador ao longo do tempo, contemplando assim o seu comportamento nos momentos de autenticação.

[1] Baseado na ultima versão conhecida colocada em consulta pública.

Métodos complementares de verificação da identidade

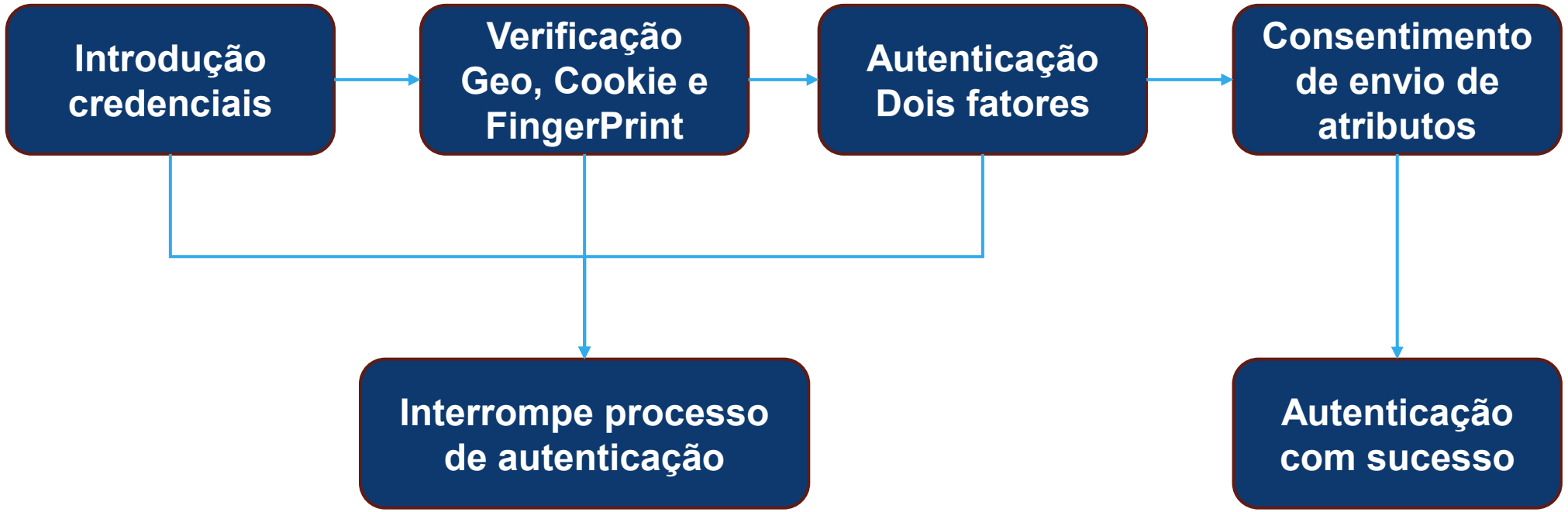
- Como complemento às credenciais (utilizador e palavra-chave), implementámos:
  - Verificação por Geo-Localização.
  - Verificação por Cookie persistente.
  - Impressão digital com dados obtidos na interação com o utilizador.

  Vertente contínua
  - Autenticação de dois fatores, atualmente composto por 5 métodos configuráveis pelos utilizadores.

  Vertente multifator

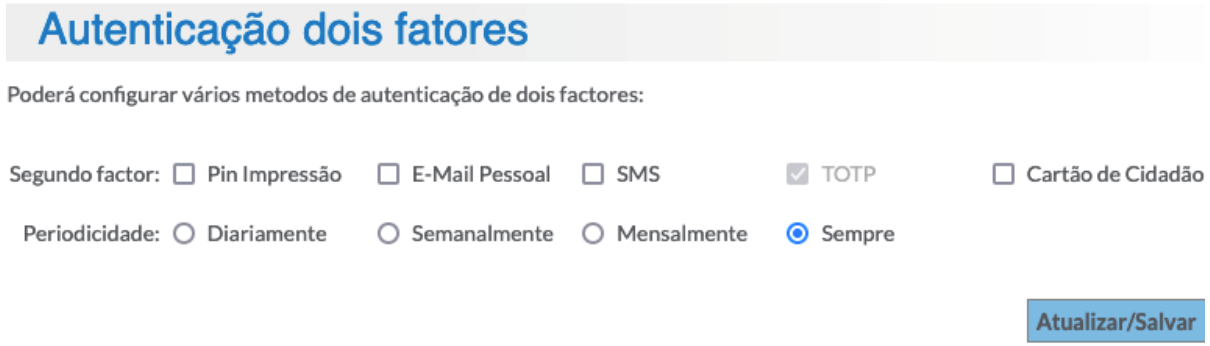
Autenticação de dois fatores

- Como entra no fluxo de autenticação?
  - No simpleSAMLphp entra como "***Authentication Processing Filters***"



Autenticação de dois fatores

- O que implicou o desenvolvimento:
  - Interface externa para configuração dos métodos 2FA;



  - Adaptadores/conectores para os métodos 2FA;
  - *Authentication Processing Filter* em SimpleSAMLphp:
    - Composto por: *Class Auth/Process, Class Controller* e *Template twig* formulário.

Métodos 2FA

- Métodos disponíveis:
  - PIN (como se fosse uma segunda palavra-chave);
    - 9 caracteres, usado na impressão interna, fraco mas transitório
  - Código temporário E-Mail;
  - Código temporário SMS (AMA GAP);
  - TOTP (software);
  - Cartão de cidadão ou chave-móvel digital (OAuth2).

