Jornadas FCCN 2023

RCTS Certificados

Emissão e Renovação de Certificados via ACME

ACME

João Guerreiro
joao.guerreiro@fccn.pt

fct Fundação para a Ciência e a Tecnologia FCCN

Agenda

1. **Motivação**
2. **Protocolo ACME**
3. **Certbot**
4. **Pacote de Ansible**

Motivação

https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

2023/03/03

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

- **a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.** Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on "broken" revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

- **Validade máxima de 90 dias** (antes: 1 ano)

Motivação

https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

2023/03/03

In a future policy update or CA/Browser Forum Ballot Proposal, we intend to introduce:

- **a reduction of TLS server authentication subscriber certificate maximum validity from 398 days to 90 days.** Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on "broken" revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.

- **Validade máxima de 90 dias** (antes: 1 ano)

SECTIGO®

October 2023

Date of last 1 year certificate sale will be declared

Motivação

- Validade **90 dias**
- **Centenas** de certificados
- **Centenas** de servidores

Motivação

- Validade **90 dias**
- **Centenas** de certificados
- **Centenas** de servidores

→ **Impraticável manualmente**

Motivação

- Validade **90 dias**
- **Centenas** de certificados
- **Centenas** de servidores

Impraticável manualmente

Automação!

ACME – O que é?

- **A**utomated **C**ertificate **M**anagement **E**nvironment
- Protocolo de comunicação
  - Entre **Cliente** (nosso servidor) e **CA** (*Sectigo*)
  - Automático
- Permite:
  - Automatizar processo de obtenção (e renovação) de certificados SSL
  - **Sem intervenção manual**

ACME – Etapas

ACME

1. Registo

- Cliente prova à CA que controla um domínio (e.g., *eduroam.pt*)

ACME – Etapas

1. Registo

- Cliente prova à CA que controla um domínio (e.g., *eduroam.pt*)

HTTP

- Simples de automatizar
- Compatível com servidores web
- Sem *wildcards*
- Porta 80

ACME – Etapas

1. Registo

- Cliente prova à CA que controla um domínio (e.g., *eduroam.pt*)

HTTP

- Simples de automatizar
- Compatível com servidores web
- Sem *wildcards*
- Porta 80

DNS

- Permite certificados *wildcards*
- Não depende da porta 80
- Necessita alterações no DNS

ACME – Etapas

1. Registo

- Cliente prova à CA que controla um domínio (e.g., *eduroam.pt*)

HTTP

- Simples de automatizar
- Compatível com servidores web
- Sem *wildcards*
- Porta 80

ACME – Vantagens

- **Automático!!** (emissão, revocação, renovação, etc.)
- Mantém certificados **atualizados**
- **Reduz** hipóteses de **erro humano**
- **Melhor segurança**
- **Mais fácil em adaptar-se a outras CAs** (vs. API)

Certbot – O que é?

- Ferramenta **grátis** e ***open-source***
- **Cliente ACME**
  - Comunica com uma CA (*eg., Sectigo*)
  - Protocolo ACME
- Instalado + configurado:
  - Obtenção e renovação automática de certificados SSL

Pacote Ansible – ACME

- **Funcionalidades**
  - Instala *certbot*
  - Regista Cliente ACME na CA (Sectigo)
  - Faz pedido de certificado(s)
  - Transfere certificado(s)
  - Confirma se certificados ainda estão válidos (periodicamente)

