Jornadas FCCN 2023

# RCTSaai

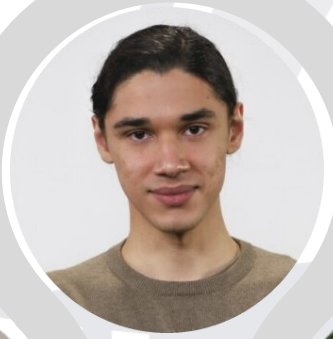
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

Esmeralda Pires – epires@fccn.pt

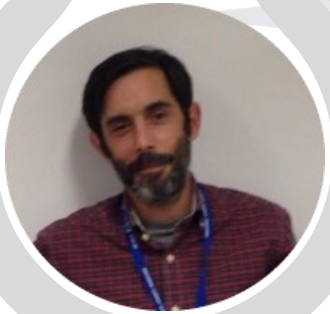
Jornadas FCCN 2023

Esmeralda Pires

Marco Coelho



Filipe Santana



Pedro Simões

João Guerreiro

Gonçalo Santos
(Estagiário)

# RCTSaai – 2021/2022

**77**

Entidades Participantes na RCTSaai

**73**

Entidades Participantes eduGAIN

Autenticações

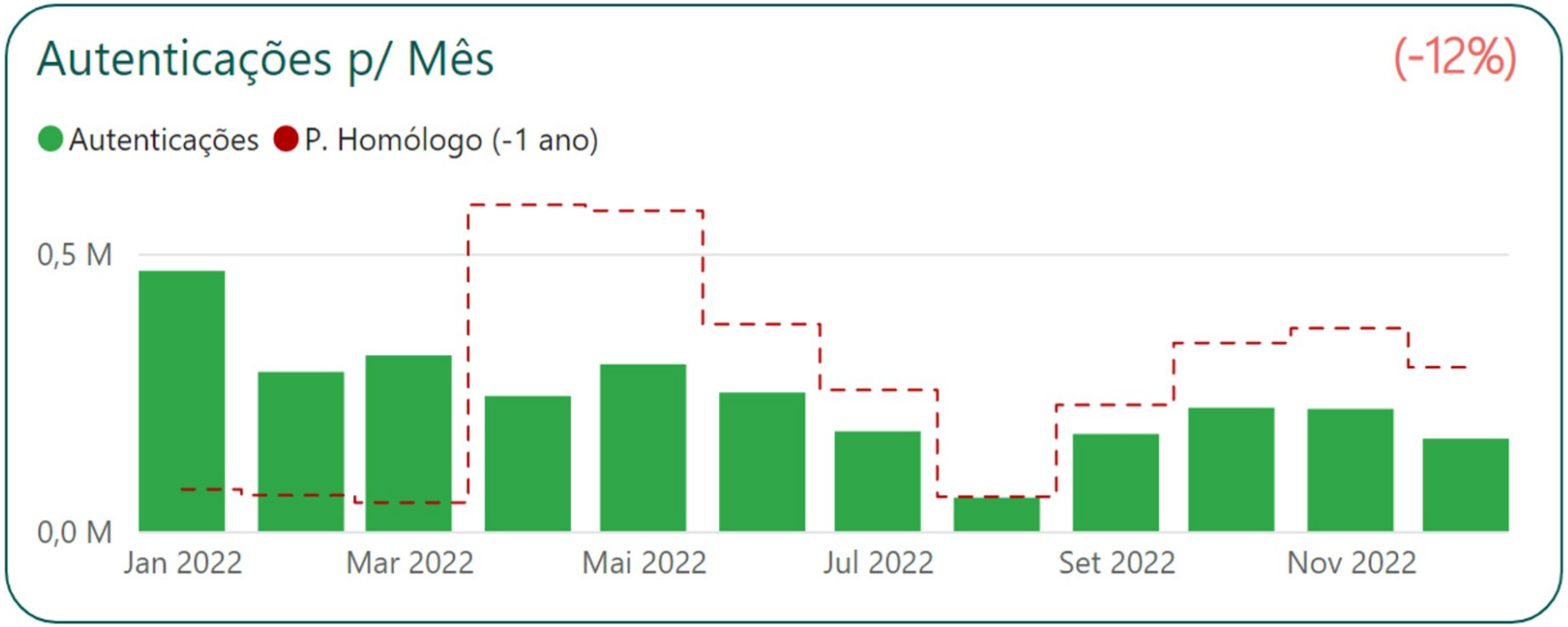
2,9 M

P. Homólogo: 3,3 M
(-11.68%)

Utilizadores Distintos

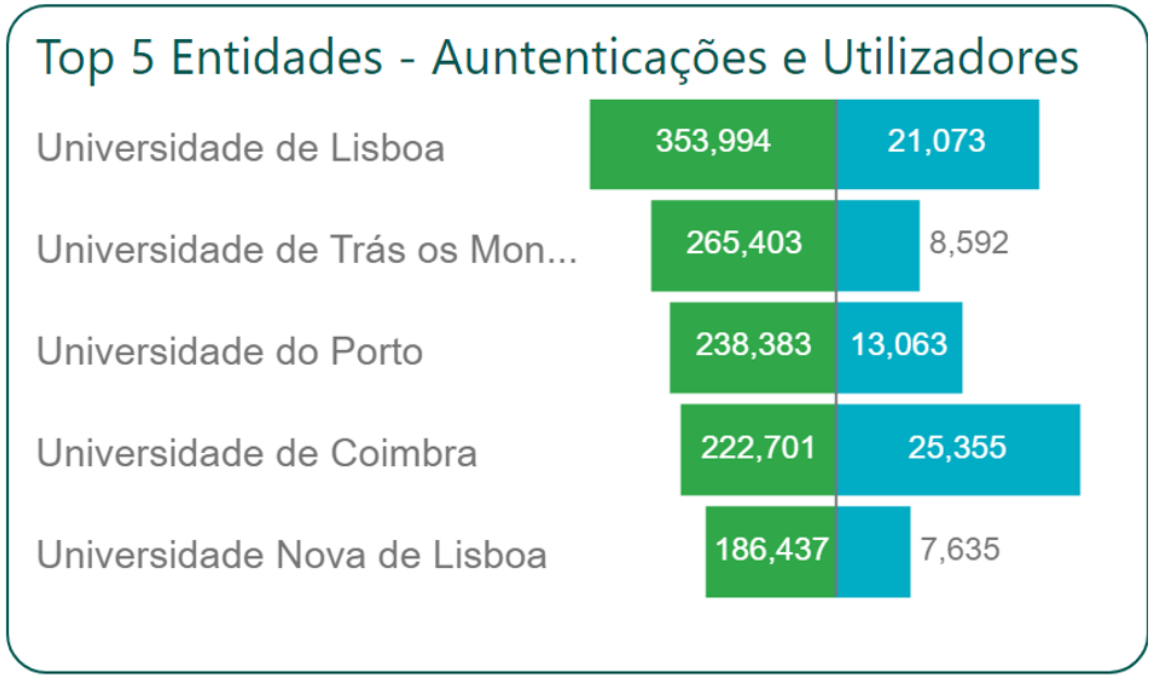
148,9 K