Atributo *eduPersonAssurance*

- Com o autenticação de dois fatores é um dos elementos necessário para se poder aplicar os perfis de confiabilidade:
  - https://rctsfederation.fccn.pt/policy/assurance/RCTS-P2
    - O controlo e verificação da identidade, TEM DE ser efetuada, podendo ser pessoal, remota ou com credenciais de outros serviços. [1]
  - https://rctsfederation.fccn.pt/policy/assurance/RCTS-P3
    - O controlo e verificação da identidade, TEM DE implementar um sistema de verificação de identidade de acordo com o Regulamento eIDAS [eIDAS] para nível de confiança Elevado. [1]

Fontes:

[1] - https://share.fccn.pt/sites/rctsaai/areatecnica/assurance/Perfis/

[2] - https://refeds.org/assurance

A seguir …

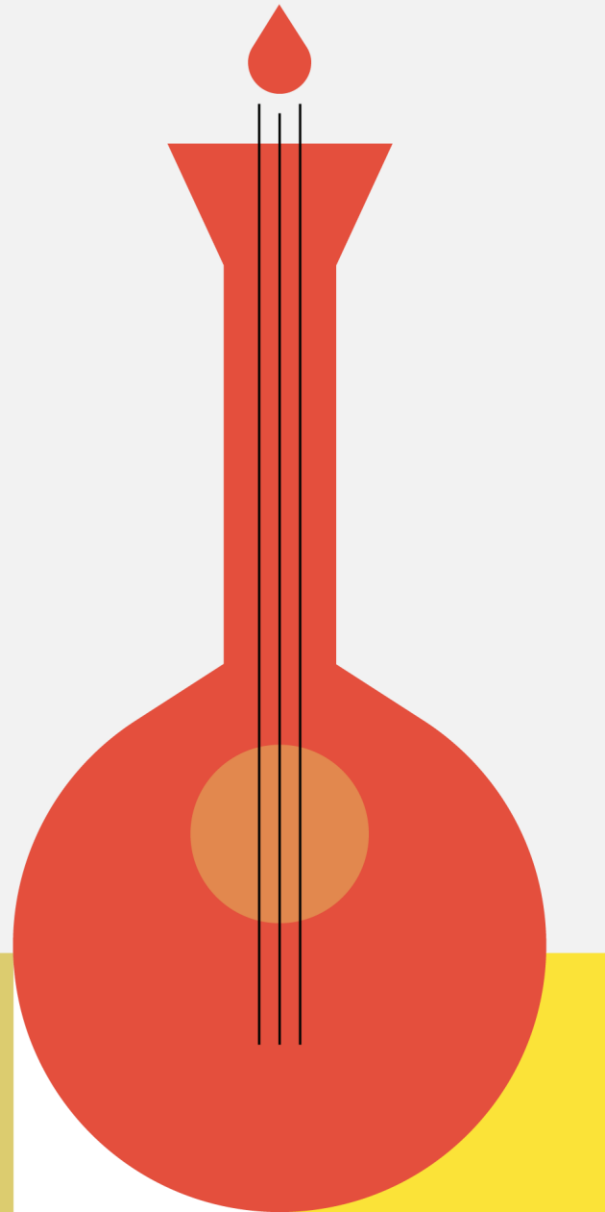
- Implementação do login pelo cartão de cidadão;
- Explorar outros métodos de 2FA, como hardware TOTP;
- Permitir ao utilizadores criar palavras-chaves para serviços específicos;
- Promoção da ativação e uso de 2FA
  - Durante autenticações anteriores.
- Evolução dos atributos *PersonalAssurance*

jornadas FCCN

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

Obrigado!

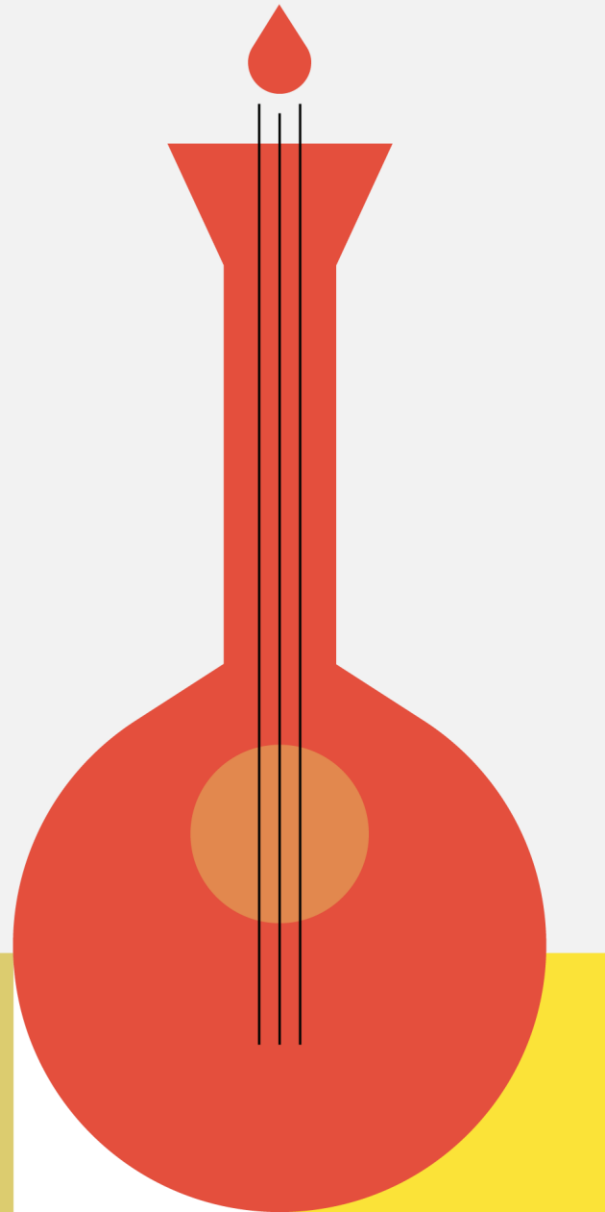
jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL DE COIMBRA

