

Jornadas
— FCCN

RCTS **aaai**
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

Infraestrutura de Autenticação Federada

jornadas.fccn.pt



FCCN
serviços digitais fct

fct Fundação
para a Ciência
e a Tecnologia

arditi agência regional para o
desenvolvimento da investigação
tecnológica e inovação

SIH

UNIVERSIDADE da MADEIRA



Agenda



Ponto de Situação RCTSaai e Plano de Ação para Adoção dos Perfis de Confiabilidade

1 *João Guerreiro
Esmeralda Pires*



Adoção da solução privacyIDEA para Autenticação Multifactor (MFA) no Instituto Universitário Egas Moniz

2 *Porfírio Trincheiras*



Monitorização de Infraestruturas

3 *Válter Gouveia*

Patrocinador da Sessão

jornadas.fccn.pt





RCTS **aa**i
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

Ponto de Situação

FCCN – João Guerreiro



Feedback



Acede a menti.com | e usa o código 7629 0290

Ok

Ok

Good

Ok

Pb

The dark side

Sim

Sim



Sim

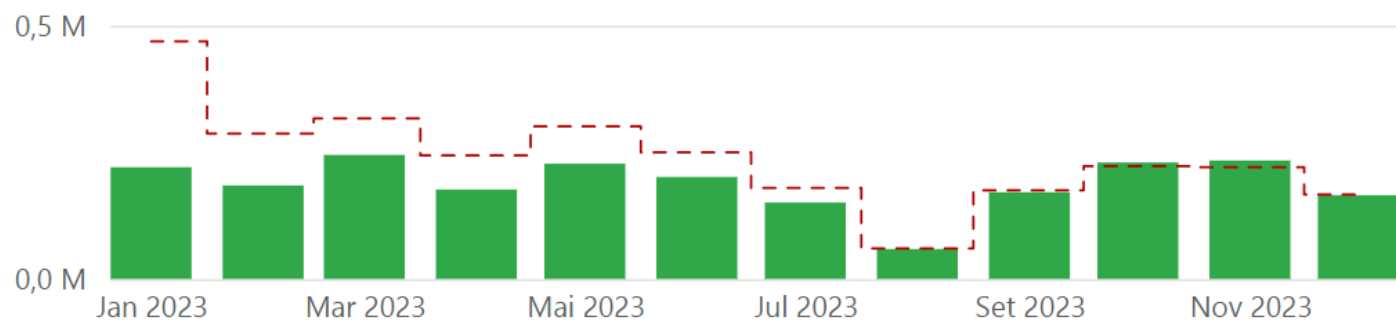
Sim

Sim

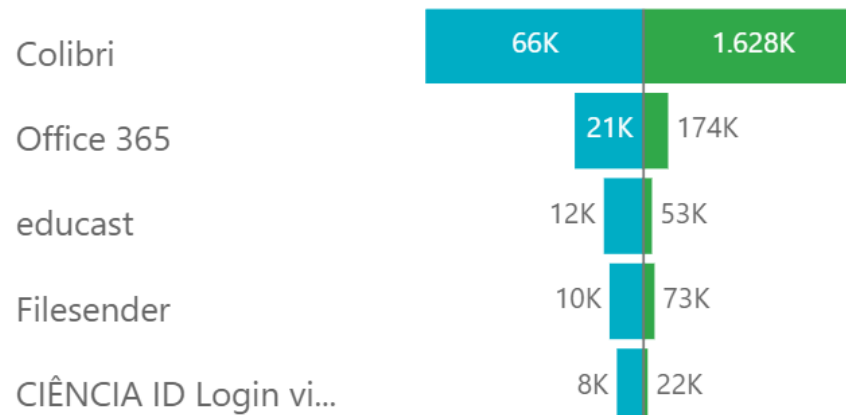


Autenticações p/ Mês

● Autenticações ● P. Homólogo (-1 ano)



Top 5 Serviços - Utilizadores e Autenticações



Autenticações

2,3 M

P. Homólogo: 2,9 M (-22%)

Utilizadores Distintos

147,3 K

P. Homólogo: 148,9 K (-1%)

Entidades Aderentes

78

(+2)

Entidades no eduGAIN

74

(+5)



Acede a menti.com | e usa o código 4620 6632

Estariam interessados num serviço em que
pudessem aceder a este tipo de informação para
a vossa Instituição?



Sim

Não



Acede a [menti.com](https://www.menti.com) | e usa o código 4620 6632

Conhecem o serviço dashboard.rctsaai.pt?



Sim

Não



Filtros ⓘ

Limpar

Serviço

Todos os Serviços ▾

Visualizar detalhes por Serviço

Período

Mês ▾

De

janeiro ▾

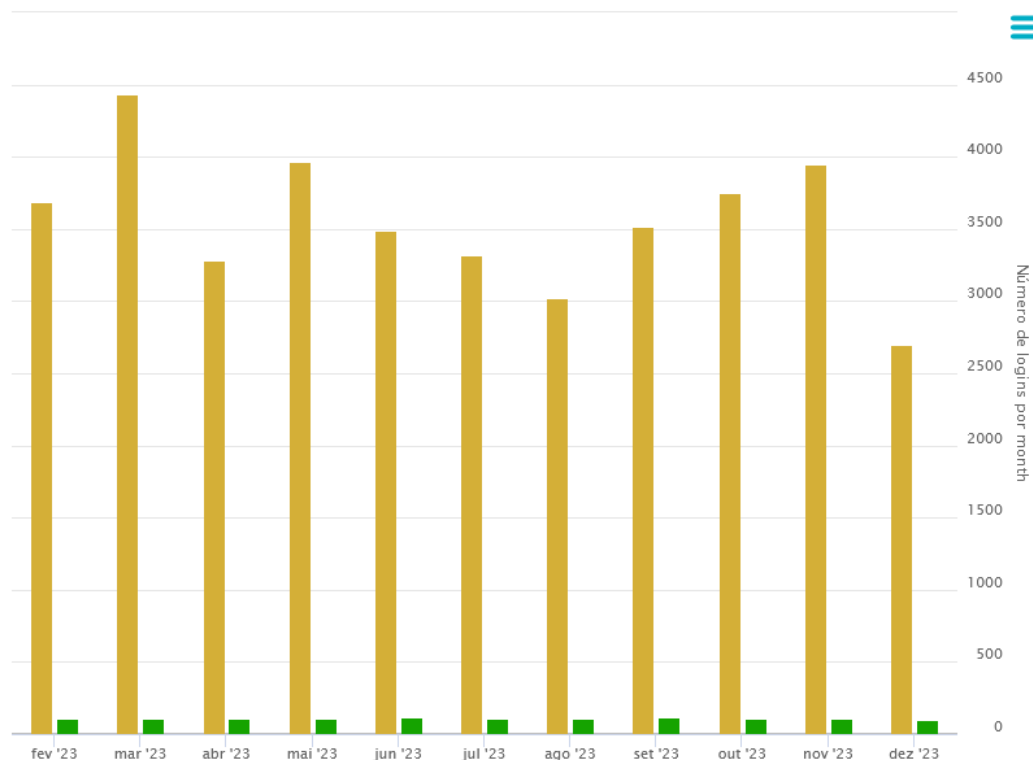
2023 ▾

Até e incluindo

deze... ▾

2023 ▾

Logins por mês



Acede a menti.com | e usa o código 4620 6632

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



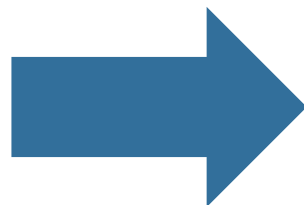
Sim

Não



RCTS **aa**i
REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

46 SERVIÇOS



36 SAML



10 OIDC



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



Estamos quase a 100%!


74 entidades de 78

93 IDPs de 103



Estamos quase a 100%! 



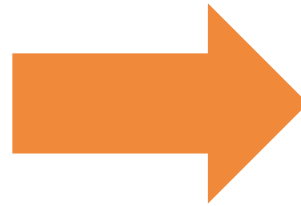
- Metadata vai passar a estar apenas no  **eduGAIN**
IDPs de Instituições que têm acesso aos conteúdos B-ON integrar o eduGAIN



SPs no eduGAIN


REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

**46 Fornecedores
de Serviço**



 **eduGAIN**

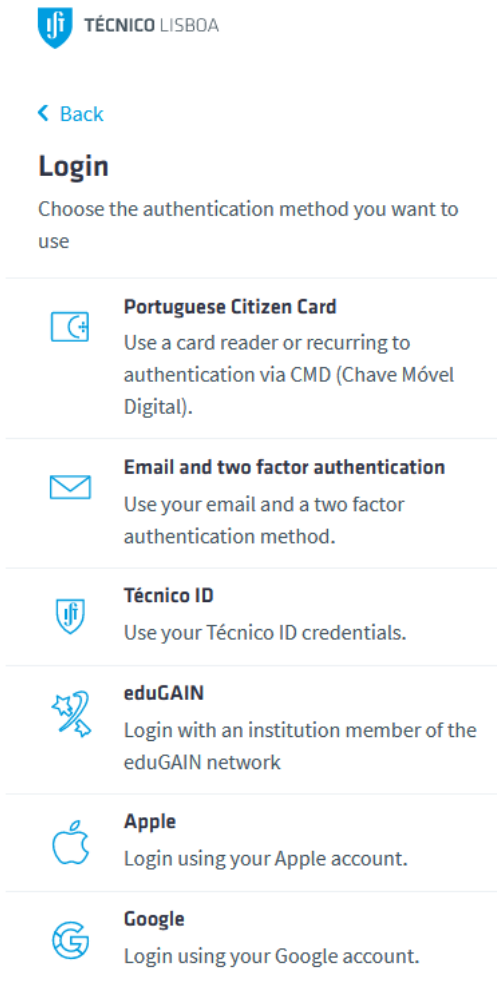
**6 Fornecedores
de Serviço**



Integração de serviços no

Exemplo: FenixEdu Connect

- Serviço do Instituto Superior Técnico, Universidade de Lisboa
- **Objectivo:** Abrir leque de utilizadores de serviço à comunidade europeia do



Acede a [menti.com](https://www.menti.com) | e usa o código 4620 6632

Identificam serviços que usem actualmente e que pudessem beneficiar com a integração no edugain?



Sim

Não



Acede a [menti.com](https://www.menti.com) | e usa o código 4620 6632

Quais as maiores dificuldades dessa possível integração? (Eg., Complexidade no serviço, falta de recursos, desconhecimento do procedimento, etc.)

leader fast inspiration
creative
bold focus
transpiration



Acede a [menti.com](https://www.menti.com) | e usa o código 4620 6632

Qual a versão do Fornecedor de Identidade utilizado pela sua Instituição?



- Shibboleth IDP v2
- Shibboleth IDP v3
- Shibboleth IDP v4
- Shibboleth IDP v5
- SimpleSAMLphp v2
- SimpleSAMLphp v1
- Outro



Software Shibboleth IDP – Fim de vida (EOL)

Versão	5.1.1	5.0.0	4.3.2	4.3.1	4.3.0	4.2.1	4.1.6	4.1.0	4.0.1	4.0.0	3.4.8
EOL		mar/24	set/24	mar/24	mar/23	jan/23	abr/22	mai/21	mar/21	jun/20	dez/20

Apenas as versões 4.3.2 e 5.1.1 têm suporte oficial da Shibboleth



Software Shibboleth IDP – Vulnerabilidades

Versão	Exposição dos dados do utilizador	Precisão dos dados do utilizador	Hijacking de sessão	Negação de serviço (DOS)	Exploração remota	Recomendações
5.1.1/4.3.2						
5.0.0			L			2024-03-20
4.3.1			L			2024-03-20
4.3.0	L	L	L			2023-03-30
4.1.6			C	C	C	2022-12-16
4.1.5			C	C	C	Spring Vulnerability
3.4.4	M	M		M	M	2019-09-18

Severidade: **L** – Low, **M** – Moderate, **C** – Critical



Fornecedores de Identidade



Pacote de Ansible para Instalação de Shibboleth IDP v4.3.2 em Debian 11/12
Ver Área do RCTSaai em share.fccn.pt/sites/rctsai



FCCN – Pacote ACME

Funcionalidades

- Instala e configura *certbot*



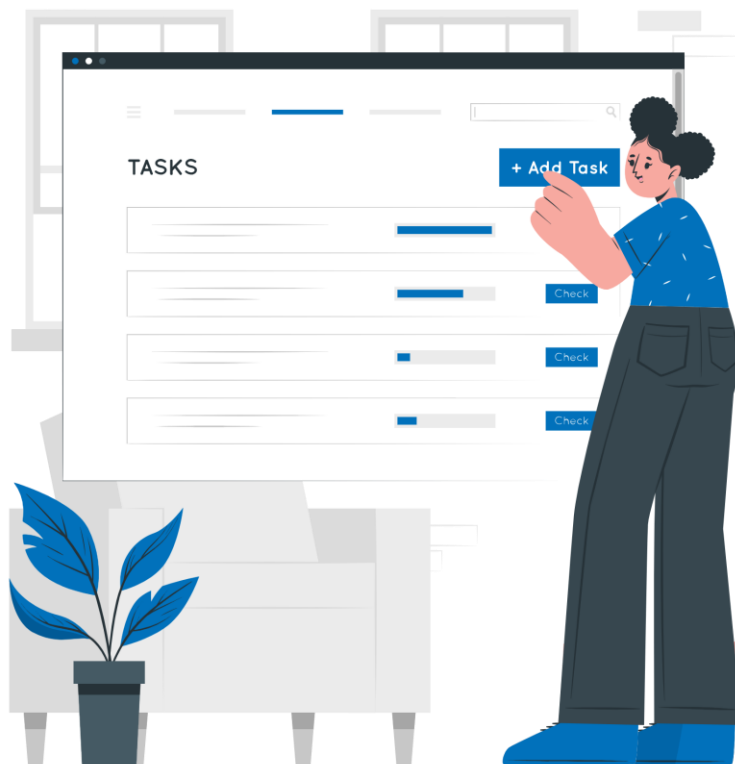
ANSIBLE

No servidor, o *certbot* vai periodicamente:

- Confirmar se certificados se mantêm válidos
- **Se necessário, pede e transfere novo certificado**
- **Pode reiniciar aplicações (*apache, nginx, etc.*)**



Pacote Ansible e documentação em share.fccn.pt/sites/rctscertificados



Plano de Ação para Adoção dos Perfis de Confiabilidade

FCCN – Esmeralda Pires (epires@fccn.pt)





<https://share.fccn.pt/sites/rctsaai/areatecnica/assurance/Perfis>



RCTSaai eduGAIN Participantes Serviços Área Técnica Contactos FAQ

Perfis de Confiabilidade RCTS

Perfis de Confiabilidade RCTS

Os perfis de Confiabilidade RCTSaai tem como objetivo definir um conjunto de regras que permite validar e afirmar a qualidade da identidade digital dos utilizadores da Federação de Identidade Digital RCTS.