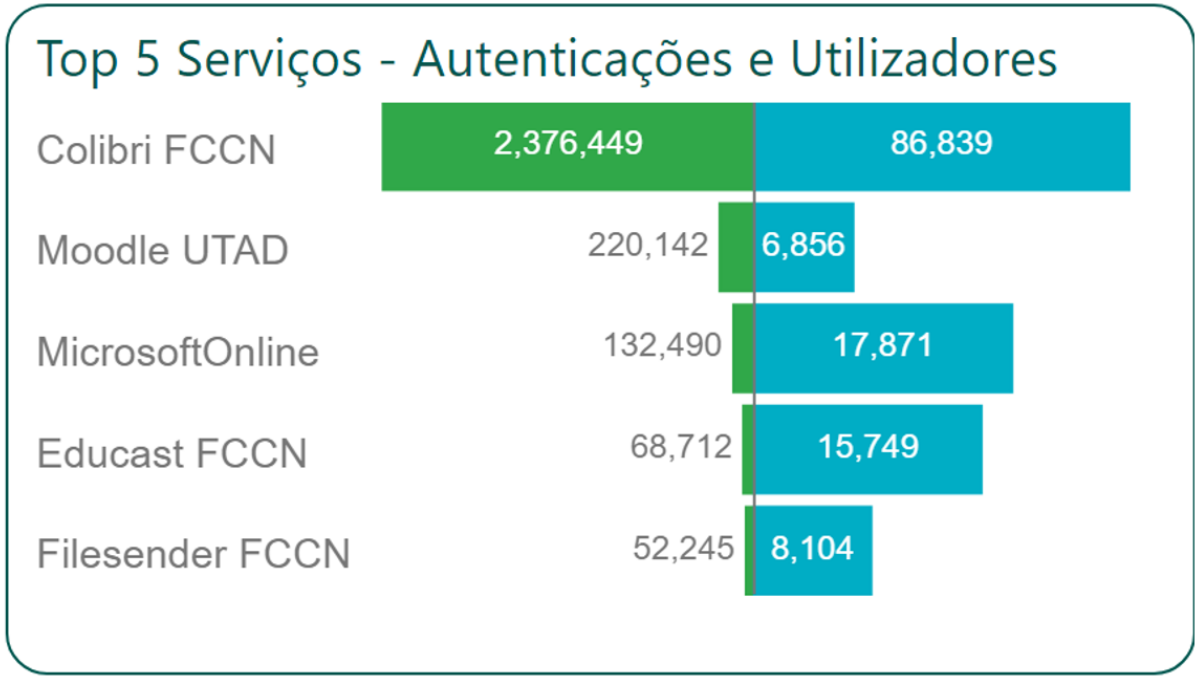
P. Homólogo: 130,6 K
(+14.01%)



# RCTSaai – 2021/2022

## TOP 5



# RCTSaai – Serviços

RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

38
Fornecedores de Serviço

eduGAIN

6
Fornecedores de Serviço

Interreg España - Portugal
Fondo Europeo de Desarrollo Regional
Fundo Europeu de Desenvolvimento Regional

UNISF

filmeu

utad
moodle

moodle
UNIVERSIDADE LUSÓFONA

TÉCNICO LISBOA

SMARTMEDIA
PLATAFORMA DE GESTÃO MULTIMÉDIA

FenixEdu Connect



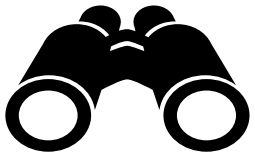
fct Fundação para a Ciência e a Tecnologia
FCCN

# RCTSaai – Serviços eduGAIN via Proxy

## Ponto de Situação

RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

b on biblioteca do conhecimento online



1. Análise com 5 instituições

2. Avançar com as restantes instituições

# Piloto “IdP as a Service”

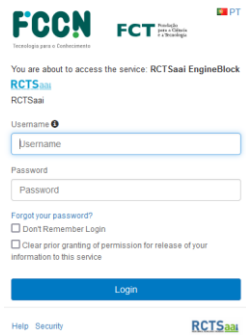
RCTSaai
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

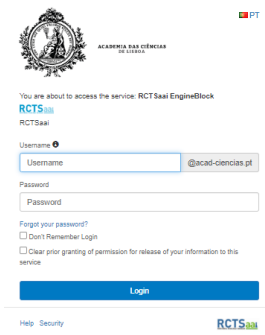
## OBJECTIVOS

- ✓ Identificar uma solução “chave na mão” da componente de Fornecedor de Identidade
- ✓ Adaptável aos vários cenários das instituições (AzureAD, AD, etc.)
- ✓ Direcionado para instituições de pequena dimensão e/ou com equipas técnicas reduzidas