jornadas FCCN

RCTSaai INVITE



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

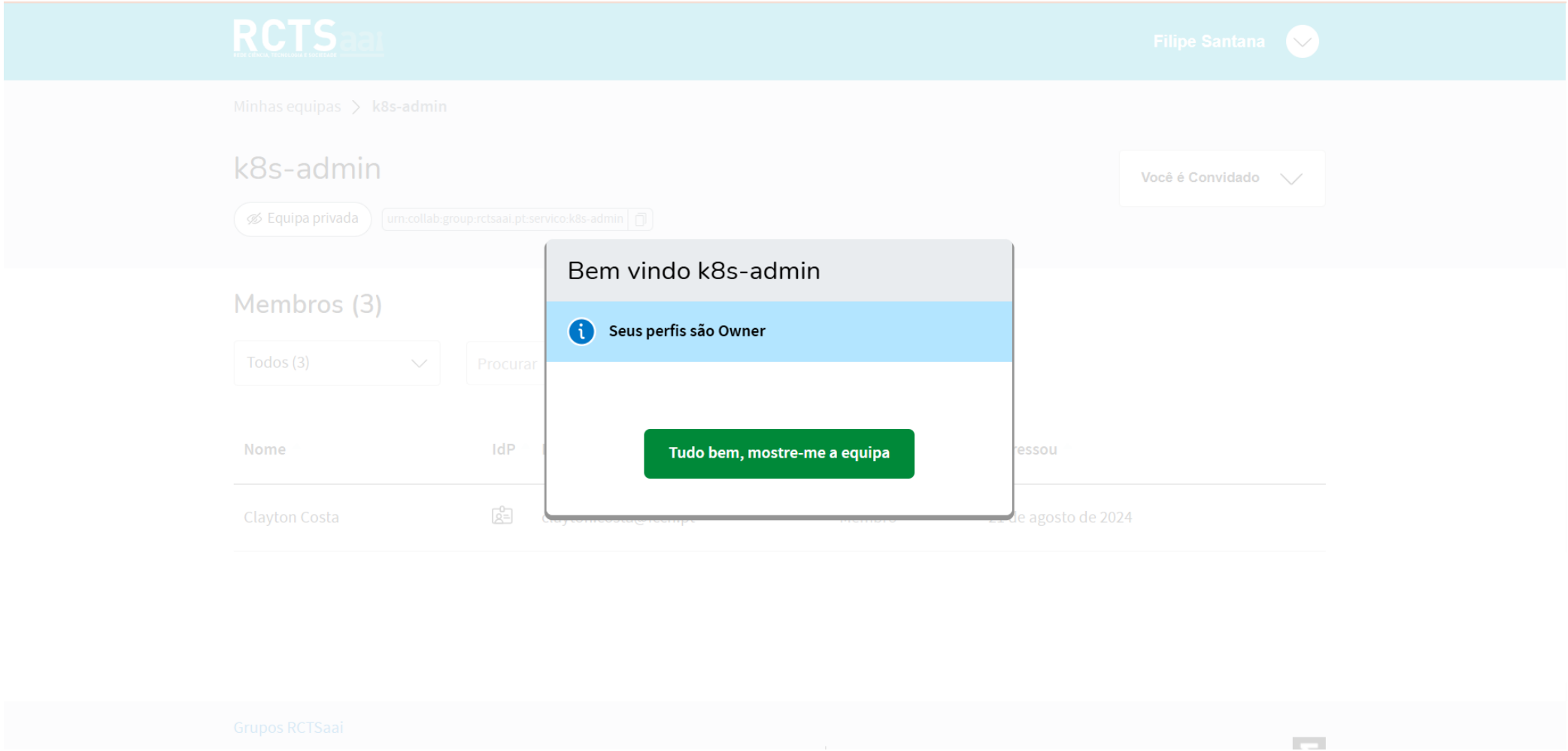
Introdução

O processo de login federado, já está relativamente maduro.

O grande desafio agora está na gestão de acessos.

Muitas vezes, o usuário é convidado para utilizar uma aplicação ou sistema, mas não sabe para onde ir em seguida.

Exemplo do atual Teams



Além disso

- Muitos acessos são concedidos manualmente e de forma desorganizada.
- Em muitos casos não há prazos definidos, o que significa que muitos utilizadores mantêm acessos que não deveriam mais ter.
- Há também múltiplos pontos de controle espalhados pela instituição, dificultando a visão geral e aumentando os riscos.

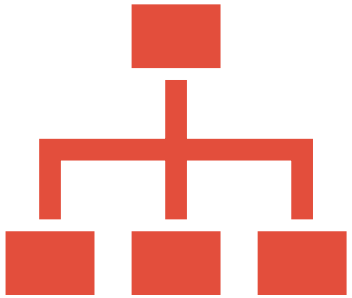
RCTSaai INVITE

Foram desenvolvidas duas versões de uma aplicação

- **Invite**: Interface para criação de perfis e realizar novos convites
- **Invite-Welcome**: Interface para o utilizador aceitar e visualizar as aplicações que tem permissão de acesso

RCTSaai INVITE

Com o RCTSaai Invite, sua instituição pode gerenciar com facilidade e segurança os direitos de acesso de grupos de **perfis** para aplicativos e sistemas.



Para gerenciar adequadamente os perfis em sua instituição, o invite tem uma estrutura de *gerenciamento de acesso* que consiste em uma série de **membros**.

Características do acesso ao Invite

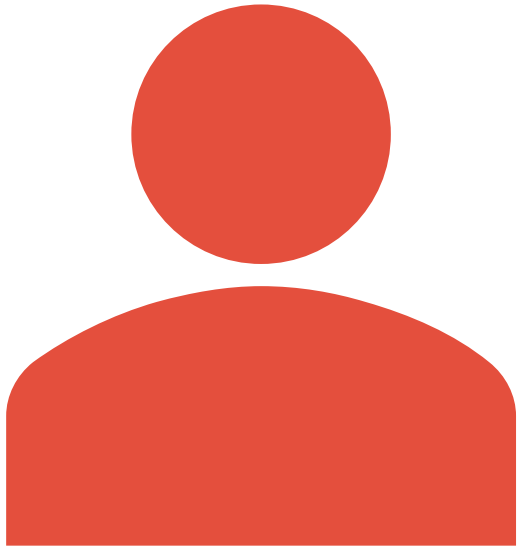
Administrador da instituição: cria perfis e atribui gestores à estes perfis.

Gestor: nomeia os gestor de convite.

Gestor de Convite: Quem dentro da sua instituição deve conceder acesso aos usuários para aplicações e sistemas

Utilizador: Alunos de outras instituições, professores convidados temporários ou ex-alunos. (Acesso apenas ao Invite-Welcome)