Estes perfis estão organizados por vários componentes que se encontram divididos da seguinte forma:

- **Identificadores:** define os requisitos inerentes ao processo de atribuição de um identificador único e permanente que representa uma pessoa física.
- **Verificação de Identidade e Gestão de Credenciais:** define os requisitos inerentes ao processo de identificação, credenciação dos indivíduos, atribuição de credenciais e respetiva renovação e substituição realizado por uma organização.
- **Qualidade dos Atributos:** define os requisitos relativos ao processo de atribuição de determinados níveis de qualidade e atualização dos atributos transmitidos pela organização.

Os componentes que definem a robustez do processo de autenticação são baseados no REFEDS Single Factor Authentication Profile [REFEDS-SFA], no REFEDS Multi-Factor Authentication Profile [REFEDS-MFA] e no documento de diretrizes para a identidade digital Authentication and Lifecycle Management NIST [NIST 800-63B].

Perfis de Confiabilidade RCTS

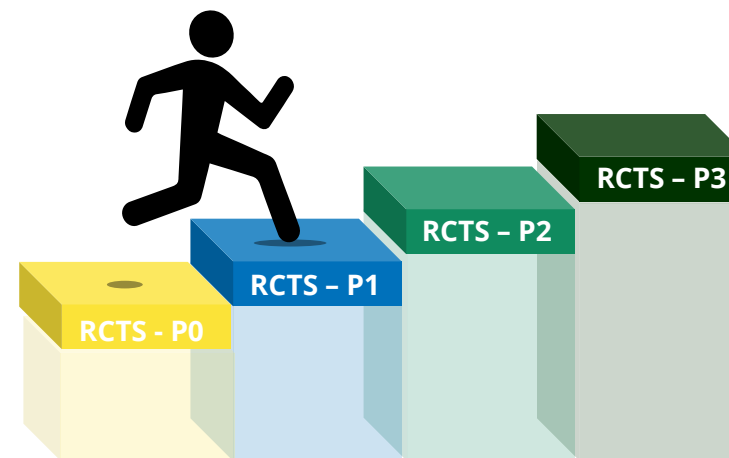
- Perfil RCTS-P0
- Perfil RCTS - P1
- Perfil RCTS - P2
- Perfil RCTS - P3

Representação dos Valores do Perfis

- Perfil RCTS - P0
- Perfil RCTS - P1
- Perfil RCTS - P2
- Perfil RCTS - P3

Analisar e Classificar Utilizadores

Configurar o Fornecedor de Identidade



Estrutura dos Requisitos Operacionais



Definição dos Requisitos Operacionais = P0 P1 P2 P3



Definição dos Requisitos Operacionais = P0 P1 P2 P3

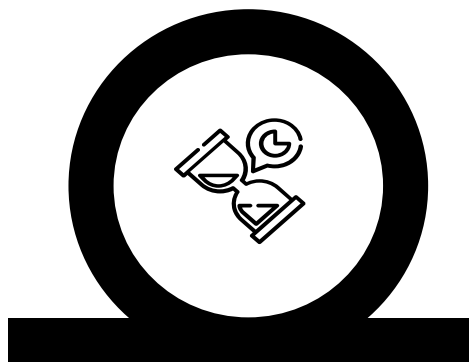


Identificadores

- 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



Definição dos Requisitos Operacionais = P0 P1 P2 P3



Qualidade dos
Atributos

- Qualidade dos atributos *eduPersonAffiliation*, *eduPersonPrimaryAffiliation* e *eduPersonScopedAffiliation*
- Apenas para afiliação de aluno, docentes e membro
- Indicar frequência de atualização após a mudança de função ou término da afiliação
- Indicar se o tempo de atualização do valor da afiliação dentro de 1 mês a 1 dia do evento que desencadeou a mudança



Definição dos Requisitos Operacionais = P0 P1 P2 P3



Verificação de Identidade
e
Gestão de Credenciais

- Registo e Acreditação
- Controlo de Verificação de Identidade (pessoal, remota, outra)
- Emissão, entrega e ativação de Credenciais
- Suspensão, revogação e reativação de Credenciais
- Renovação e substituição de Credenciais



Verificação de Identidade – Casos de Uso



Requisitos P0



- Processo de inscrição na universidade
- Inscrição realizada no portal web via auto-registo e verificação através da confirmação do contacto (e-mail, número de telefone, etc)

Requisitos P1



- Processo de Matrícula de um estudante;
- Identificação pela exibição de um documento de identidade aparentemente autêntico

Requisitos P2



- Processo de registo de um funcionário
- Identificação através da apresentação de um documento de identidade e verificação posteriores através do NIF e outros documentos

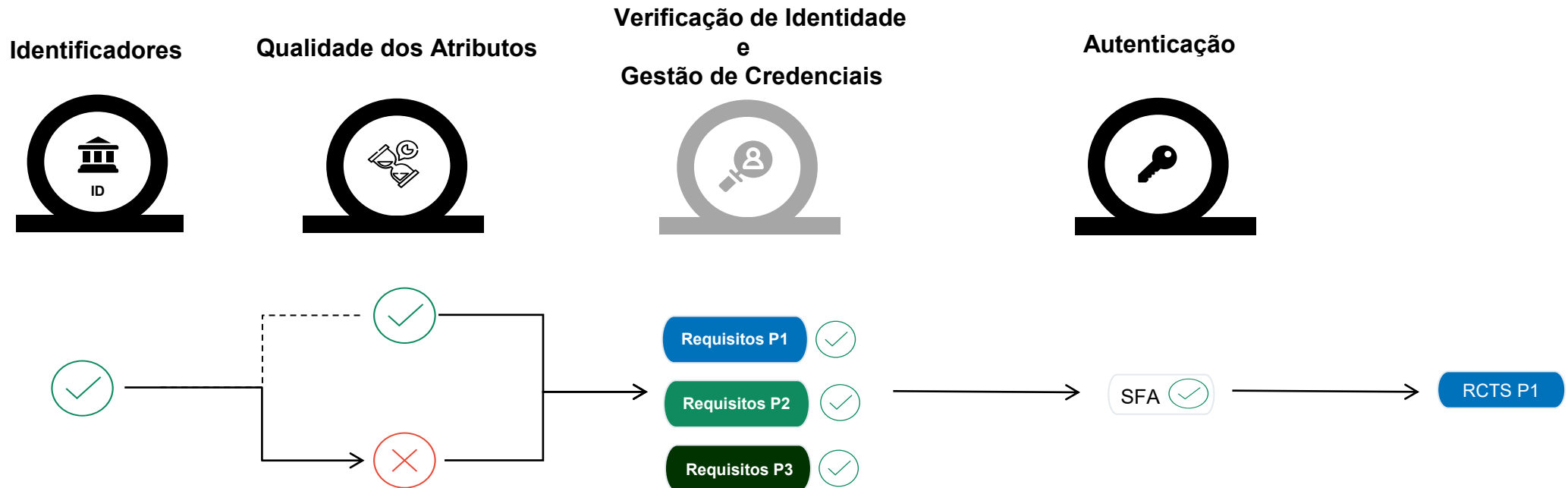
Requisitos P3



- Acesso a serviços críticos ou altamente confidenciais onde é essencial a verificação da identidade dos acessos.
- Identificação verificada através de outras credenciais como por exemplo o Chave Móvel Digital ou Cartão de Cidadão



Atribuição de Perfis – Instituições que não suportam MFA



<https://refeds.org/assurance/IAP/medium>
<https://refeds.org/assurance/cappuccino>

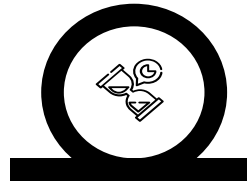


Atribuição de Perfis – Instituições que suportam MFA

Identificadores



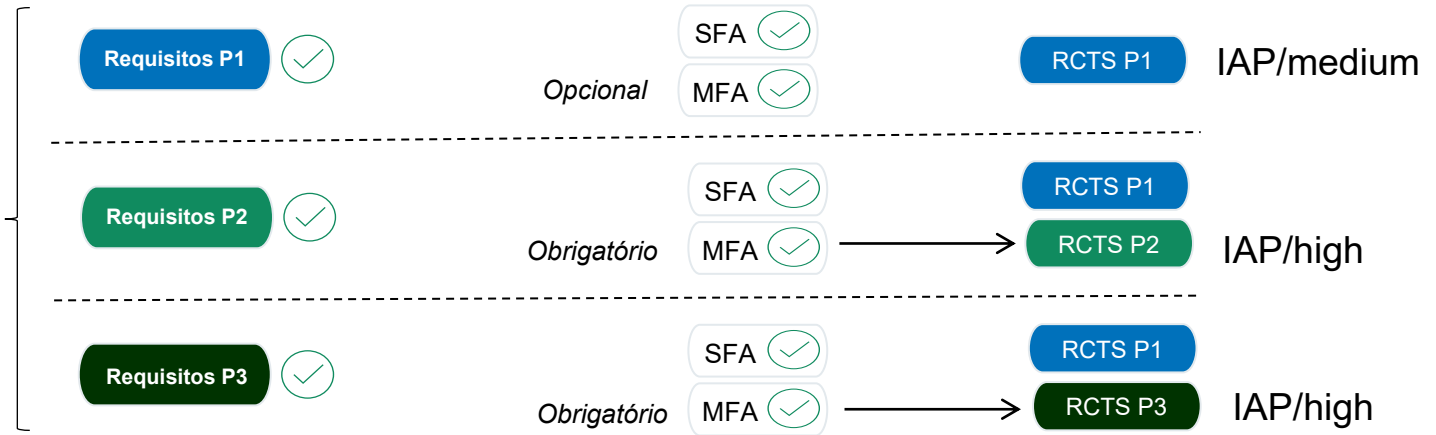
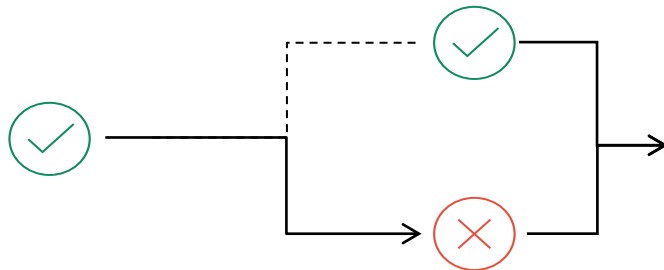
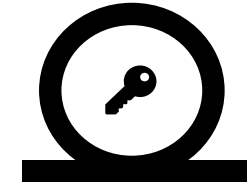
Qualidade dos Atributos



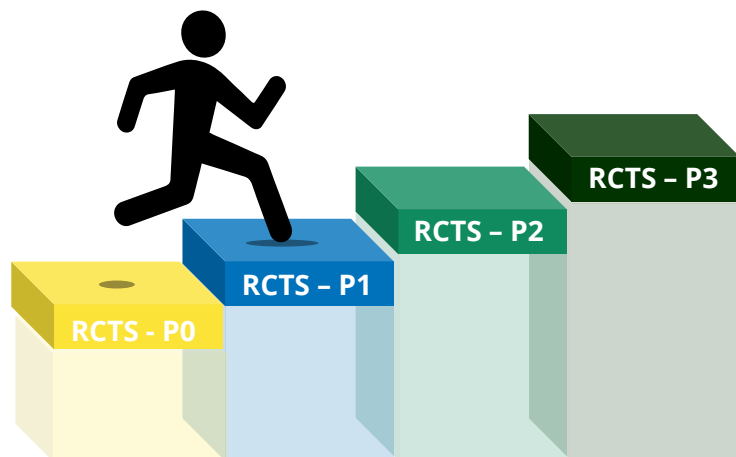
Verificação de Identidade
e
Gestão de Credenciais



Autenticação



Passos necessários para adotar os perfis



1

Declaração de Práticas de Gestão de Identidades (V2)



2

Consultar Informação dos vários perfis de Confiabilidade

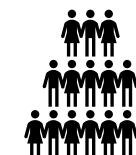


Passos necessários para adotar os perfis



3

Identificar os perfis de Confiabilidade da instituição e respetivos utilizadores que se enquadram no perfil



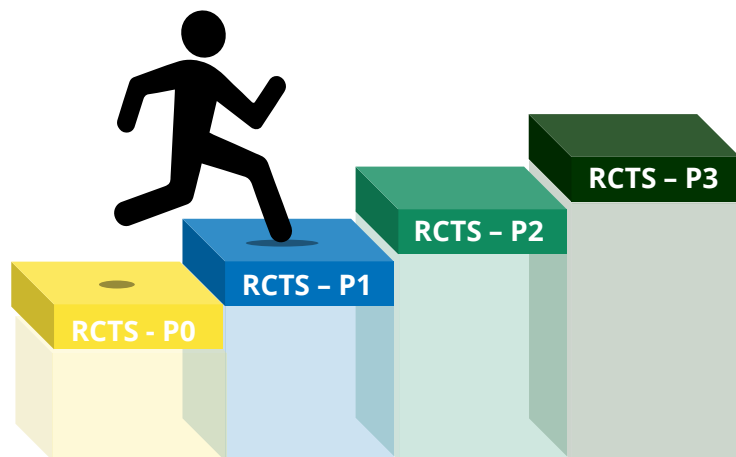
SFA ✓

RCTS P1

MFA ✓

RCTS P2

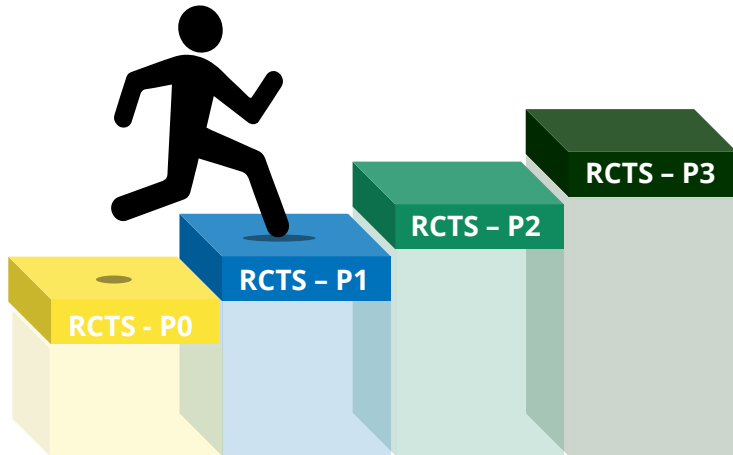
RCTS P3



Uma instituição pode ter utilizadores com vários níveis de confiança.