Shibboleth

OVERT Software Solutions Ltd



# Alterações nos Browsers

Browser Changes and Federation

https://wiki.refeds.org/display/GROUPS/Browser+Changes+and+Federation

REFEDS Spaces Search Log in

Working-Groups

Pages
Blog

CHILD PAGES

Working-Groups Home
Browser Changes and Federation
Engagement with W3C FedID CG
Hackathon 2023-02-28 and 2023-...
Meetings
Slides, blogs, and videos
State of browser privacy evolution

Space tools

Pages / Working-Groups Home

## Browser Changes and Federation

Created by Heather Flanagan, last modified by Judith Bush on Jun 16, 2023

**This is our focus**
As browsers continue to threaten the cross-site methods used in authentication protocols to fight navigational tracking, we see that R&E community investment in testing these changes as a way to have a strong influence in the evolution of these changes. The two issues currently unaddressed are IdP picking from a list – and the massive scale they need to support for our in our community, – and the hops that are implemented in many authentication flows involving hub federations, federated proxies, and proxies bridging non-compliant IdPs into the federation.

### Overview

FedCM ("A privacy preserving federated identity Web API" - *quote from GitHub*) is several browser vendors go at ensuring users can still use buttons for "Sign in with <third party IdP vendor>..." even as the privacy preserving practices around third party cookies etc. are rolled out - privacy practises that would inevitably break the current login pattern. This baseline will enable us to continue offering our R&E community federated access as long as we take part in its development, and adapt our community's critical software stacks.

This new approach to protect end-user privacy that browsers are proposing appears to have a significant impact on R&E federation access practices. If you have software, have your developers reviewed https://fedidcg.github.io/FedCM/? Are they aware of a hackathon planned in Feb to test R&E tools and provide the W3C with feedback? Have you considered business continuity effects for your systems, especially if your suppliers do not address the new browser controls?

**Start here**
State of browser privacy evolution


- Overview
- State of browser privacy evolution
  - Co-chairs
- Meetings
- Deliverables
- Events
- Terms
- Resources
  - Communication
  - W3C resources
  - Industry resources
  - Child pages
  - 2023 Conference and other resources
  - 2022 Conference resources