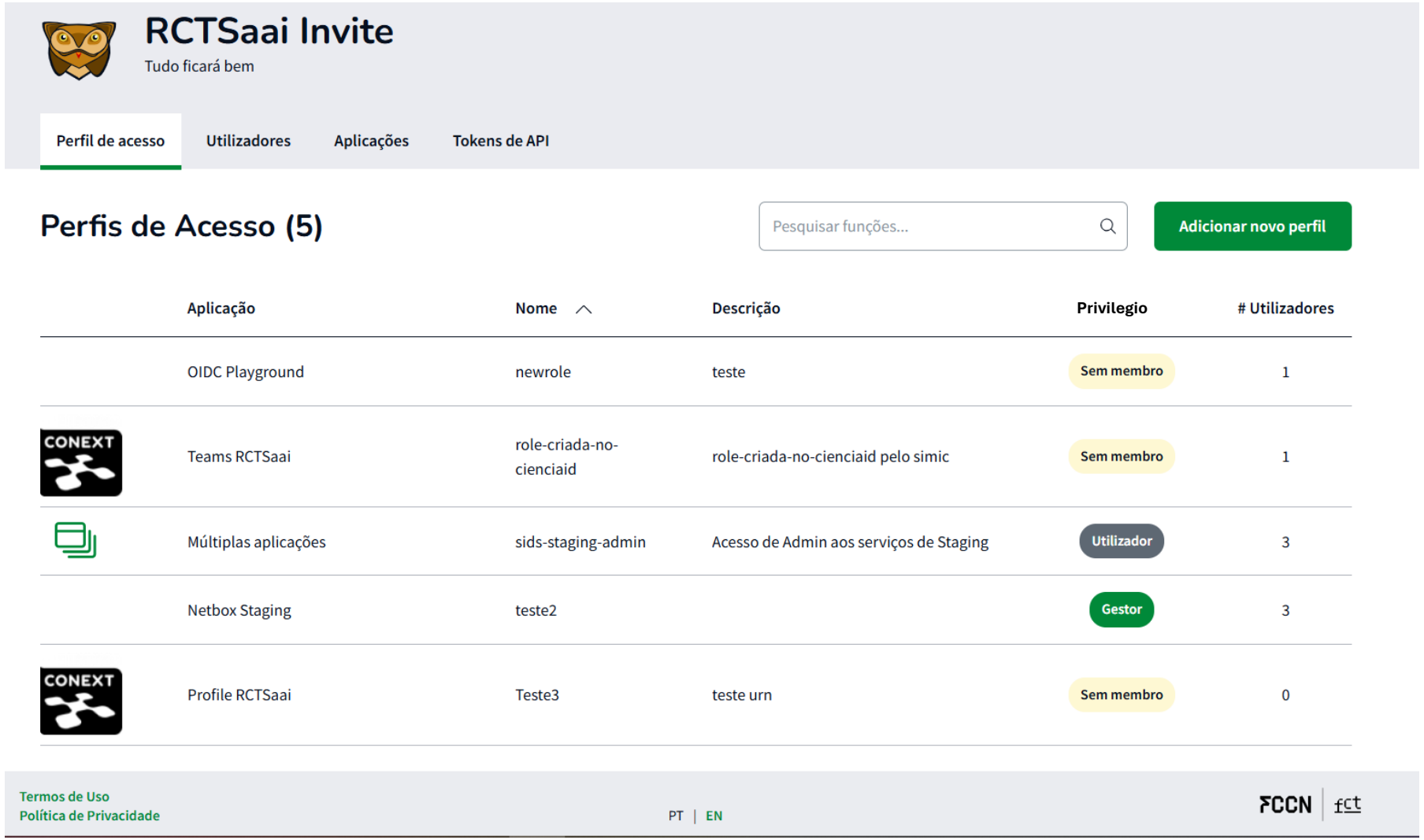
Acesso dos utilizadores



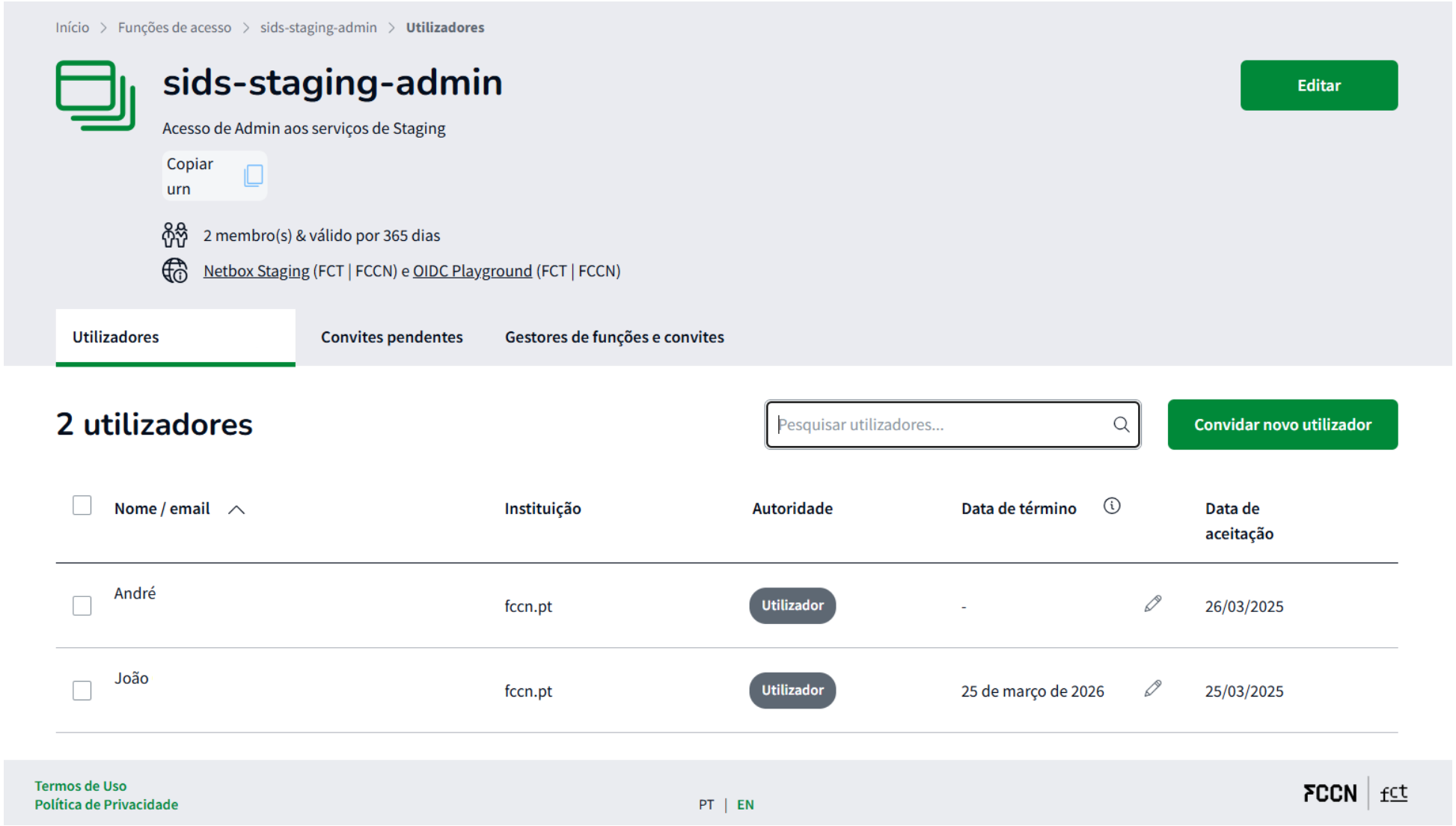
Os usuários terão acesso aos aplicativos vinculados ao RCTSaai, com base no **perfil** que a instituição atribui ao usuário.