Passos necessários para adotar os perfis



4

A equipa de FCCN realiza várias reuniões com a instituição e realiza uma auditoria com base na Declaração de Práticas de Gestão de Identidade.



SFA ✓

RCTS P1

MFA ✓

RCTS P2

RCTS P3



FCCN | **fct**





<https://share.fccn.pt/sites/rctsaai/areatecnica/assurance/Perfis>



Reuniões de Avaliação



- ✓ Verificar que a instituição compreende os requisitos dos perfis
- ✓ Fornecer documentos de Avaliação de acordo com os perfis da instituição
- ✓ Instituição preenche documentos de Avaliação
- ✓ FCCN realiza auditoria e disponibiliza documento que reflete a avaliação realizada durante a auditoria.

3.2 REQUISITOS OPERACIONAIS

3.2.1 IDENTIFICADORES [= P0 P1 P2 P3]

[=] Os requisitos desta secção são válidos e comuns para todos os perfis RCTS-P0, RCTS-P1, RCTS-P2 e RCTS-P3.

Data	dd/mm/yyyy	Responsável
Área Funcional do Perfil de Confiabilidade	<p>7.1.1 Identificadores Permitidos</p> <ol style="list-style-type: none"> Cada FORNECEDOR DE IDENTIDADE TEM DE ter um identificador Global Único O identificador do UTILIZADOR transmitido pelo FORNECEDOR DE IDENTIDADE TEM DE ser pelo menos um dos seguintes: <ul style="list-style-type: none"> • SAML 2.0 persistent name identifier [OASIS SAML] • SAML 2.0 subject-id ou pairwise-id [OASIS SIA] • OIDC sub con type public o pairwise [OpenID.Conn] • eduPersonUniqueId [eduPerson] • eduPersonPrincipalName [eduPerson] Caso o UTILIZADOR possua mais do que um identificador único no FORNECEDOR DE IDENTIDADE, TEM DE garantir que UTILIZADOR pode escolher com qual pretende realizar a autenticação. 	
Declaração do Responsável da Instituição		
Evidência de Conformidade		
Notas do Avaliador		
Testes Realizados		
Documentação Aplicável		
Data	dd/mm/yyyy	Responsável
Área Funcional do Perfil de Confiabilidade	<p>7.1.2 Pessoa Física</p> <p>O identificador do utilizador TEM DE representar uma pessoa física afiliada com a Organização com o qual o Fornecedor de Identidade está associado.</p>	
Declaração do Responsável da		



Passos necessários para adotar os perfis



Configuração do Fornecedor de Identidade

Configurar o Fornecedor de Identidade

▲ Exemplo de configuração do atributo eduPersonAssurance com base num atributo que suporta os perfis no LDAP

Ficheiro: /opt/shibboleth-idp/conf/attribute-resolver-connectors.xml

```
<!-- Valores Estáticos RAF (Refeds Assurance Framework) Utilizados em conj
<Attribute id="refedsAssuranceFramework">
  <Value>https://refeds.org/assurance</Value>
  <Value>https://refeds.org/assurance/ID/unique</Value>
  <Value>https://refeds.org/assurance/ID/eppn-unique-no-reassign</Va
  <Value>https://refeds.org/assurance/ATP/ePA-1m</Value>
</Attribute>

<!-- RAF (Refeds Assurance Framework) e eduPersonAssurance -->
<!-- Utilizados em conjunto com o atributo filteredEduPersonAssurance
<!-- Devem estar aqui representados os perfis para os quais a institui
<Attribute id="allowedLDAPeduPersonAssurance">
  <Value>https://rctsfederation.fccn.pt/policy/assurance/rcts-p2</Va
  <Value>https://rctsfederation.fccn.pt/policy/assurance/rcts-p2</Va
  <Value>https://rctsfederation.fccn.pt/policy/assurance/rcts-p3</Va
</Attribute>

<!-- Utilizado em conjunto com o atributo eduPersonAssurance -->
<Attribute id="assuranceLevel0">
  <Value>https://rctsfederation.fccn.pt/policy/assurance/rcts-p0</Va
  <Value>https://refeds.org/assurance/IAP/low</Value>
</Attribute>
```

Ficheiro: /opt/shibboleth-idp/conf/attribute-resolver-rctsaai-core.xml

Perfis de Confiabilidade RCTS

- Perfil RCTS-P0
- Perfil RCTS - P1
- Perfil RCTS - P2
- Perfil RCTS - P3

Representação dos Valores do

Perfis

- Perfil RCTS - P0
- Perfil RCTS - P1
- Perfil RCTS - P2
- Perfil RCTS - P3

Analisar e Classificar Utilizadores

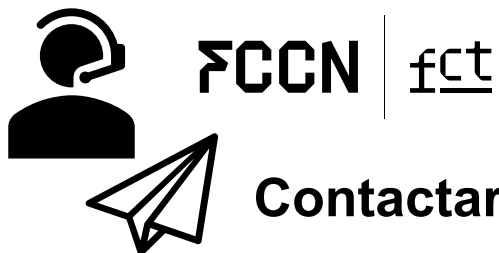
Configurar o Fornecedor de
Identidade



<https://share.fccn.pt/sites/rctsaai/areatecnica/assurance/Perfis>



Plano de Ação para 2024



Contactar os responsáveis técnicos dos Fornecedores de Identidade

- *Para cada Fornecedor de Identidade será necessário o preenchimento da nova declaração de gestão de identidades V2*
- *Avaliar os perfis em que os seus utilizadores se enquadram e fornecer documentação de avaliação*
- *Agendar auditoria e apresentar resultados*
- *Com base no resultado da auditoria realizar a respetiva configuração do IdP*



Obrigada!

Esmeralda Pires (epires@fccn.pt)
João Guerreiro (joao.guerreiro@fccn.pt)

FCCN | fct



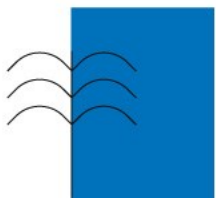
Adoção da solução privacyIDEA para Autenticação Multifactor (MFA)

Porfírio Trincheiras



EGAS MONIZ SCHOOL
of HEALTH & SCIENCE

jornadas.fccn.pt





privacyID3A

AUTHENTICATION SYSTEM



Porque escolhemos o privacyIDEA

1

**Opensource /
GNU AGPL**

2

**Grande utilização
na academia**

3

**Várias integrações
pré-disponíveis**



Utilização académica

caso de uso

130 000 utilizadores

EduVPN + shibboleth + privacyIDEA

Munique, Alemanha

Construir uma solução VPN multi-instituto para a comunidade de 130.000 utilizadores de Munique
Universidade Técnica de Munique tum.de TUM
Universidade Ludwig Maximilian de Munique lmu.de LMU
HM Hochschule München Universidade de Ciências Aplicadas de Munique hm.edu
Universidade de Ciências Aplicadas de Weihenstephan-Triesdorf hswt.de

<https://www.eduvpn.org/eduvpn-deployment-at-the-leibniz-supercomputing-centre/> 



Integração com fabricantes

- Integração via freeradius
- Integração com suporte de fabricantes

The screenshot shows the Aruba ClearPass Guest Administration interface. The left sidebar contains a navigation menu with categories like Guest, Devices, Onboard, Configuration, and Administration. The main content area is titled 'Install Extension' and includes a search bar with the value 'a9793039-ddd7-4867-b6ee-1e28ff238834'. Below the search bar is a table with columns for Name, Version, and State. One entry is visible: 'P...IDEA Authentication' with version '1.0.0' and state 'Not installed'. A circular callout highlights the 'Install' button for this entry.

Name	Version	State
P...IDEA Authentication	1.0.0	Not installed



Instalação e configuração

Ubuntu 22 LTS

```
# wget https://lancelot.netknights.it/NetKnights-Release.asc
# mv NetKnights-Release.asc /etc/apt/trusted.gpg.d/
# add-apt-repository http://lancelot.netknights.it/community/jammy/stable
# apt update
# apt install privacyidea-apache2
# pi-manage admin add admin -e admin@localhost
```



Configuração

PrivacyIDEA

Config > System > System Config

- Use @ sign to split the username and the realm.
- Increase the failcounter if the wrong PIN was entered.
- Prepend the PIN in front of the OTP value. Otherwise it will be post pended.
- Include SAML attributes in the authentication response.

The screenshot displays the PrivacyIDEA System Configuration page. The left sidebar contains a navigation menu with options like 'System Config', 'Get System Documentation', 'SMTP servers', 'RADIUS servers', 'privacyIDEA servers', 'SMS Gateways', 'Tokengroups', 'Service IDs', and 'CAS'. The main content area is divided into several sections:

- General Settings:** Includes checkboxes for 'Use @ sign to split the username and the realm.', 'Increase the failcounter if the wrong PIN was entered.', 'Prepend the PIN in front of the OTP value . Otherwise it will be post pended.', and 'Include SAML attributes in the authentication response.' There is also a text input for 'Clear failcounter after minutes' set to 1440.
- Advanced Settings:** Includes checkboxes for 'Do not use an authentication counter per token.', 'Include SAML attributes even if the user failed to authenticate.', and 'Automatic resync during authentication'.
- Timeouts and Cache:** Includes text inputs for 'Auto resync timeout' (300), 'User Cache expiration in seconds' (86400), and 'Override Authorization Clients' (127.0.0.1, 10.0.0.8).
- SMTP Configuration:** Includes a dropdown menu for 'SMTP server for password recovery' with the instruction 'Select a predefined SMTP server configuration.'
- Token Settings:** Includes text inputs for 'OTP length of newly enrolled tokens' (6), 'Count Window of newly enrolled tokens' (10), 'Max Failcount of newly enrolled tokens' (10), 'Sync Window of newly enrolled tokens' (1000), and 'The challenge validity time' (+∞).



Configuração

PrivacyIDEA

Realms > All Realms > + create realm

Default	Realm name	resolvers
<input type="button" value="set Default"/>	defrealm	deflocal [] (passwdresolver) <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	egasmoniz.edu.pt	Egasmoniz.edu.pt [] (ldapresolver) <input type="button" value="Edit"/> <input type="button" value="Delete"/>
	<input type="text" value="new realm"/>	<input type="checkbox"/> Egasmoniz.edu.pt (ldapresolver) <input type="checkbox"/> deflocal (passwdresolver) <input type="button" value="Create realm"/>



Configuração

PrivacyIDEA

Realms > All Realms > create realm > new LDAP resolver

All Resolvers

New Resolvers

New passwordresolver

New ldapresolver

New sgresolver

New samesolver

New htresolver

[Help about UserResolver](#)

Edit LDAP Resolver Egasmoniz.edu.pt

Resolver name:

Server URI:

Pooling strategy:

STARTTLS: Use STARTTLS on a plain LDAP connection usually on port 389.

Base DN: Scope:

Bind Type:

Bind DN:

Bind Password:

Timeout (seconds): Cache Timeout (seconds):

Size Limit:

Server pool retry rounds: Server pool skip timeout (seconds):

Per process server pool: This setting activates a LDAP server pool that is persisted between requests.

Edit user store: The user data in this database can be modified from within privacyIDEA.

Fixed OpenLDAP **Fixed Active Directory**

Logname Attribute:

Search Filter:

Attribute mapping:

Multivalued Attributes:

UID Type:



Configuração

PrivacyIDEA

Tokens > Enroll Token

HOTP: Event based One Time Passwords.

The screenshot shows the 'Enroll a new token' page in the PrivacyIDEA web interface. The navigation bar at the top includes 'Tokens', 'Users', 'Machines', 'Config', 'Audit', and 'Components'. The left sidebar has 'All tokens' selected, with 'Enroll Token' highlighted. The main content area features a dropdown menu with 'HOTP: Event based One Time Passwords' selected. Below the dropdown are input fields for 'Username', 'PIN/Password', and 'Extended Attributes', and an 'Enroll Token' button.