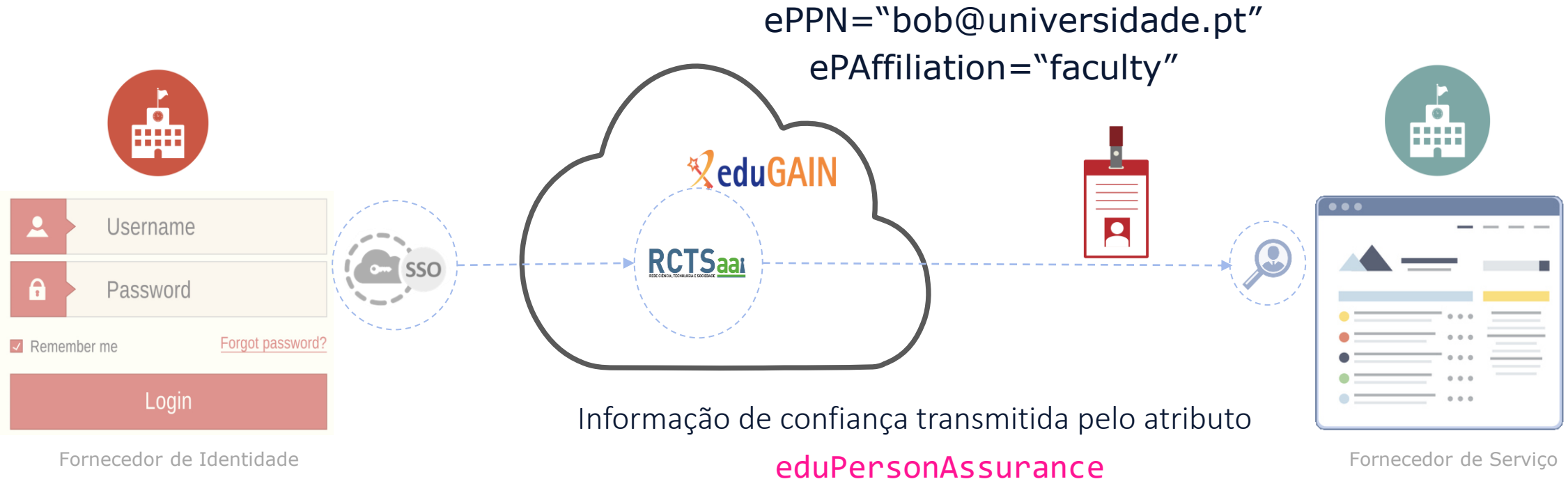

### Co-chairs

@Zacharias Törnblom and @Judith Bush

https://wiki.refeds.org

# REFEDS Assurance Suite

Especificações que definem requisitos para garantir a **Confiança na Identidade e Autenticação** do utilizador.




Informação de confiança transmitida pelo atributo

eduPersonAssurance

Jornadas FCCN 2023

# REFEDS Assurance Suite

eduPersonAssurance = { Múltiplo Valor }

## IDENTIFICADORES

- https://refeds.org/assurance/ID/unique
- https://refeds.org/assurance/ID/no-eppn-reassign

## VERIFICAÇÃO DE IDENTIDADE

- https://refeds.org/assurance/IAP/low
- https://refeds.org/assurance/IAP/medium
- https://refeds.org/assurance/IAP/high

## ATRIBUTOS

- https://refeds.org/assurance/ ATP/ePA-1m
- https://refeds.org/assurance/ ATP/ePA-1d

## AUTENTICAÇÃO

- Single Factor Authentication
- Multi Factor Authenication

REFEDS

Jornadas FCCN 2023

# REFEDS Assurance Suite – Cappucino & Espresso

| | CAPPUCINO | ESPRESSO |
|---|---|---|
| | ➢ Para casos de uso de baixo risco | ➢ Para casos de uso de alto risco |
| IDENTIFICADORES | https://refeds.org/assurance<br>https://refeds.org/assurance/ID/unique<br>https://refeds.org/assurance/ID/no-eppn-reassign | https://refeds.org/assurance<br>https://refeds.org/assurance/ID/unique<br>https://refeds.org/assurance/ID/no-eppn-reassign |
| VERIFICAÇÃO DE IDENTIDADE | https://refeds.org/assurance/IAP/low<br>https://refeds.org/assurance/IAP/medium<br>https://refeds.org/profile/cappucino | https://refeds.org/assurance/IAP/low<br>https://refeds.org/assurance/IAP/medium<br>https://refeds.org/assurance/IAP/high<br>https://refeds.org/profile/espresso |
| | eduPersonAssurance | eduPersonAssurance |

REFEDS



fct Fundação para a Ciência e a Tecnologia FCCN

# Federação de Identidade RCTS - Policy Framework

**01** POLÍTICA DA FEDERAÇÃO RCTS

**02** PERFIS TECNOLÓGICOS
- RCTSaai
- eduroam

**03** PERFIS DE CONFIABILIDADE
- Nível de Confiança Básico V1.0

# Estrutura dos Documentos

## 03 PERFIS DE CONFIABILIDADE

| RCTSaai – P0 | RCTSaai – P1 | RCTSaai – P2 | RCTSaai – P3 |
|---|---|---|---|

1. Conformidade e Auditagem
2. Organização
   - 2.1 Governação e Procedimentos na Operação do Fornecedor de Identidade
   - 2.2 Avisos e Dados do Utilizador

# Estrutura dos Documentos

## 03 PERFIS DE CONFIABILIDADE - REQUISITOS OPERACIONAIS

3.1 Identificadores

3.4 Verificação de Identidade e Gestão de Credenciais

- 4.1 Registo de Credenciais
- 4.2 Controlo e Verificação de Identidade
- 4.3 Emissão, Entrega e Ativação
- 4.4 Suspensão, Revogação e Reativação
- 4.5 Renovação e Suspensão