Um **perfil** contém utilizadores que têm os mesmos direitos em um ou mais aplicativos.

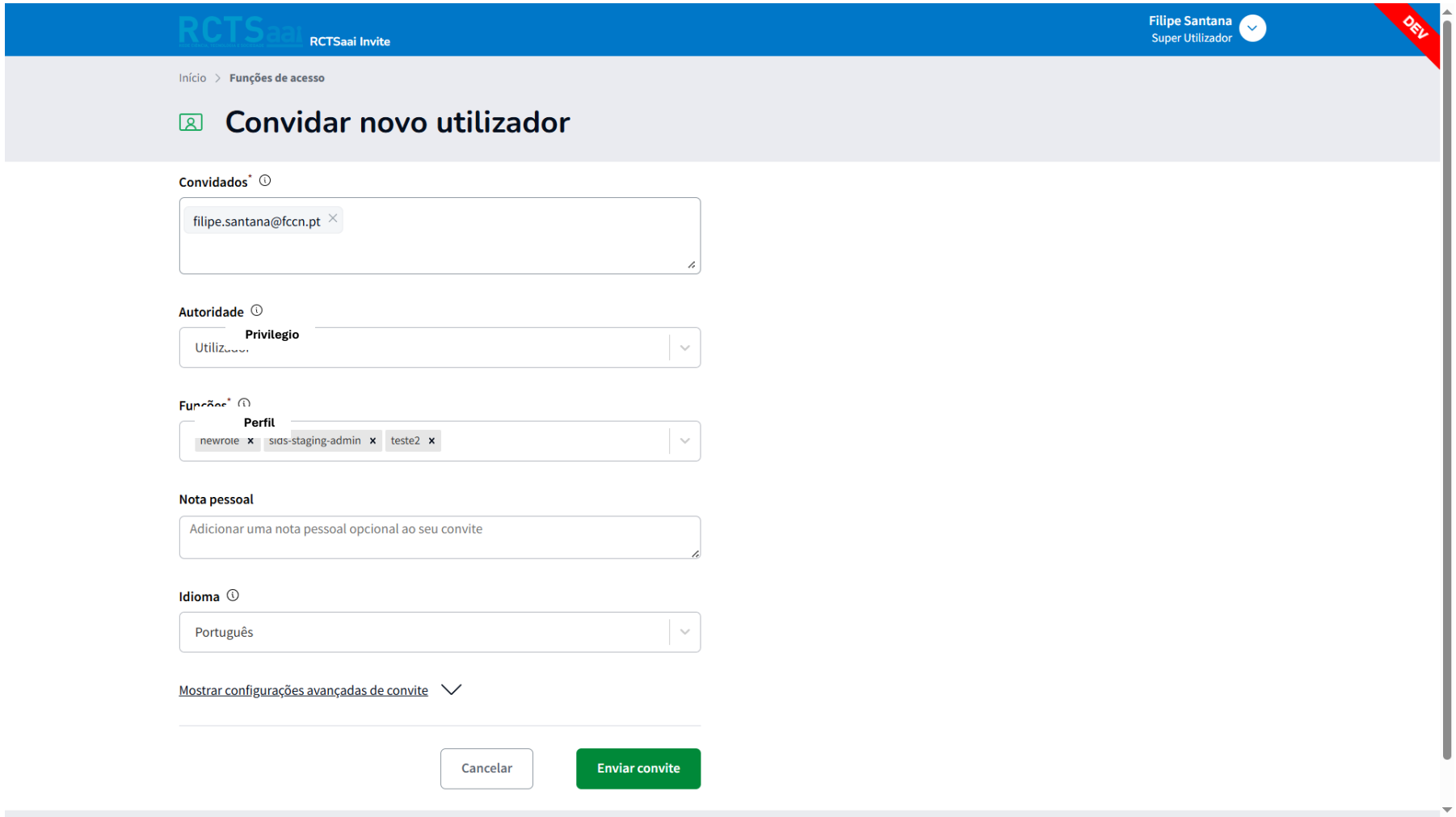
Acesso ao Invite



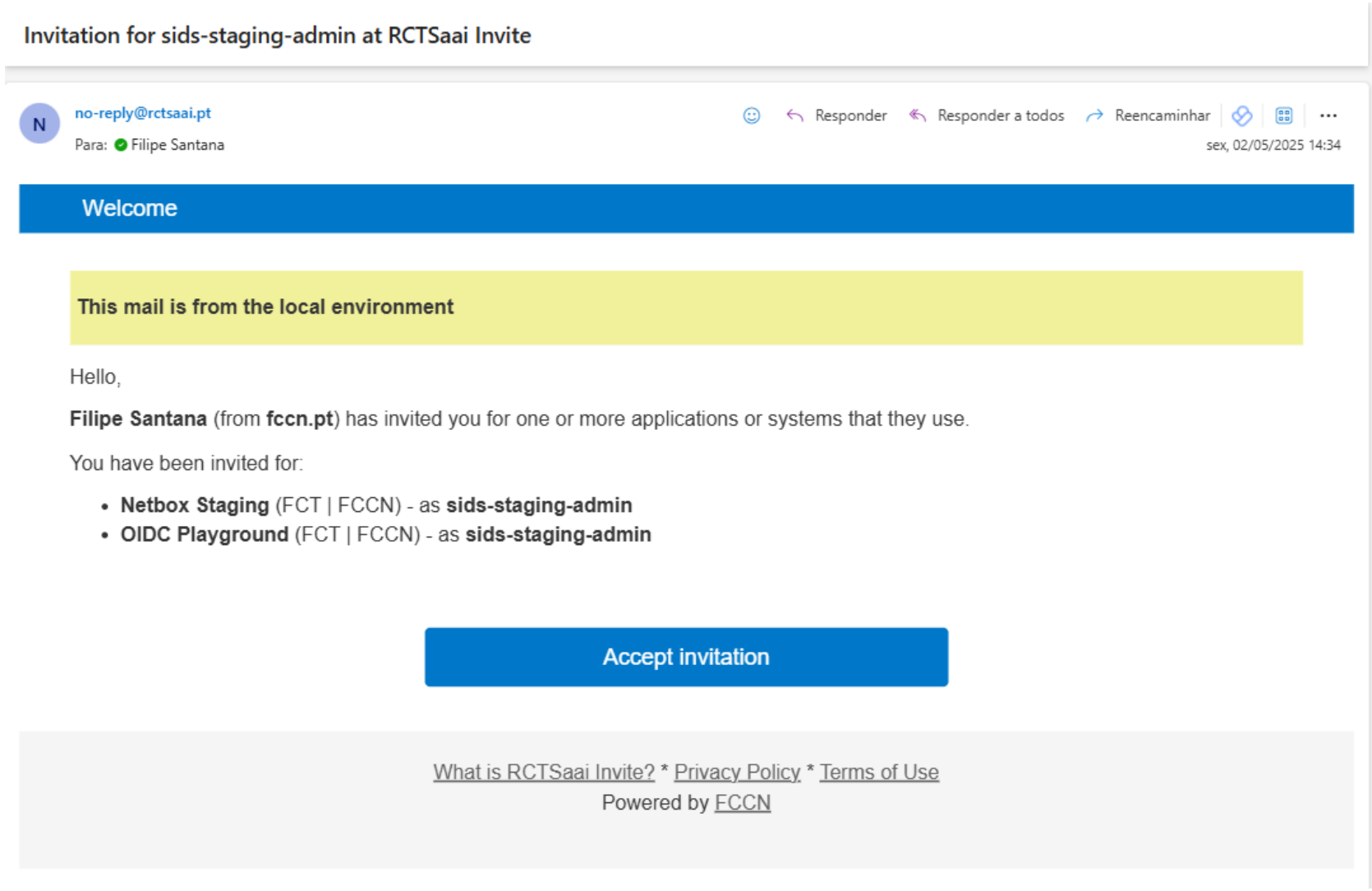
Utilizadores de um perfil



Utilizador Aceitando Convite



Utilizador Aceitando Convite



Invitation for sids-staging-admin at RCTSaai Invite

N no-reply@rctsaai.pt

Para: Filipe Santana