Configuração

PrivacyIDEA




 **Policies > All policies**

System
Policies
Events
Periodic Tasks
Tokens
Machines
Users
Realms

All Policies

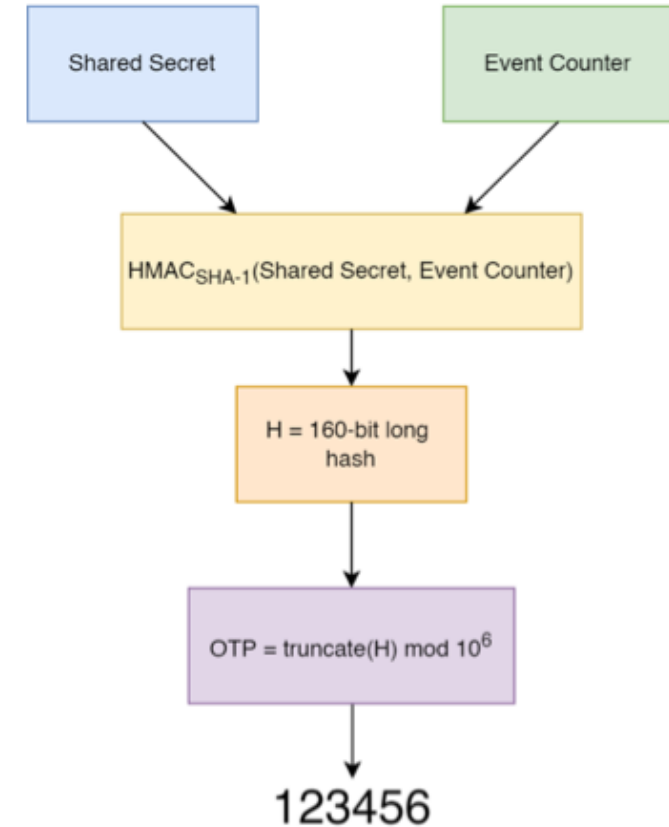
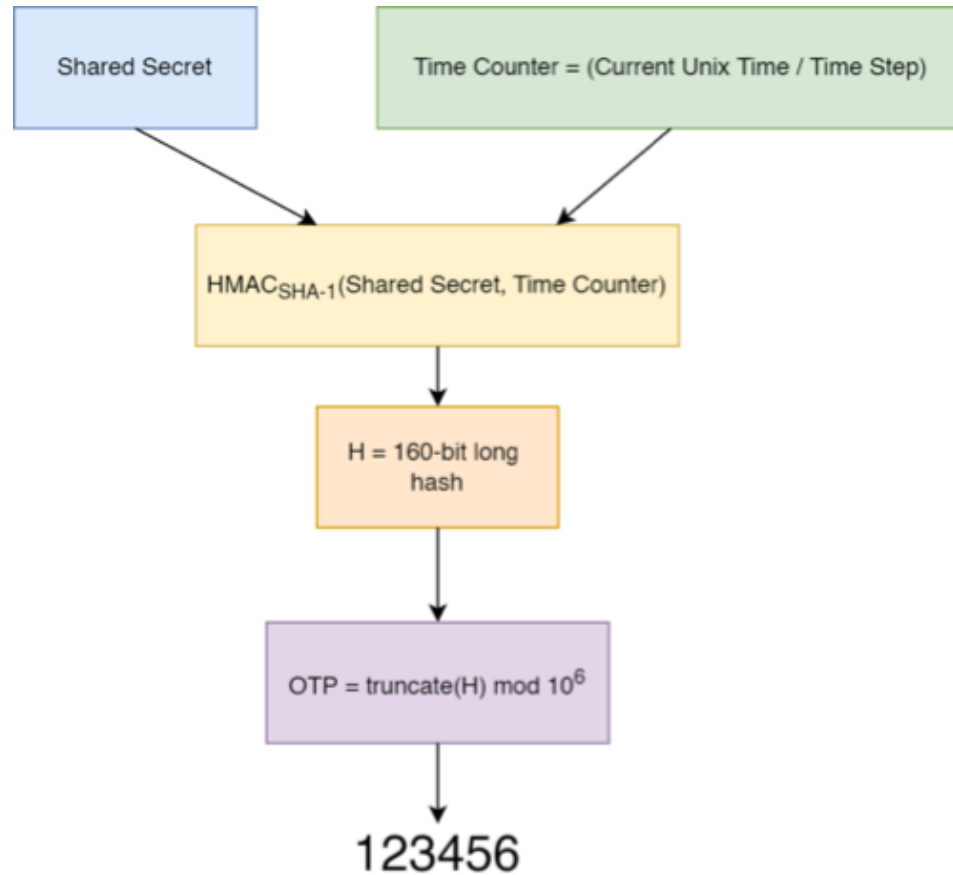
Create new Policy

[Help about Policies](#)

Priority	Active	Policy Name	Scope	Action	Realm	User	Resolver	Client	
1	✓	enroll_tokenlabel	enrollment	max_token_per_user: 3 tokenissuer: EgasMoniz tokenlabel: <u>@</u>/<s>	0	0	0	0	 Delete
1	✓	LIMIT_TOKEN_TYPES	user	delete: true enrollHOTP: true enrollTOTP: true totp_timestep: 60	0	0	0	0	 Delete
1	✓	hide_welcome	webui	hide_welcome_info: true	0	0	0	0	 Delete



TOTP vs HOTP



Fonte das imagens <https://rublon.com/blog/hotp-totp-difference/>





Integração Idp SimpleSAML

Integração como AuthProc

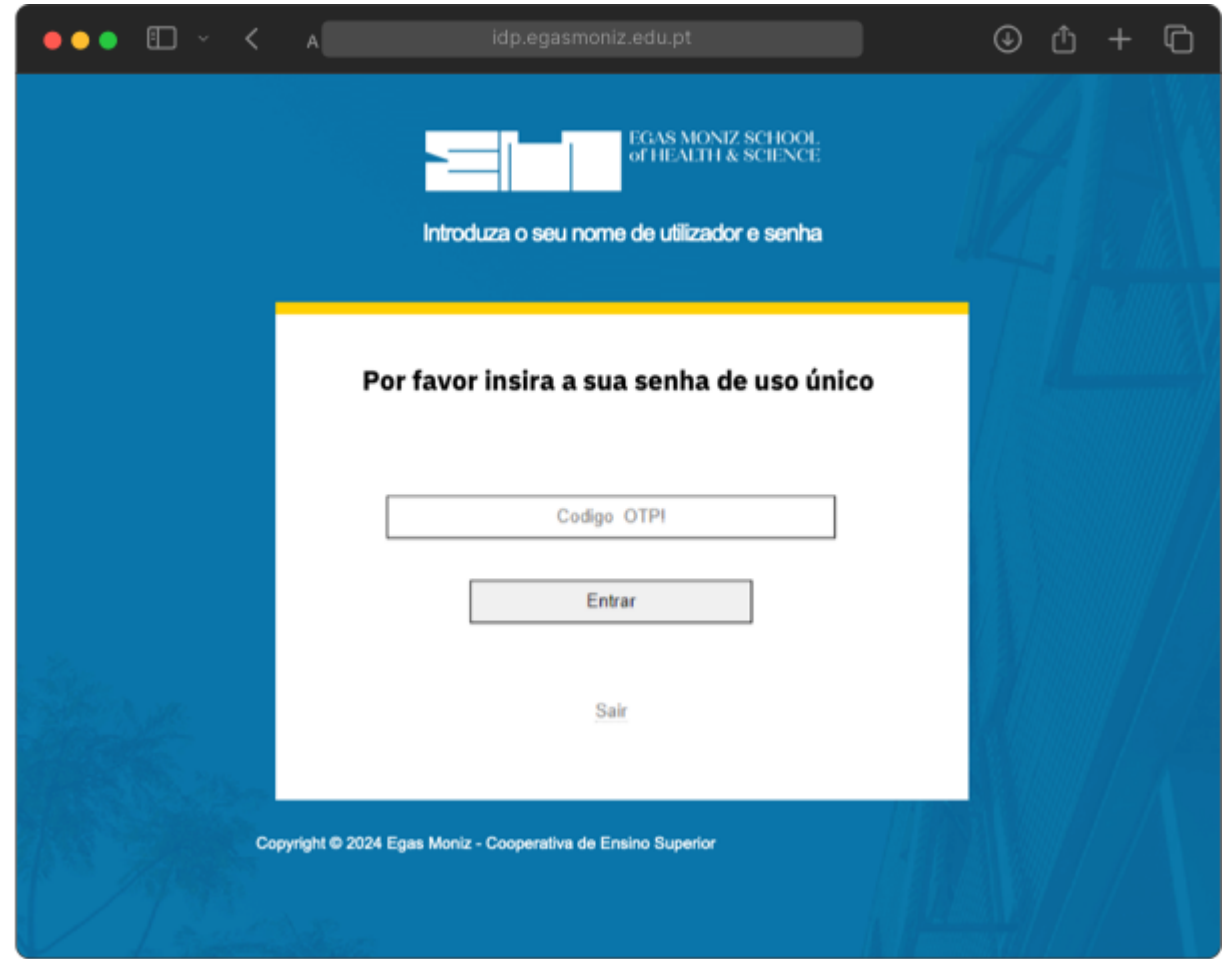
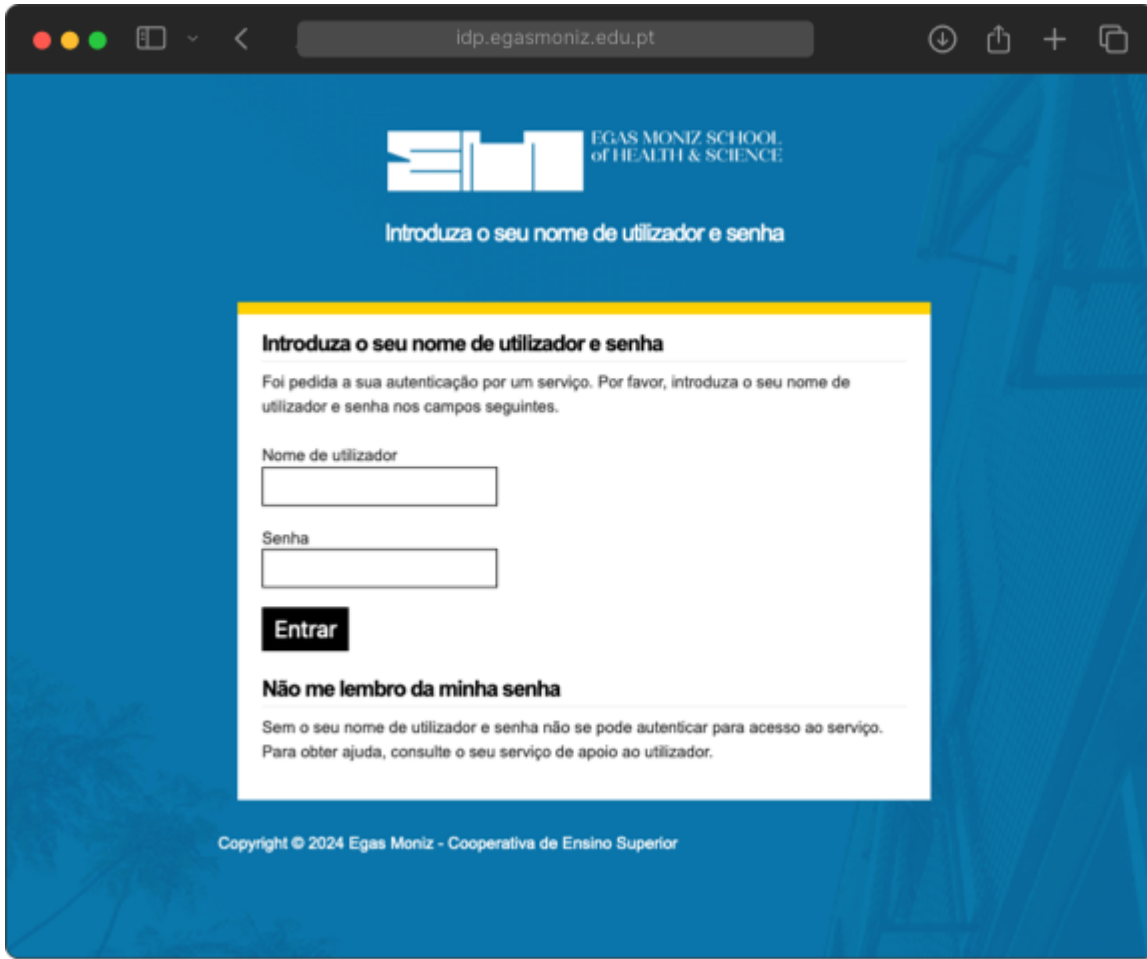
```
#composer require privacyidea/simplesamlphp-module-privacyidea
```

```
39 = array(
    'class'=> 'privacyidea: PrivacyideaAuthProc' ,
    'privacyideaServerURL' => 'https://mfa.egasmoniz.edu.pt' ,
    'realm'=> 'egasmoniz.edu.pt' ,
    'uidKey'=> 'SAMAccountName' ,
    'sslverifyhost' => false,
    'sslverifypeer' => false,
    'serviceAccount' => 'idp',
    'servicePass'=> *****
    'SSO' = 'true',
    'otpFieldHint' => 'Codigo OTP!',
    'excludeClientIPs' => array("10.0.0.0-10.255.255.255"),
    # 'doEnrollToken' => 'true',
    # 'typeOfTokenToEnroll' => 'totp',
),
```