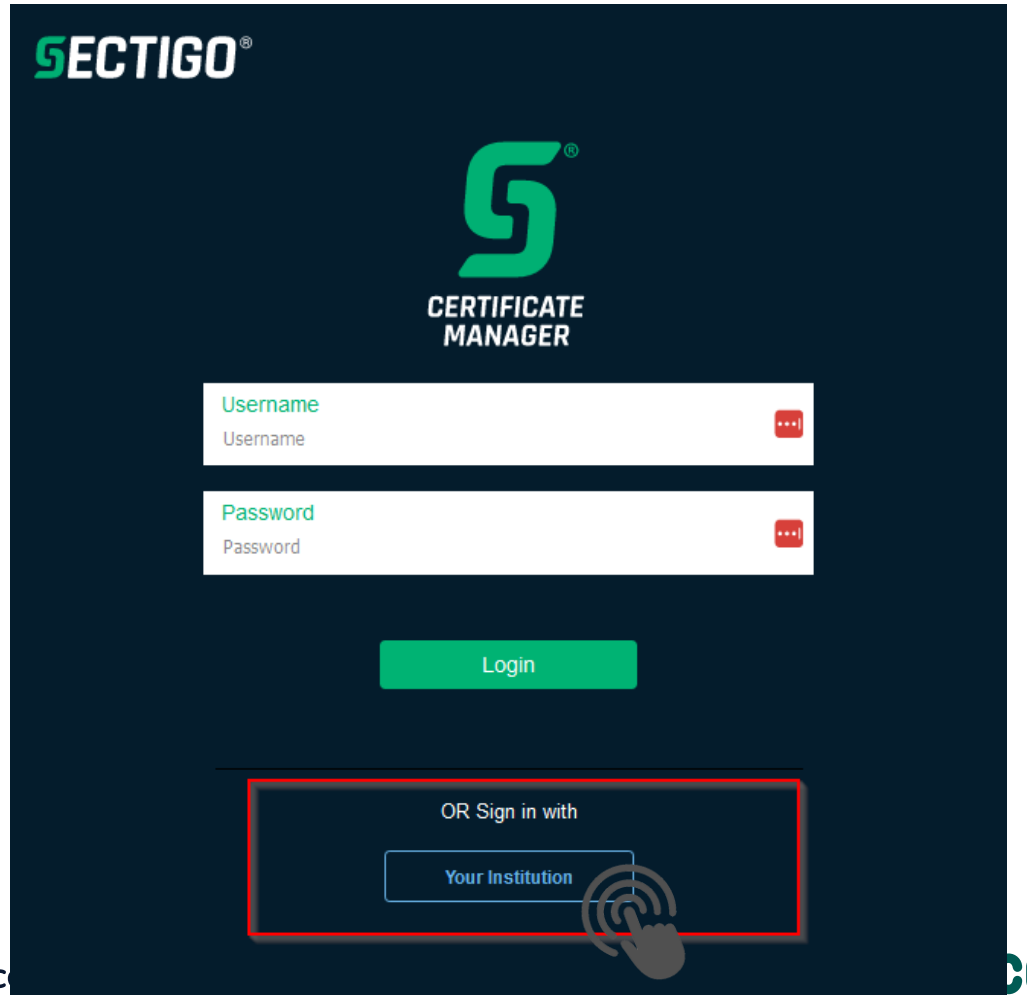
Como utilizar?

1. **Administradores de Certificados da Instituição**

Como utilizar?

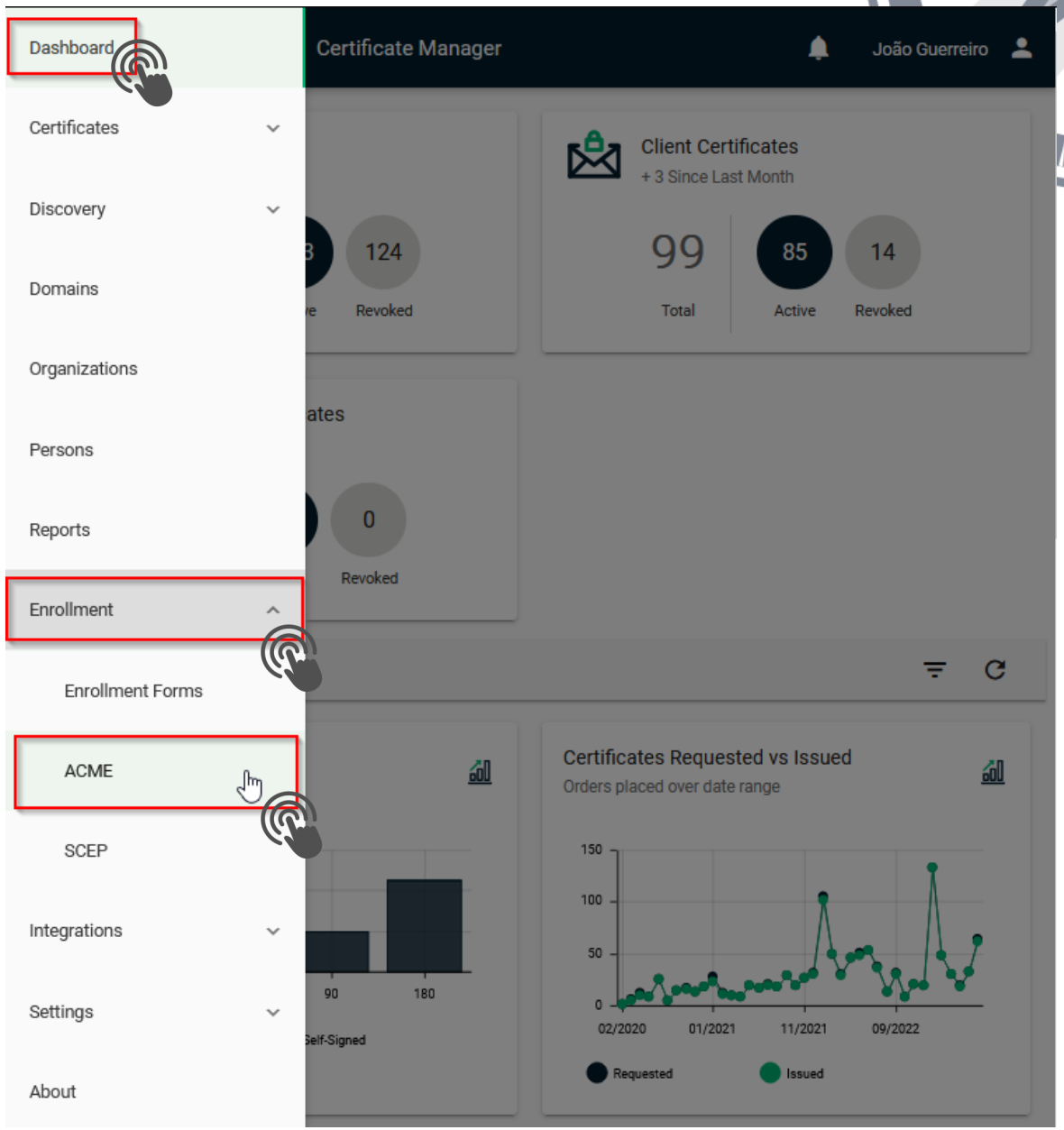
1. **Administradores de Certificados da Instituição**
   - Criar conta(s) ACME