Responder | Responder a todos | Reencaminhar

sex, 02/05/2025 14:34

Welcome

This mail is from the local environment

Hello,

Filipe Santana (from **fccn.pt**) has invited you for one or more applications or systems that they use.

You have been invited for:

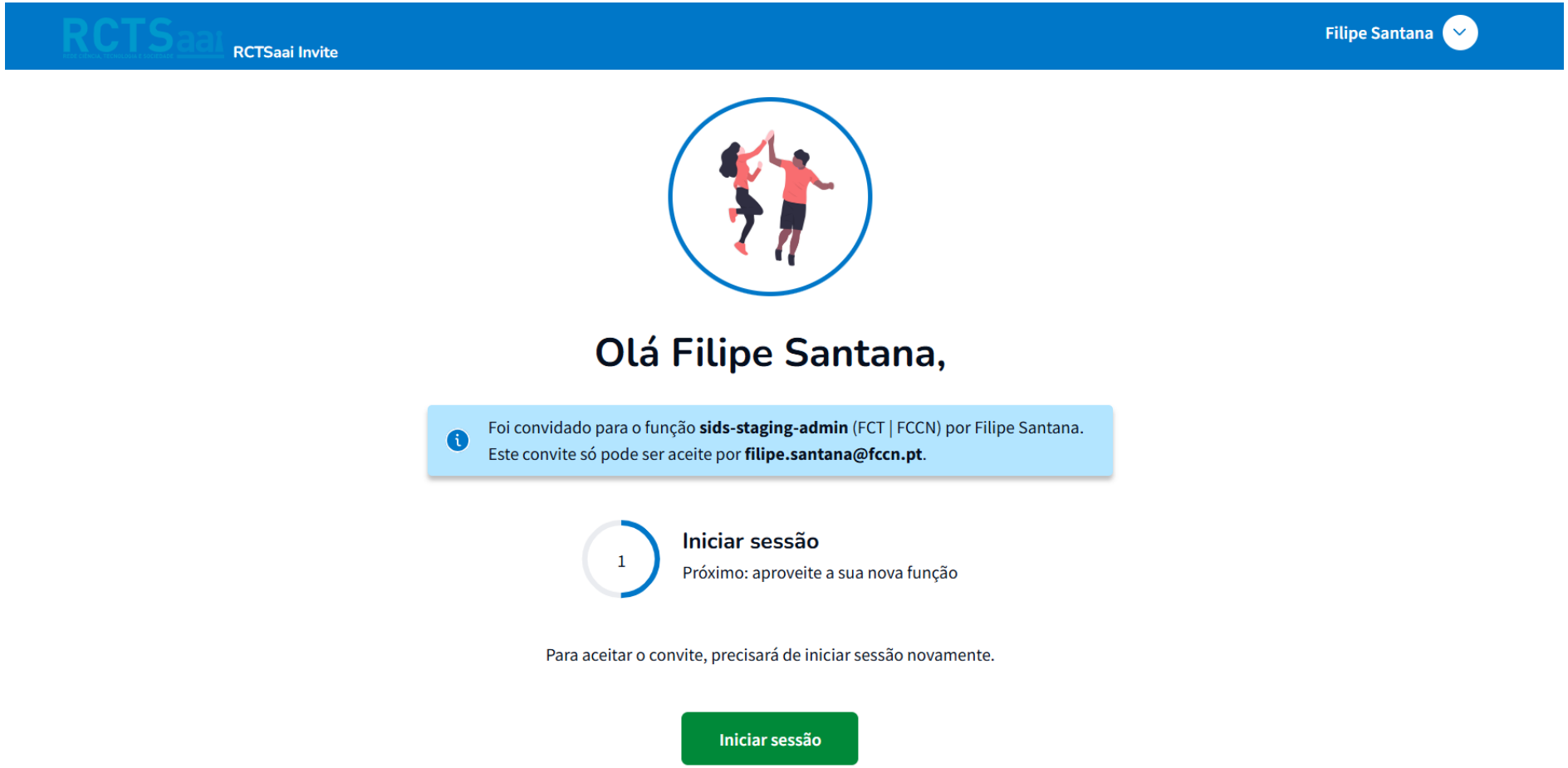
- **Netbox Staging** (FCT | FCCN) - as **sids-staging-admin**
- **OIDC Playground** (FCT | FCCN) - as **sids-staging-admin**