Integração Idp SimpleSAML





Integração Idp shibboleth

Shibboleth 3

<https://github.com/wraezor/privacyIDEA-shibboleth-tfa> 

Shibboleth 4 e 5

<https://github.com/privacyidea/shibboleth-plugin> 

Outros

<https://github.com/privacyidea> 





Integração OpenVPN

OpenVPN 2.6

<https://pam-python.sourceforge.net/> 

https://github.com/privacyidea/pam_python 





Integração OpenVPN

Client.ovpn

```
#AD/PASSWORD AUTENTICATION
seten CLIENT_CERT 0
auth-user-pass
auth-nocache
static-challenge "Código de Segurança OTP" 1
```

/etc/pam.d/openvpnotp

```
IW /etc/pam. d/openvpnotp
account required pam_permit.so
auth [success=1 default=ignore] pam_python.so /us/src/pam_python/privacyidea_pam.py url=https://mfa.egasmoniz.edu.pt authtok_prompt=pin
auth requisite pam_deny.so
auth required pam_permit.so
auth required pam_winbind. so debug
```

Server.conf

```
username-as-common-name
client-config-dir /etc/openvpn/ccd
#plugin /usr/lib/x86_64-linux-gnu/openvpn/plugins/openvpn-plugin-auth-pam.so openvpn
plugin /us/lib/x86_64-linux-gnu/openvpn/plugins/openvpn-plugin-auth-pam.so "openvpnotp login USERNAME password PASSWORD pin OTP"
```





Integração OpenVPN

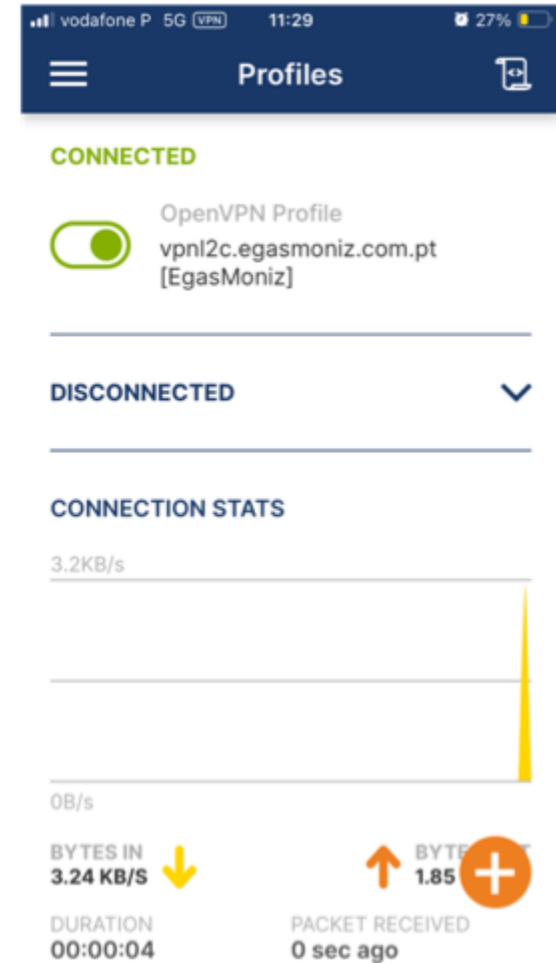
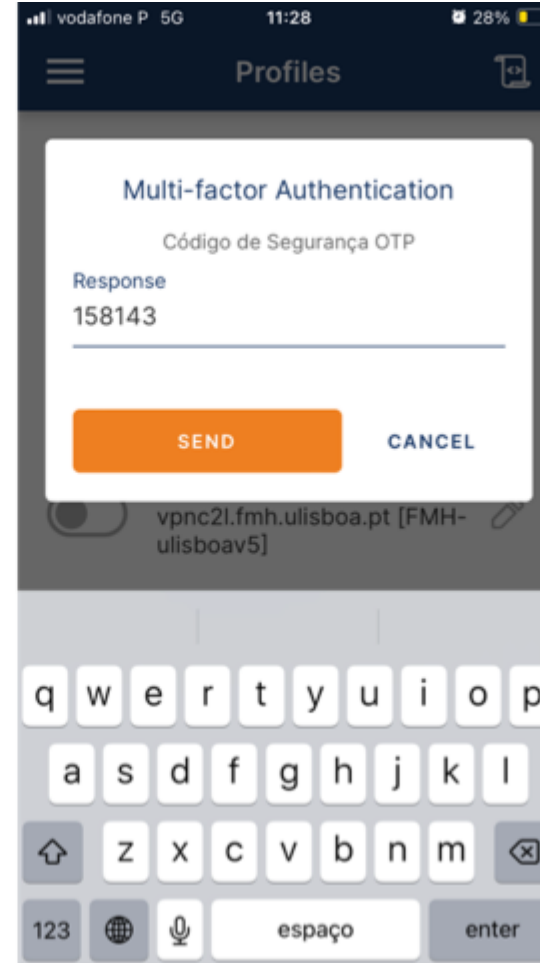
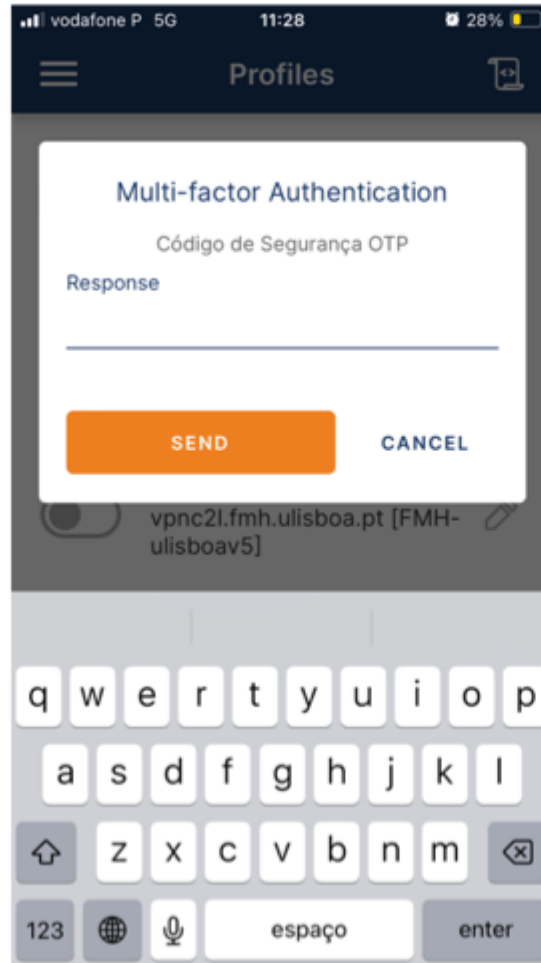
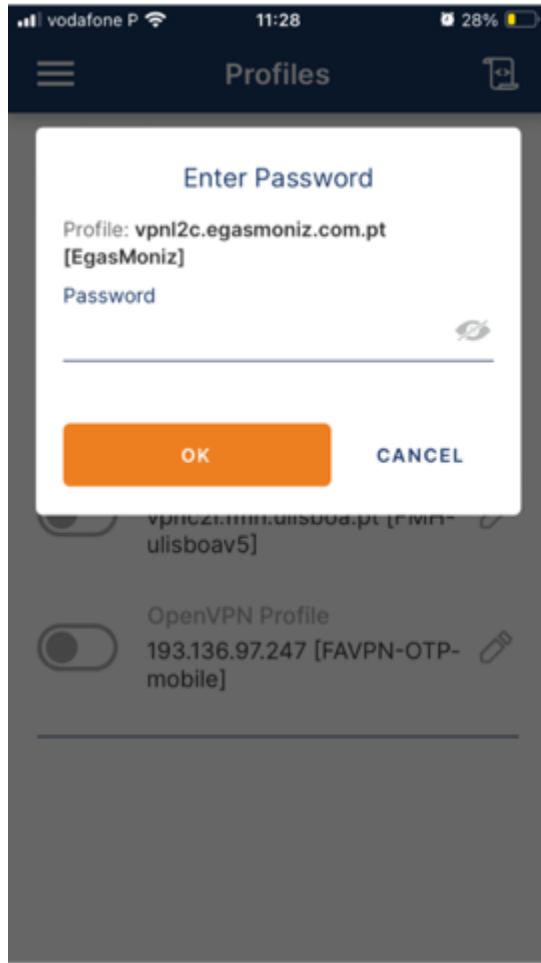
```
I A openvpn-2.6.3/src/plugins/auth-pam/auth-pam.c (c) my_conv(int n, const struct pam message **msg_array,
if (strstr(match_value, "USERNAME") )
{
    aresp[il- resp = searchandreplace (match_value, "USERNAME", up->username) ;
}
else if (stistI(match_value, "PASSWORD")){
    {
        aresp[i].resp = searchandreplace (match_value, "PASSWORD", up->password) ;
    }
else if (strstI (match_value, "COMMONNAME") )
    {
        aresp[11.resp = searchandreplace (match_value, "COMMONNAME", up->common
_name) ;
    }
else if (stistr (match_value, "OTP"))
    {
        aresp [t] .resp = searchandreplace (match_value, "OTP", up->response) :
    }
else
    {
        aresp[il.resp = strdup (match_value) ;
    }
if (aresp [i] .resp == NULL)
    {
        ret = PAM_CONV_ERR;
    }
}
```

```
I A /usr/src/pam python/privacyidea pam.py (pyth
def pam_sm_authenticate (pamh, flags, argv) :
config = _get_config(argv)
debug = config.get("debug")
try_first_pass = config.get ("try_first_Pass")
prompt = config.get ("prompt", "pin")
if prompt [-1] != ":" :
    prompt += ":"
rval = pamh.PAM_AUTH_ERR
syslog.openlog(facility=syslog.LOG_AUTH)
```





Integração OpenVPN



Integração legacy webapps

```
function authenticate($args = array())
{
    $params = array("user" => $args['user'],
        "pass" => filter_input(INPUT_POST, 'otp')
    );

    if ($this->rcmail->config->get('privacyidea_api_realm')) {
        $params["realm"] = $this->rcmail->config->get('privacyidea_api_realm');
    }




    $ch = curl_init();
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, 0);
    curl_setopt($ch, CURLOPT_URL, $this->rcmail->config->get('privacyidea_api_url'));
    curl_setopt($ch, CURLOPT_POST, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, http_build_query($params));
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    $res = curl_exec($ch);

    if ( $res === false ) {
        $args['abort'] = true;
        $args['error'] = curl_error($ch);
        curl_close($ch);
        return $args;
    }

    curl_close($ch);
    $js = json_decode($res);

    if ( $js === null && json_last_error() !== JSON_ERROR_NONE ) {
        $args['abort'] = true;
        $args['error'] = json_last_error();
        return $args;
    }

    if ( $js->(result)->(status) === TRUE && $js->(result)->(value) === TRUE ) {
        return $args;
    } else {
        $args['abort'] = true;
        $args['error'] = $js->(detail)->(message);
        return $args;
    }
}
```

	Utilizador
	Senha
	One-time password
ENTRAR	



Vista de utilizador gerar token

All tokens

Enroll Token

Help about Tokentypes

Enroll a new token

TOTP: Time based One Time Passwords.

The TOTP token is a time based token. You can paste a secret key or have the server generate the secret and scan the QR code with a smartphone app like the privacyIDEAAuthenticator turning your smartphone into an authentication device. You can also use other authenticator apps like Google Authenticator, Microsoft Authenticator, Authy or FreeOTP. But note, that these might have limitations in the supported hash algorithms or other parameters.

Token data

Generate OTP Key on the Server

The server will create the OTP key and a QR Code will be displayed to you to be scanned.

OTP length

6
>

Some Authenticator Apps only support an OTP length of 6.

Hash algorithm

sha1
>

Some Authenticator Apps only support the SHA1 algorithm.