3.5 Qualidade do Atributo

3.6 Autenticação

# 03 PERFIS DE CONFIABILIDADE

RCTSaai – P0 | RCTSaai – P1 | RCTSaai – P2 | RCTSaai – P3

## IDENTIFICADORES

1. 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]

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

| RCTSaai – P0 | RCTSaai – P1 | RCTSaai – P2 | RCTSaai – P3 |
|---|---|---|---|

**IDENTIFICADORES**

2. O identificador do utilizador representa uma pessoa física; e

3. A organização deve ser capaz de entrar em contacto com a pessoa a que o identificador foi atribuído.

4. Os identificadores atribuídos aos utilizadores NUNCA DEVE ser reatribuídos/reutilizados.

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

- RCTSaai – P0
- RCTSaai – P1
- RCTSaai – P2
- RCTSaai – P3

**IDENTIFICADORES**

eduPersonAssurance = { **https://refeds.org/assurance,**
**https://refeds.org/assurance/ID/unique** }

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P0 | RCTSaai – P1 | RCTSaai – P2 | RCTSaai – P3

**VERIFICAÇÃO DE IDENTIDADE**

- Requisitos Diferentes Por Perfil
- Secção de Controlo e Verificação de Identidade
  - Verificação Pessoal
  - Verificação Remota
  - Verificação Baseada em Outras Credenciais

P2 e P3

Verificação
+
Autenticação

Influencia o resultado
Médio e Alto

**AUTENTICAÇÃO**

SF **ou** MF

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P0

**IDENTIFICADORES**

**https://refeds.org/assurance/ID/unique**

**VERIFICAÇÃO DE IDENTIDADE**

Ex.: Conta auto-registada com confirmação por e-mail.

**AUTENTICAÇÃO**

SF **OU** MF

**IAP/LOW**

```
eduPersonAssurance = {
        https://refeds.org/assurance,
        https://refeds.org/assurance/ID/unique,
        https://refeds.org/assurance/IAP/low
        }
```

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P1

**IDENTIFICADORES**

**VERIFICAÇÃO DE IDENTIDADE**

**AUTENTICAÇÃO**

**https://refeds.org/assurance/ID/unique**

Ex.: Matricula de Aluno e Identificado pela exibição de um documento de identidade aparentemente autêntico

SF **OU** MF

**IAP/MEDIUM**

```
eduPersonAssurance = {
    https://refeds.org/assurance,
    https://refeds.org/assurance/ID/unique,
    https://refeds.org/assurance/IAP/low,
    https://refeds.org/assurance/IAP/medium
}
```

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P2

**IDENTIFICADORES**

**https://refeds.org/assurance/ID/unique**

**VERIFICAÇÃO DE IDENTIDADE**

Ex.: Identidade verificada por meio de um documento aparentemente autêntico e confirmada por uma fonte autorizada.

**IAP/MEDIUM**

**AUTENTICAÇÃO**

SF

```
eduPersonAssurance = {
    https://refeds.org/assurance,
    https://refeds.org/assurance/ID/unique,
    https://refeds.org/assurance/IAP/low,
    https://refeds.org/assurance/IAP/medium
}
```

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P2

**IDENTIFICADORES**

**https://refeds.org/assurance/ID/unique**

**VERIFICAÇÃO DE IDENTIDADE**

Ex.: Identidade verificada por meio de um documento aparentemente autêntico e confirmada por uma fonte autorizada.

MF

**IAP/HIGH**

**AUTENTICAÇÃO**

```
eduPersonAssurance = {
    https://refeds.org/assurance,
    https://refeds.org/assurance/ID/unique,
    https://refeds.org/assurance/IAP/low,
    https://refeds.org/assurance/IAP/medium,
    https://refeds.org/assurance/IAP/high
}
```

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P3

**IDENTIFICADORES**

**https://refeds.org/assurance/ID/unique**

**VERIFICAÇÃO DE IDENTIDADE**

Ex.: Autenticação com o cartão de cidadão

**AUTENTICAÇÃO**

SF

**IAP/MEDIUM**

```
eduPersonAssurance = {
   https://refeds.org/assurance,
   https://refeds.org/assurance/ID/unique,
   https://refeds.org/assurance/IAP/low,
   https://refeds.org/assurance/IAP/medium
}
```