Accept invitation

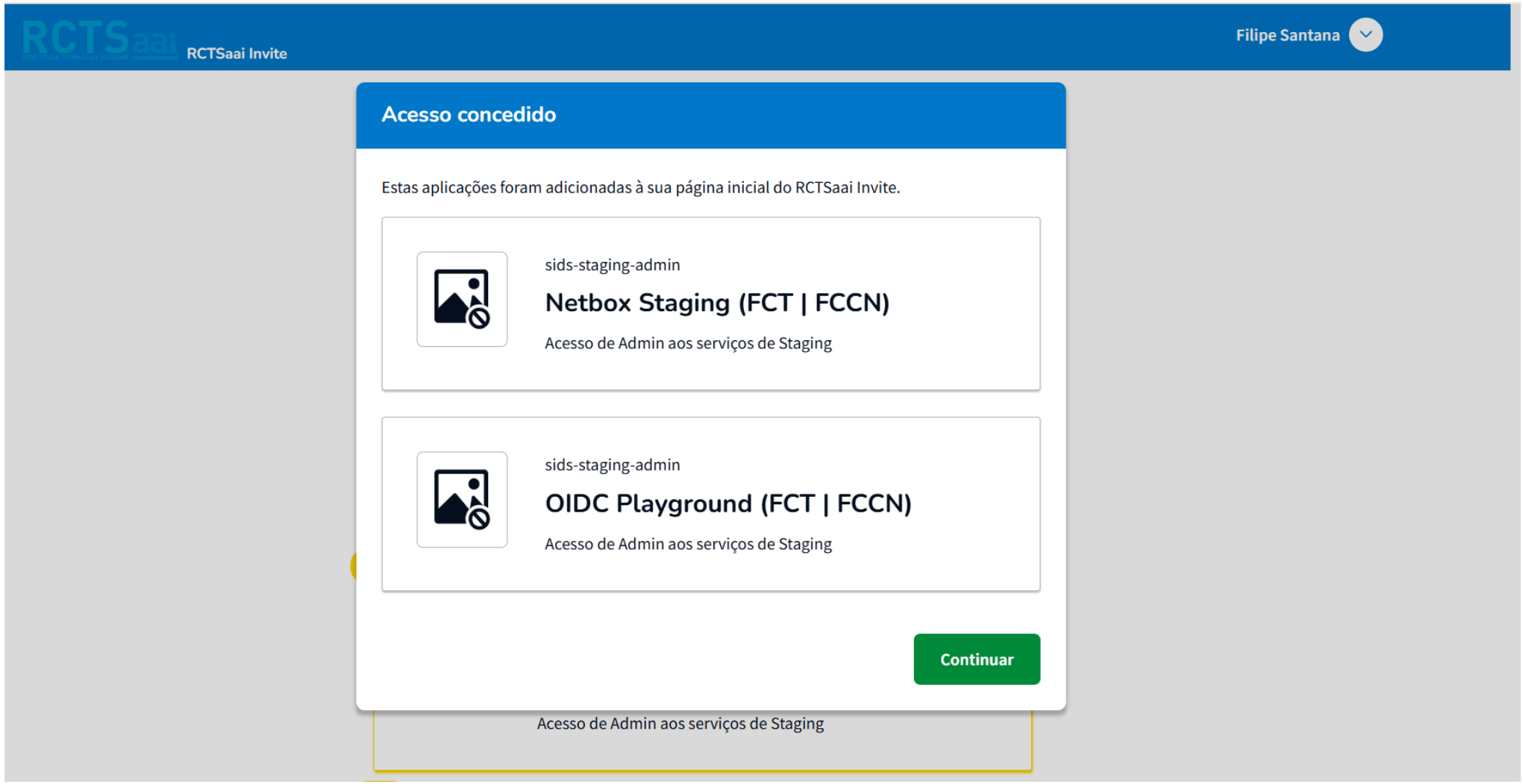
What is RCTSaai Invite? * Privacy Policy * Terms of Use