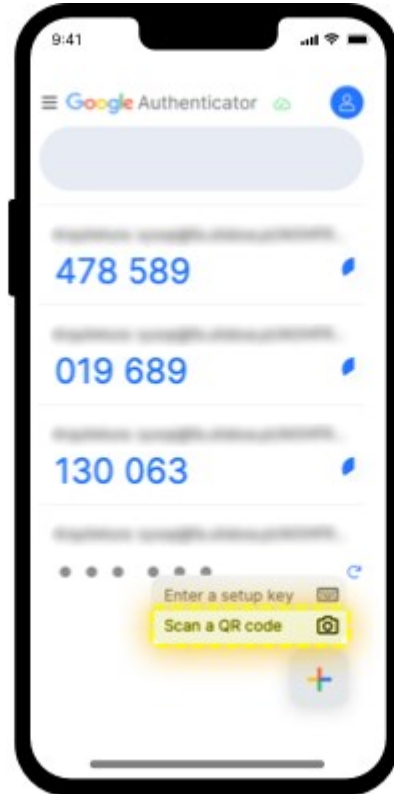
Enroll Token



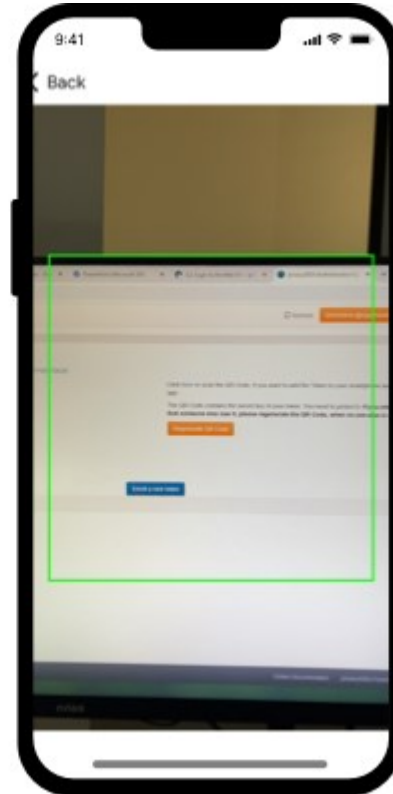
Vista de utilizador gerar token



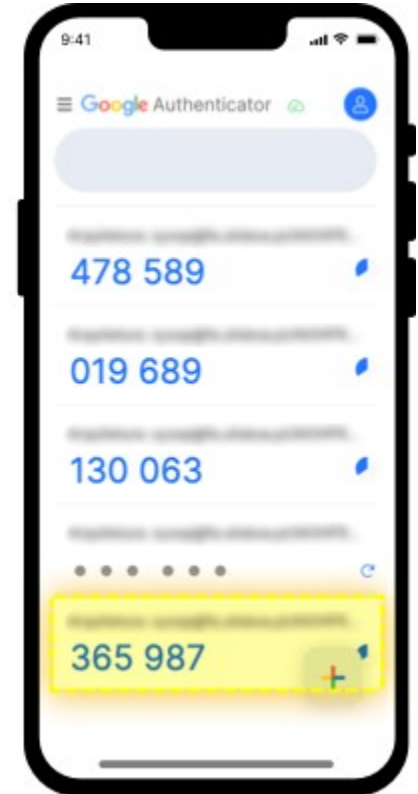
>>



>>



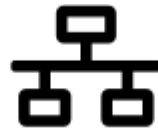
>>



Dificuldades e desafios sentidos durante a passagem a produção na EgasMoniz



Explicar a necessidade imperiosa de ter 2FA



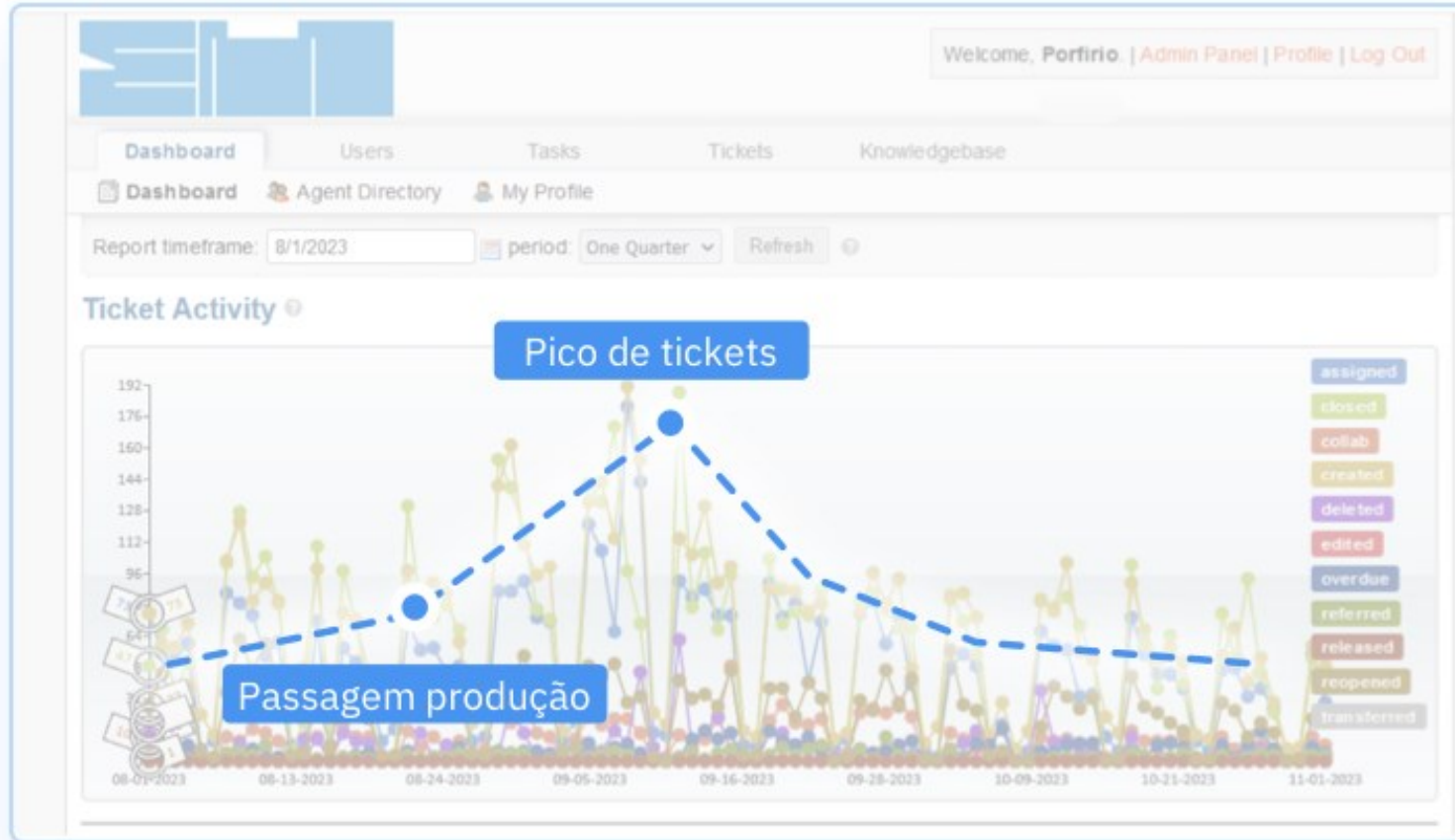
Distribuição inicial de tokens



Capacidade das equipas de suporte



Dificuldades e desafios sentidos durante a passagem a produção na EgasMoniz



Resultados obtidos após 8 meses de utilização

6033

tokens gerados



Resultados obtidos após 8 meses de utilização

Q Log

First Previous 5 6 7 8 9 10 11 12 13 14 Next Last

Download 411082 entries found.

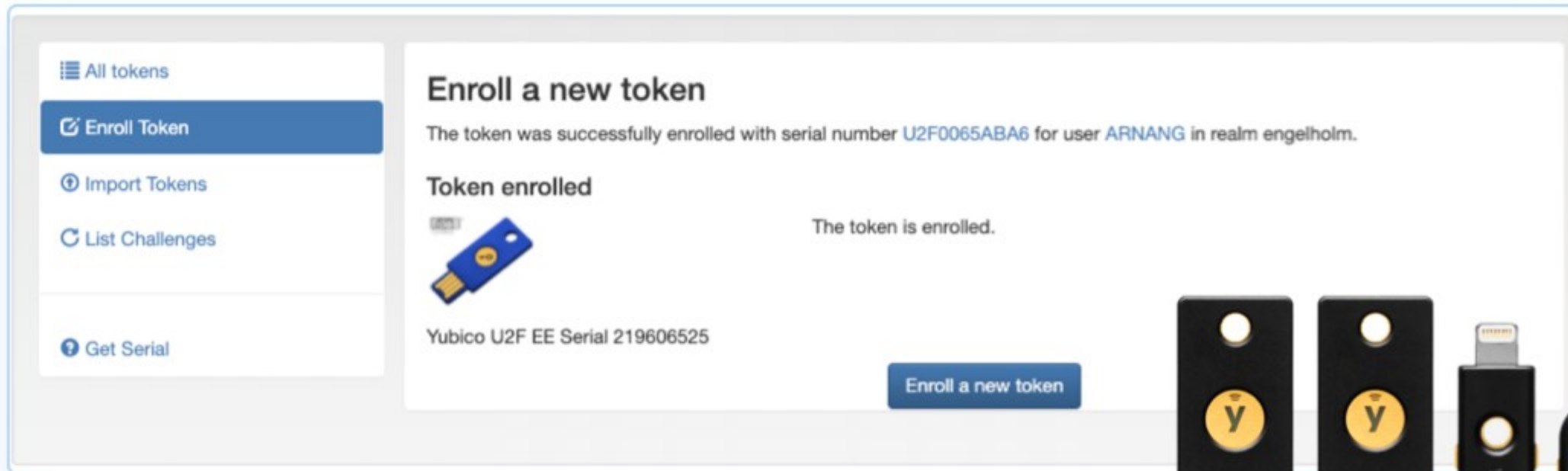
number	startdate	enddate	duration	action	success	action detail	serial	token type	administrator	user	realm	resolver	policies	client	info	sig_check	mit
410992	2024-03-26 12:20:08	2024-03-26 12:20:08	0.245328	POST /validate/check	1		TOTP05040424	totp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410991	2024-03-26 12:20:04	2024-03-26 12:20:04	0.230911	POST /validate/check	1		OATH4657669F	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410990	2024-03-26 12:19:54	2024-03-26 12:19:54	0.441811	POST /validate/check	1		OATH0041C013	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410989	2024-03-26 12:19:19	2024-03-26 12:19:19	0.221934	POST /validate/check	1		OATH42299E4B	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410988	2024-03-26 12:19:15	2024-03-26 12:19:16	0.211237	POST /validate/check	1		OATH0514FC90	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410987	2024-03-26 12:16:00	2024-03-26 12:16:01	0.43985	POST /validate/check	1		OATH0215FE91	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410986	2024-03-26 12:15:57	2024-03-26 12:15:57	0.214191	POST /validate/check	1		OATH02134A75	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK
410985	2024-03-26 12:15:42	2024-03-26 12:15:43	0.536303	POST /validate/check	1		OATH0604D7B2	hotp			egasmoniz.edu.pt	Egasmoniz.edu.pt		10.0.192.41	matching 1 tokens	OK	OK

Capacidades de auditar o sistema, mantendo um registo de todas as ações ocorridas.

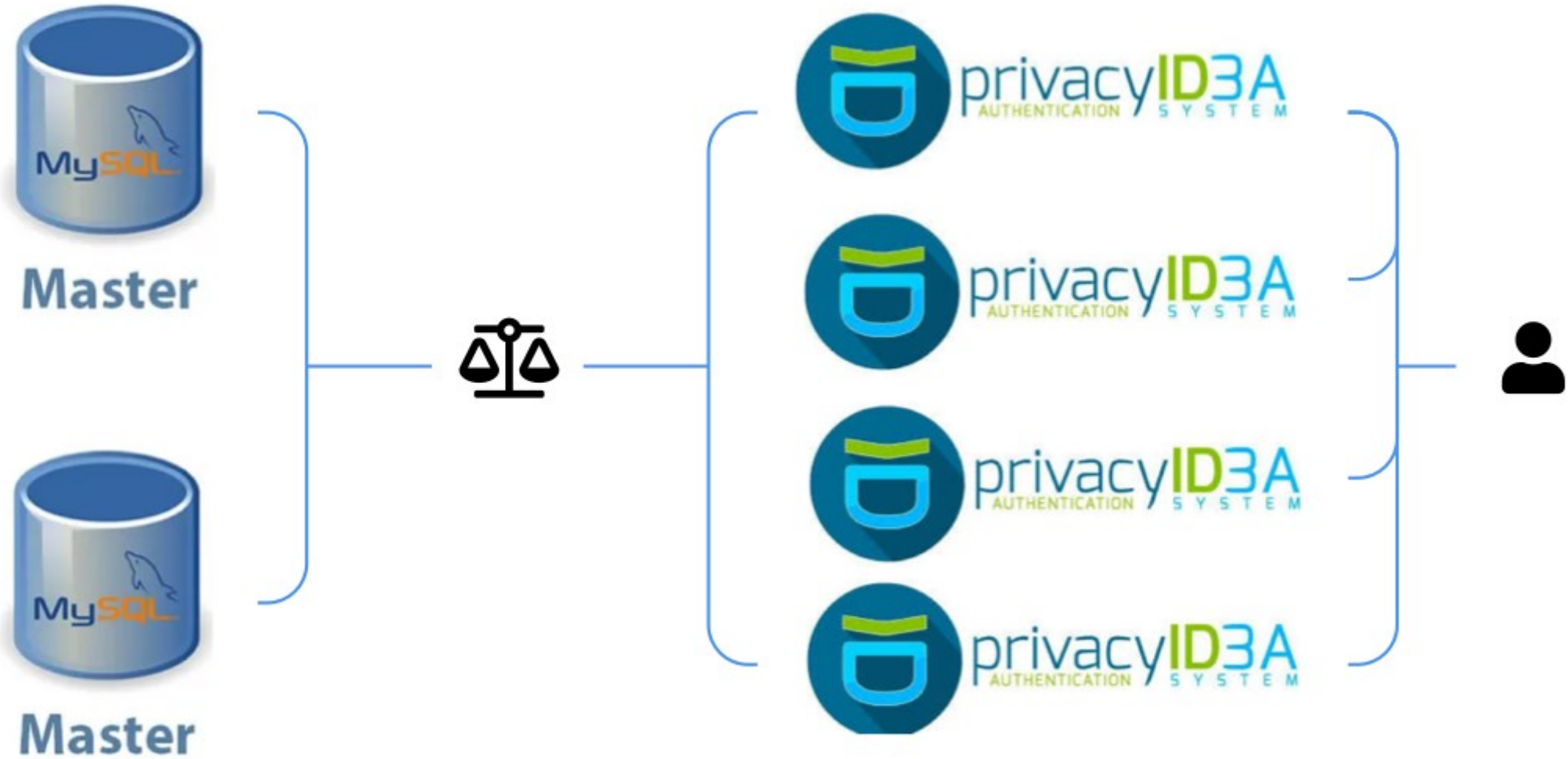


Outras possibilidades de utilização e evolução futura

- Migração para Push-Based Authentication, mais seguro e resistente a phishing
- Utilização de token u2f para aplicações com requisitos de segurança mais elevado



Cenário possível de escalabilidade, failover e redundância



Cenário possível de escalabilidade, múltiplos resolvers

The screenshot displays the OpenAM administration console interface for configuring a User Resolver. The top navigation bar includes tabs for System, Policies, Events, Periodic Tasks, Tokens, Machines, Users, Realms, and CAs. The left sidebar shows a menu for 'All Resolvers' and 'New Resolvers' with options for various resolver types, where 'New httpresolver' is currently selected. The main content area is titled 'Edit HTTP Resolver Escola1' and contains the following configuration fields:

- Resolver name:** Escola1
- Endpoint (URL):** https://escola1.universidade.pt/endpoint
- Method:** POST
- Request Mapping (JSON format):** {"customerid": "{userid}", "accessKey": "secr3t!"}
- Headers (JSON format):** {"Content-Type": "application/json, charset=UTF-8"}
- Response Mapping (JSON format):** {"username": "{Username}", "email": "{Email}"}
- Special Error Handling:**

At the bottom right, there is a 'Test HTTP Resolver' button with a text input field containing 'foo@bar.com', and a 'Save resolver' button.