# Federação de Identidade RCTS - Policy Framework

## 03 PERFIS DE CONFIABILIDADE

RCTSaai – P3

**IDENTIFICADORES**

**https://refeds.org/assurance/ID/unique**

**VERIFICAÇÃO DE IDENTIDADE**

Ex.: Autenticação com o cartão de cidadão

**AUTENTICAÇÃO**

MF

**IAP/HIGH**

```
eduPersonAssurance = {
    https://refeds.org/assurance,
    https://refeds.org/assurance/ID/unique,
    https://refeds.org/assurance/IAP/low,
    https://refeds.org/assurance/IAP/medium,
    https://refeds.org/assurance/IAP/high
}
```

# Instituição – Processo de Análise

1. Avaliar processo(s) de **Verificação de Identidade** dos utilizadores na Instituição e validar conformidade com os requisitos definidos nos perfis RCTSaai-P0,P1,P2 e P3

| | |
|---|---|
| RCTSaai – P0 | Auto-Registo com validação por e-mail |
| RCTSaai – P1 | Apresenta Doc. Identificação aparentemente válido |
| RCTSaai – P2 | Apresenta Doc. Identificação aparentemente válido e Confirmado |
| RCTSaai – P3 | eIDAS regulation (EU) Alto |

| | |
|---|---|
| SF | **IAP/MEDIUM** |
| MF | **IAP/HIGH** |

# Requisitos Lumi

*Attribute requirements*

https://puhuri.neic.no/idp_integration/attributes/

- Identifier
- Name
- email
- Affiliation
- Assurance
- Organisation

*Level of assurance requirements*

**REFEDS Assurance Framework** https://wiki.refeds.org/display/ASS

To insure sufficient **identity proofing and credential issuance, renewal, and replacement**

https://refeds.org/assurance/IAP/medium; or
https://refeds.org/assurance/IAP/high

To insure **identifier uniqueness**

https://refeds.org/assurance/ID/UNIQUE; or
https://refeds.org/assurance/ID/eppn-unique-no-reassign

neic PUHURI

# Instituição - Configuração dos Perfis

1. Classificar e armazenar o perfil dos seus utilizadores

   Exemplos:
   - Criar atributo eduPersonAssurance no LDAP
   - Criar Grupos de acordo com o Perfil

# Instituição - Configuração do Atributo *eduPersonAssurance*

2. Criar atributo eduPersonAssurance e mapear os valores com base:

- No tipo de autenticação realizada pelo utilizador

+

- Perfil do utilizador armazenado na AD

# FCCN - Próximos Passos

## Até ao final do 2ºQuadrimestre

1. Publicar Perfis de Confiabilidade

2. Disponibilizar configurações de exemplo na criação do atributo eduPersonAssurance para Shibboleth IdP e SimplesamlPHP

Jornadas FCCN 2023

# Obrigada!

**Espaço RCTSaai**
**https://share.fccn.pt/sites/rctsaai**

# Patrocinadores

## Platina

EBSCO
ELSEVIER
Microsoft
warpcom
cisco
FORTINET
axians
officelan
SECURNET
CHECK POINT
SYSCRUM
PAESSLER
THE MONITORING EXPERTS
ORACLE
NVIDIA
paloalto
software one

## Ouro

ACS Publications
Most Trusted. Most Cited. Most Read.
Clarivate
CAMBRIDGE UNIVERSITY PRESS
DE GRUYTER
HUAWEI
DIVULTEC
LOGICALIS
Architects of Change
Sage
SPRINGER NATURE
tp-link
wavecom
Bravantic
itcenter
reallife

## Prata

ROYAL SOCIETY OF CHEMISTRY
IOP Publishing
MEO EMPRESAS
aws
emerald PUBLISHING
IEEE
Logiser

## Organização

fct Fundação para a Ciência e a Tecnologia
FCCN