Powered by FCCN

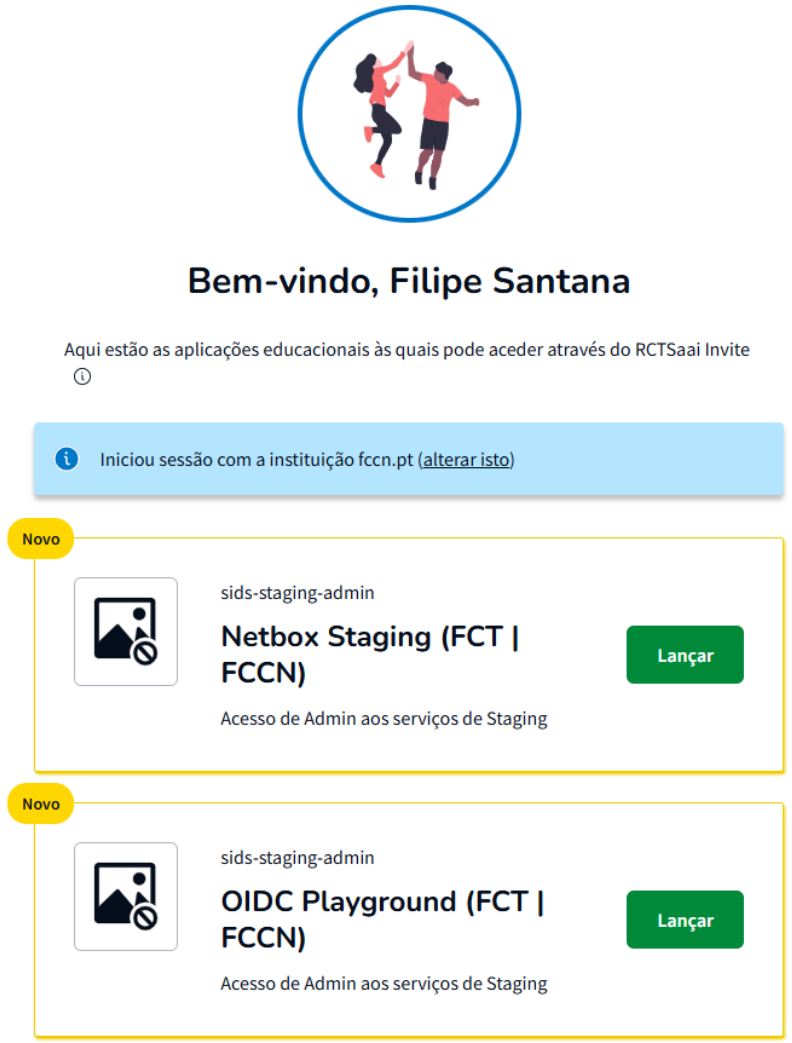
Utilizador Aceitando Convite



Utilizador Aceitando Convite



Utilizador Aceitando Convite

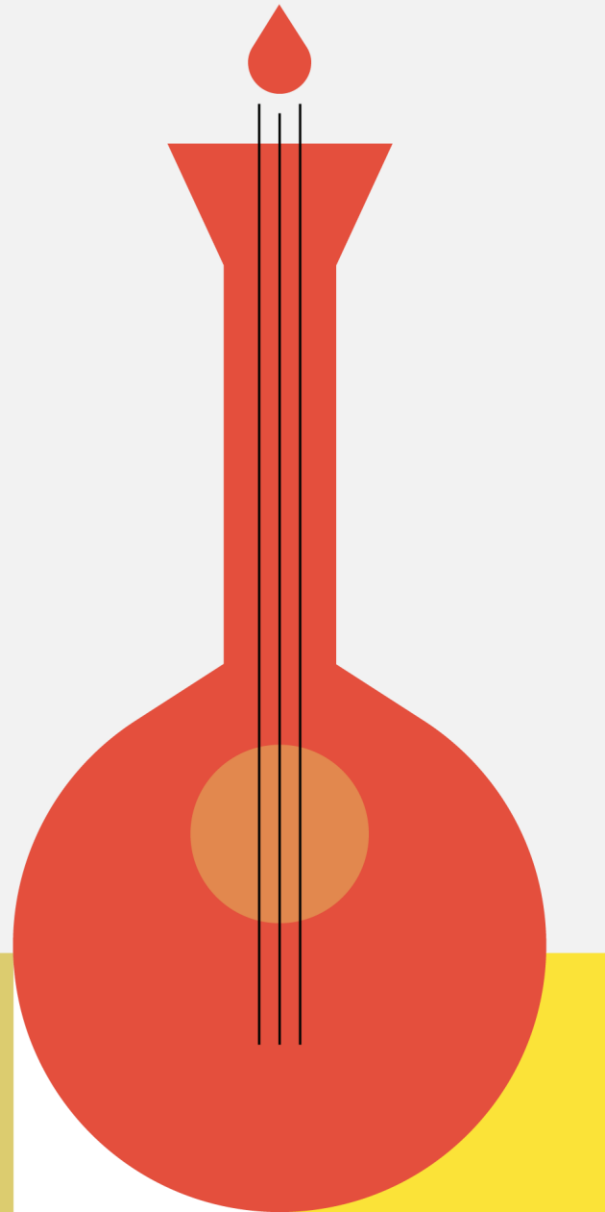


Privilegio	Tem a função/acesso ao aplicativo	Ver detalhes da função	Ver e convidar convidados	Adicionar/ Remover Convidadores	Criar/excluir função no aplicativo	Adicionar/ Remover Gerentes de Função	Adicionar aplicativos à função existente	Pode visualizar todas as funções e usuários
Utilizador	✓	✗	✗	✗	✗	✗	✗	✗
Gestor de convites	✗	✓	✓	✗	✗	✗	✗	✗
Gestor	✗	✗	✓	✓	✓	✗	✗	✗
Administrador da instituição	✗	✗	✓	✓	✓	✓	✓	✓

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA

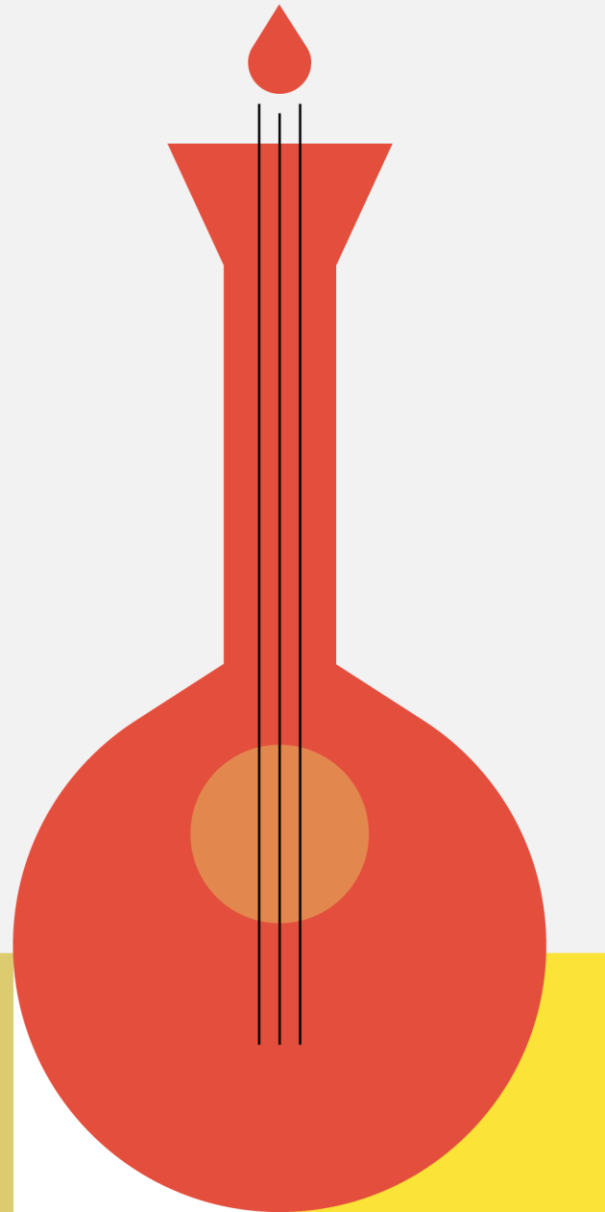
Identifica necessidades de formação nestes temas? Diga-nos quais!

jornadas FCCN

jornadas FCCN

Obrigado!

jornadas.fccn.pt | fccn.pt



FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | 1 2 9 0 UNIVERSIDADE D COIMBRA | CÂMARA MUNICIPAL COIMBRA