Cenário possível de escalabilidade, múltiplos resolvers

All Realms	Default	Realm name	resolvers		
Clear default realm	set Default	escola1.universidade.pt	escola1 [] (passwdresolver)	Edit	Delete
Help about Realms	set Default	escola2.universidade.pt	escola2 [] (passwdresolver)	Edit	Delete
	set Default	escola3.universidade.pt	escola3 [] (passwdresolver)	Edit	Delete



Cenário possível de escalabilidade, e múltiplas realms

All Realms	Default	Realm name	resolvers		
Clear default realm	set Default	escola1.universidade.pt	escola1 [] (passwdresolver)	Edit	Delete
	set Default	escola2.universidade.pt	escola2 [] (passwdresolver)	Edit	Delete
Help about Realms	set Default	escola3.universidade.pt	escola3 [] (passwdresolver)	Edit	Delete



Jornadas
— FCCN

 **PAESSLER**
THE MONITORING EXPERTS

 **SYSCRUM**

Monitorização de Infraestruturas

Válter Veiga, SYSCRUM

Membro 28917 - Ordem dos Engenheiros Técnicos

15 Abril 2024

jornadas.fccn.pt



FCCN
serviços digitais fct

fct Fundação
para a Ciência
e a Tecnologia

 **arditi** agência regional para o
desenvolvimento da investigação
tecnológica e inovação

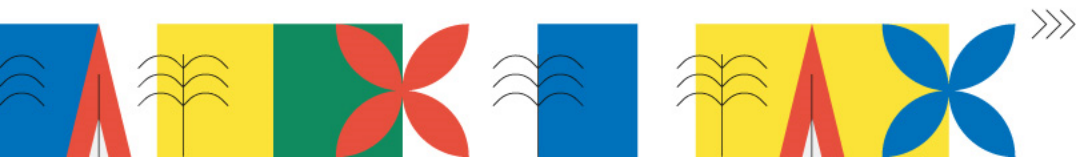
 **SIH**

 **UNIVERSIDADE da MADEIRA**

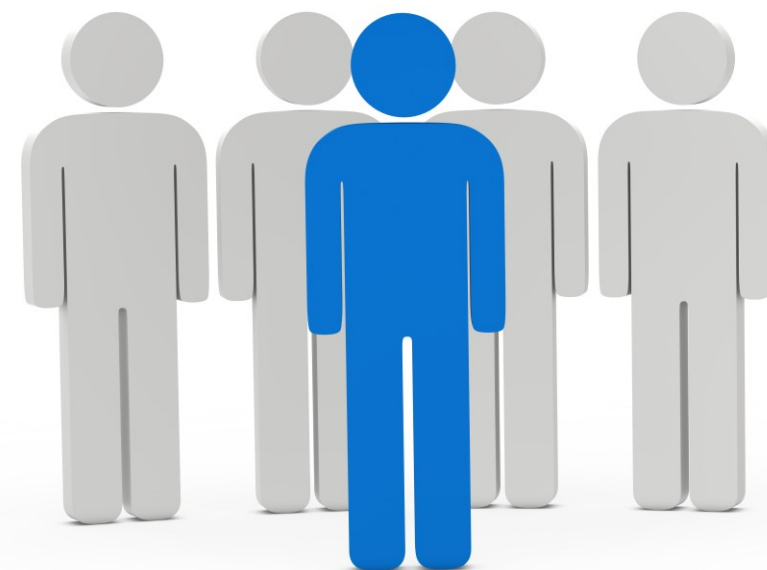


Esperança ou Certeza

jornadas.fccn.pt

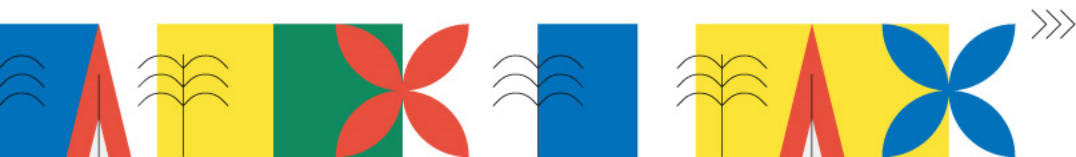


Quem Somos



Quais as nossas competências

jornadas.fccn.pt



Quem Somos



Extreme Networks
Gold Partner

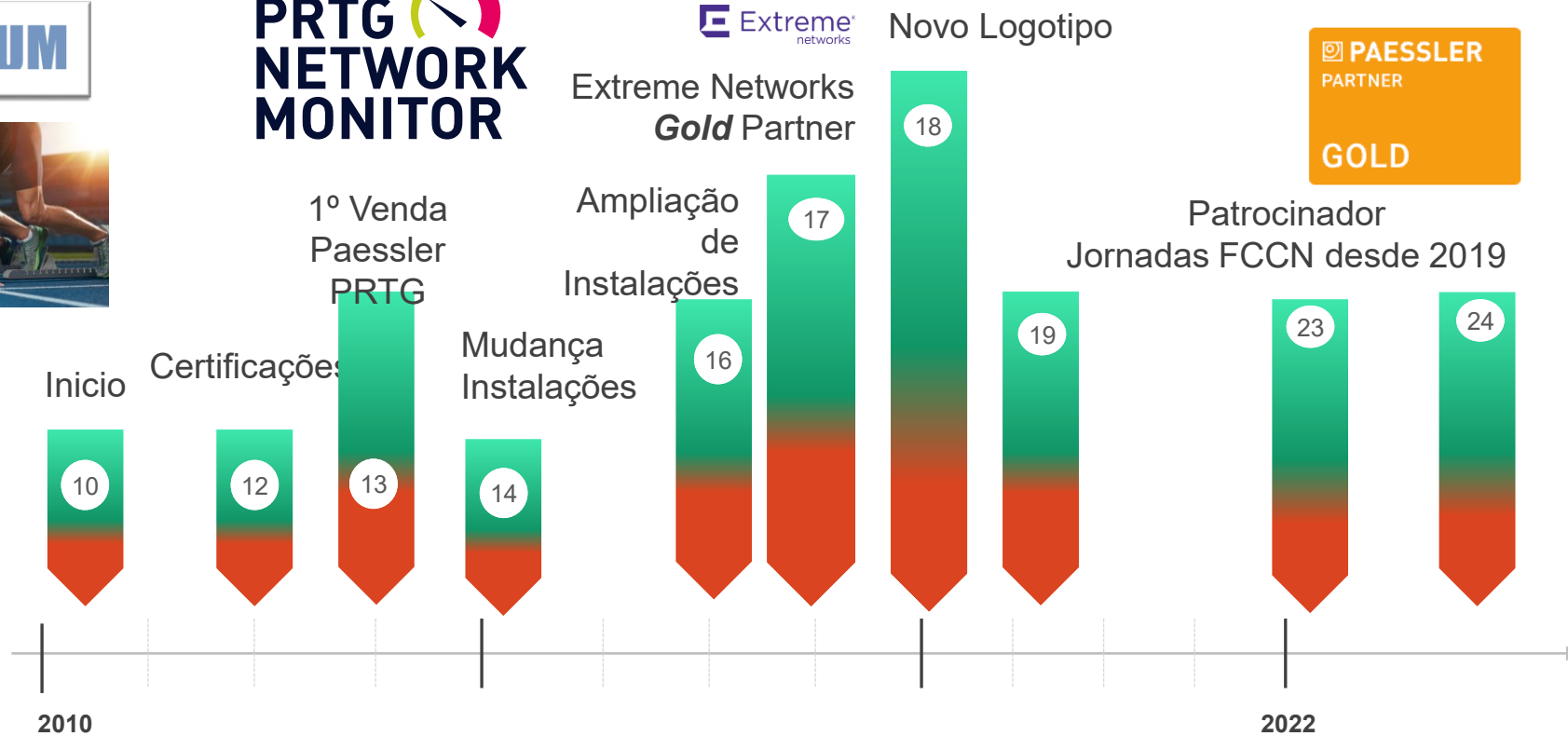
Novo Logotipo



Patrocinador
Jornadas FCCN desde 2019



PAESSLER
Gold Partner

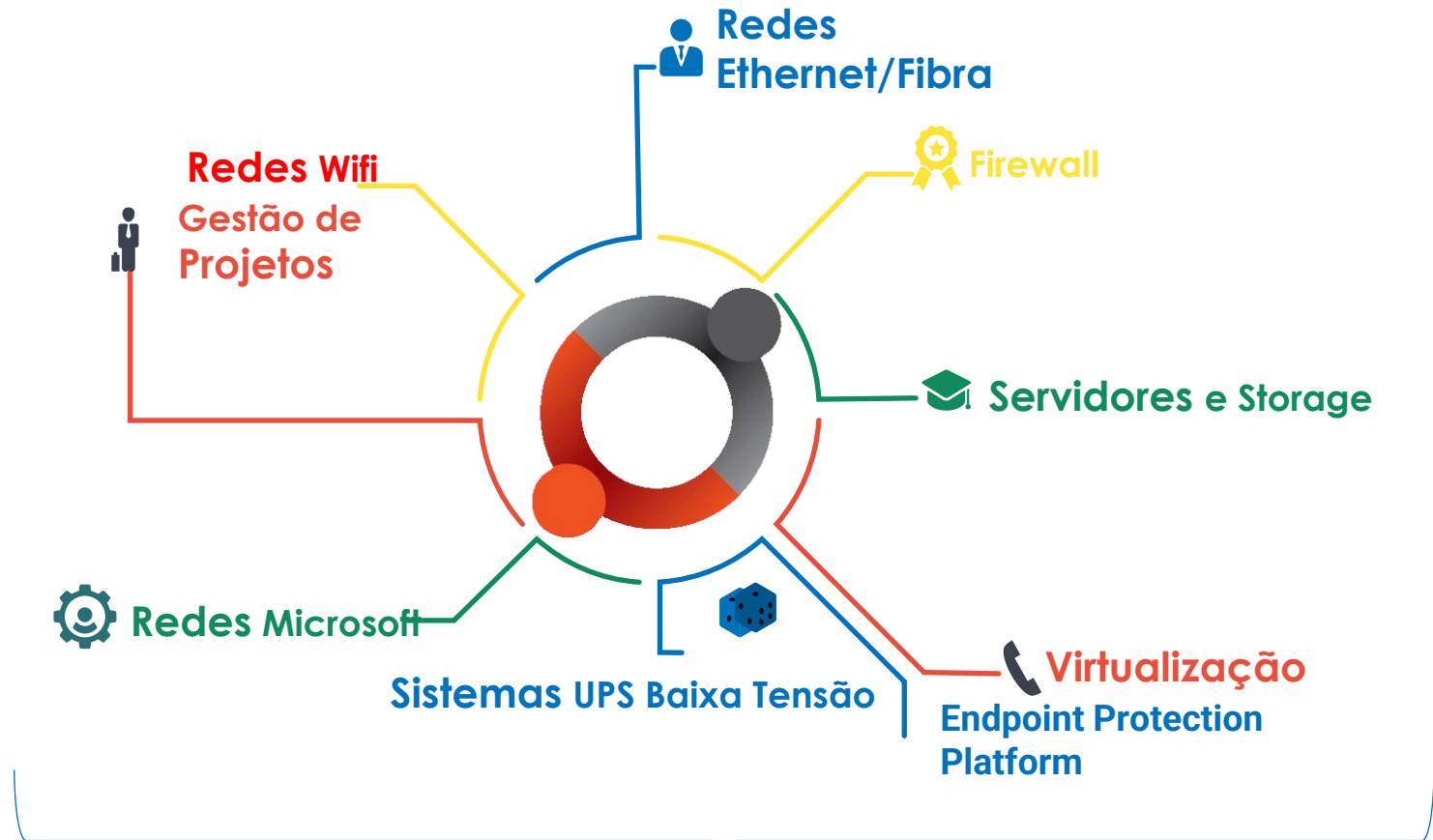


2010 - 2013
A mais longa e severa das crises

 **PAESSLER**
THE MONITORING EXPERTS

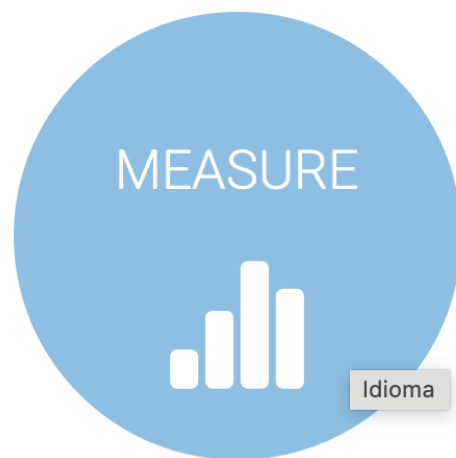


SYSCRUM Competências



Monitorizar





- Over 350 employees from over 25 countries
- US is the largest market, followed by DACH, UK and Benelux
- Companies of all sizes and industries
- 70% of Fortune 100 companies worldwide use PRTG
- A leader in IT, OT and IoT monitoring with more than 500,000 users of:

“THE
MONITORING
EXPERTS”

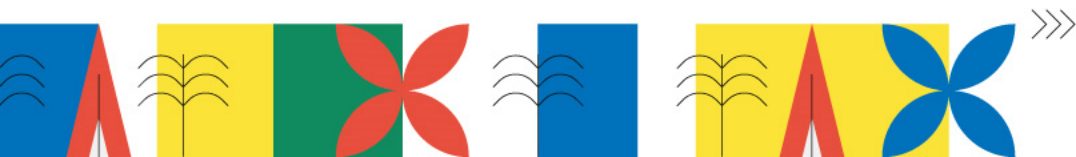
Founded in 1997
by Dirk Paessler

PAESSLER
PRTG
NETWORK
MONITOR

PAESSLER
PRTG
HOSTED
MONITOR

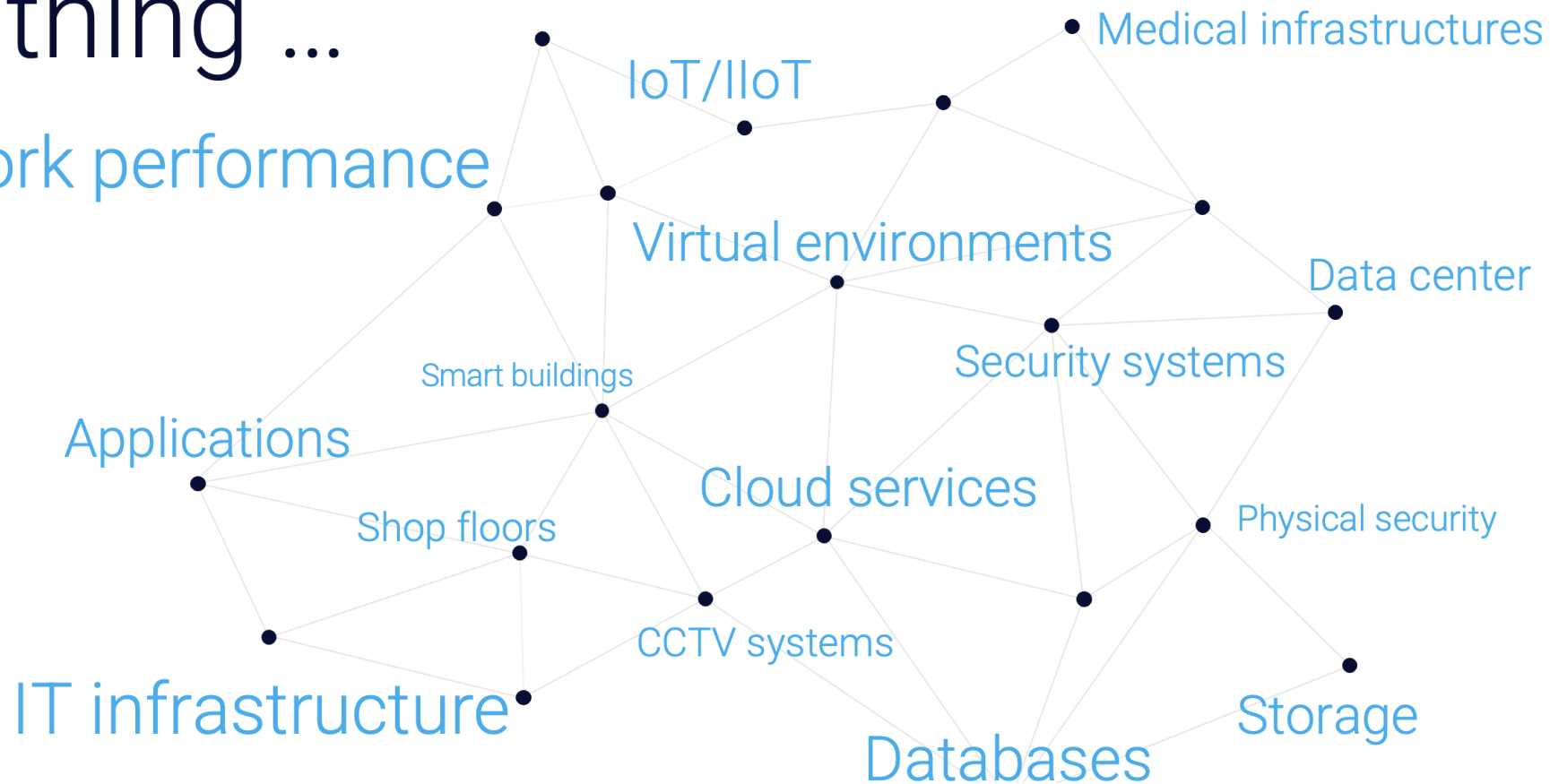
PAESSLER
PRTG
ENTERPRISE
MONITOR

jornadas.fccn.pt

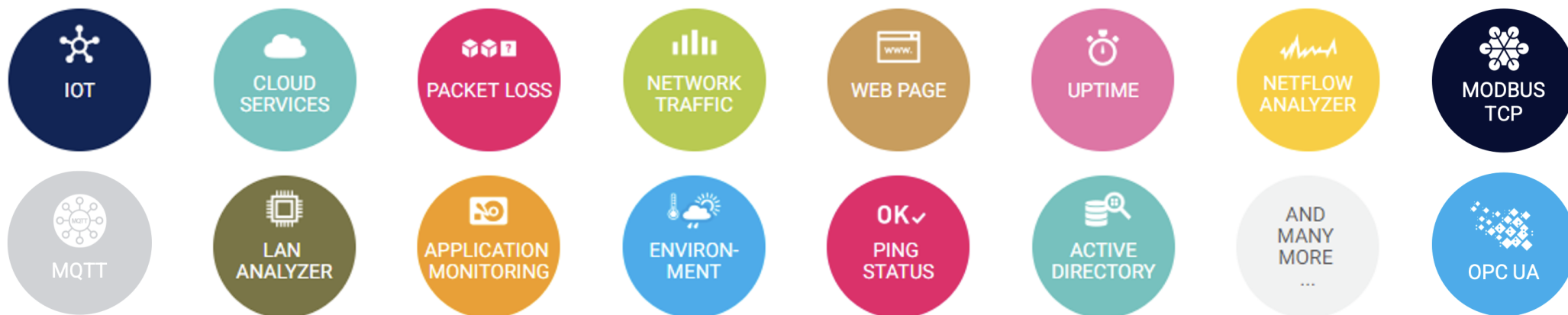


One solution to monitor every thing ...

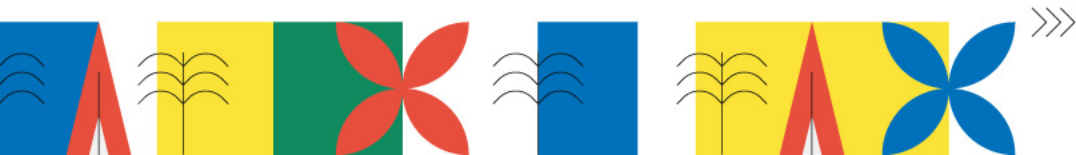
Network performance



More than 300 sensors



jornadas.fccn.pt



PRTG User Interfaces

- Ajax Web Interface
- PRTG Desktop App
- PRTG Mobile Apps



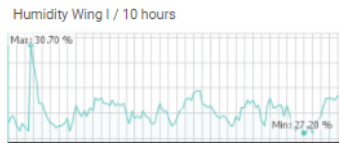
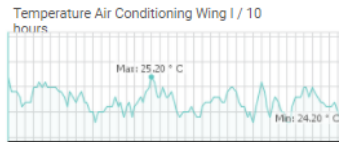
PRTG notifications

Powerful and
flexible alerting



INDUSTRY & IT

Building Technology

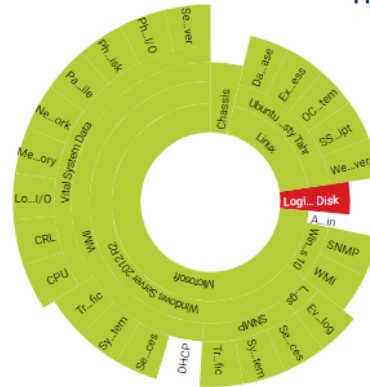


Building Access **Digital IO** OK
Value: No motion

Alarm System **Alarm** OK
Buzzer time: 3 sdd

Emergency Power **phase 2** OK
Ampd: 2.80 Ampd

IT Environment



VMware **55**

Storage **1 W 9 122 U 1**

BPS - Corporate Web Site
Global State: No data

Cloud Services **2 W 6 32 U 1**

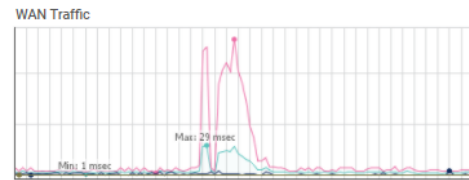
Email Website eCom File

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●



Production Environment

Environment

- NetBotz Rack Monitor
- KENTIX MultiSensor

Alarms (NetBotz Rack Monitor 200)

Status Wizard Clie Status Wizard Control

Status Voltage M1

Max: 233.00 Volts
Min: 226.00 Volts

Status Temp M1

Max: 24.50 ° Celsius
Min: 23.00 ° Celsius

Probe Device

Core Health 25% (Health) is bel.

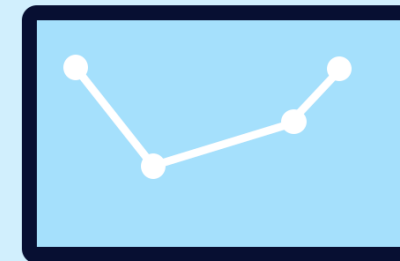
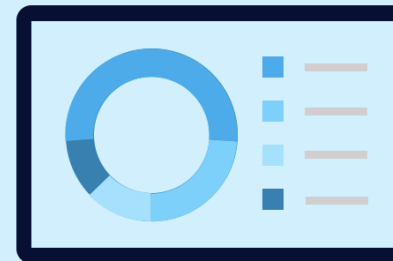
Health 25%

Probe Delay 83% Delay (Interva...

Health 59%



Have
everything
under
control.



PERPETUAL LICENSE

PAESSLER
**PRTG
NETWORK
MONITOR**

10k
max.

One time purchase

▶ Less than
1/3 renewal



I need my
PRTG
sensors

SUBSCRIPTION

PAESSLER
**PRTG
HOSTED
MONITOR**

10k
max.

PAESSLER
**PRTG
ENTERPRISE
MONITOR**

20k+

PRTG 500

Start small, upgrade later

€ 1,649.00

PER LICENSE SERVER

GET STARTED

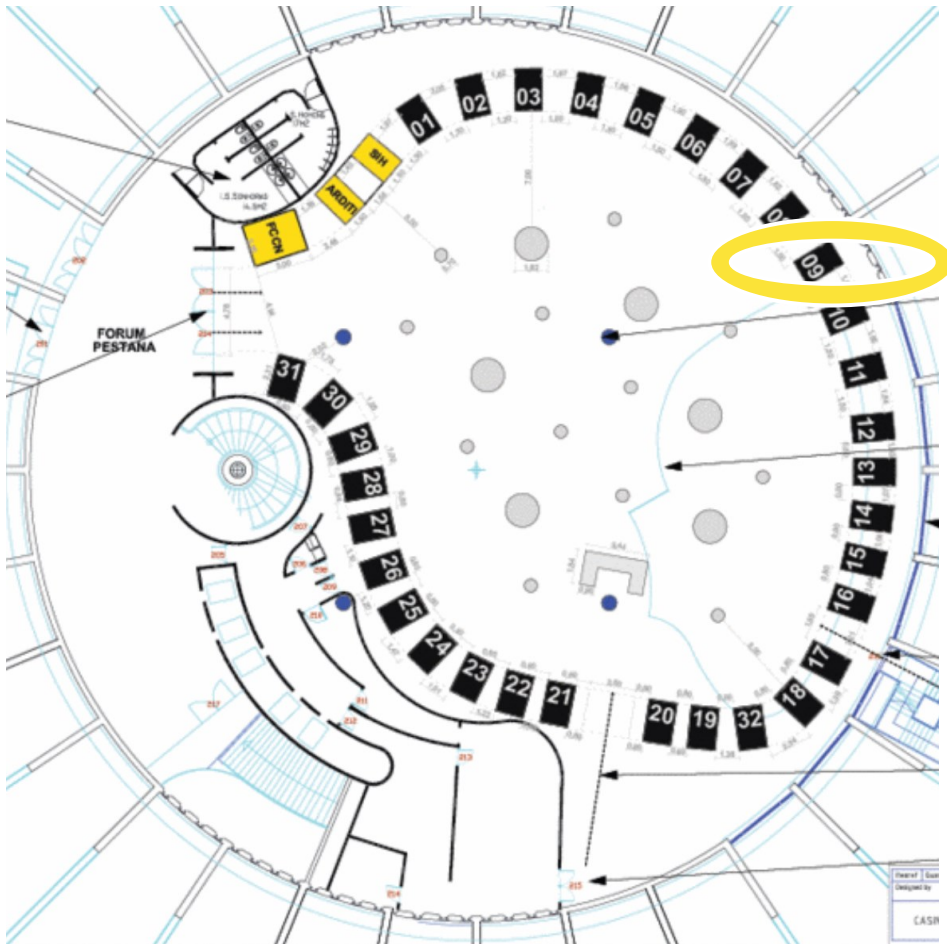
Monitor up to 500 aspects of
your devices in your network,
which usually means about 50
devices

Esperança ou Certeza

jornadas.fccn.pt



Centro de exposições Espaço 9



OBRIGADO !