https://cert-manager.com/customer/fccn



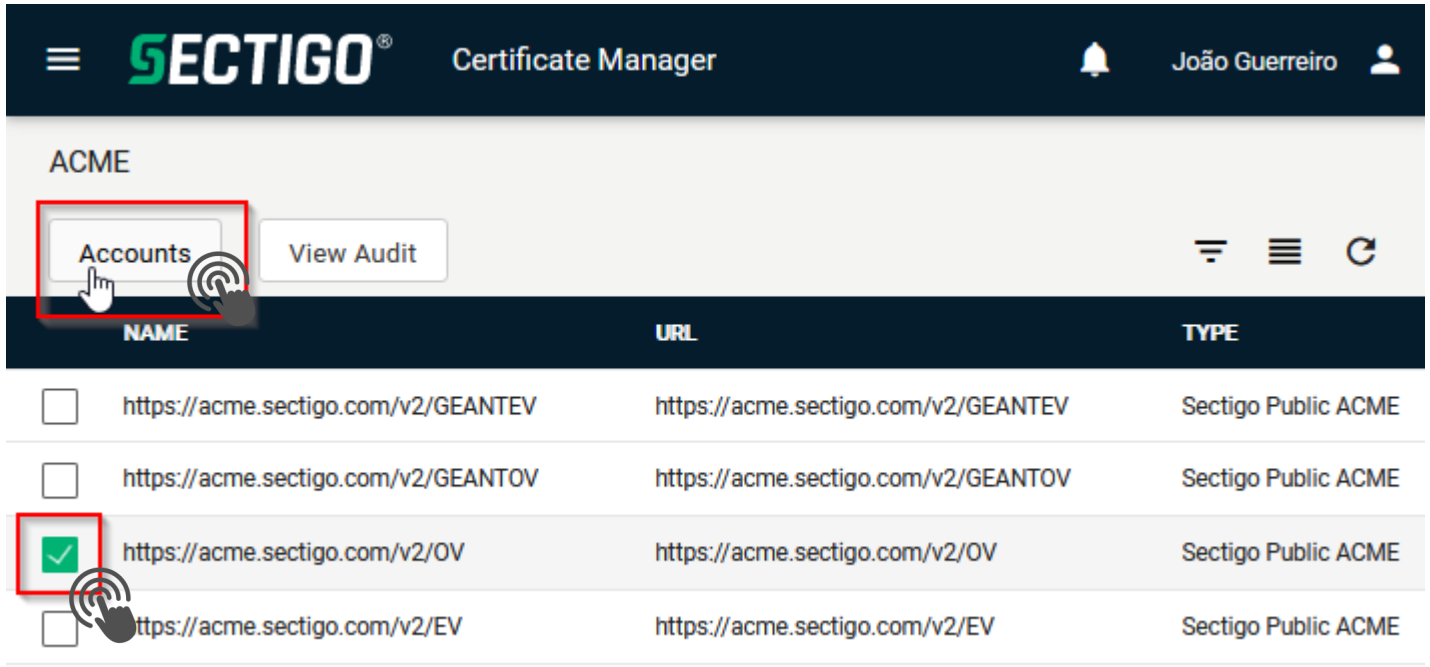
Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME



Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME



Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME

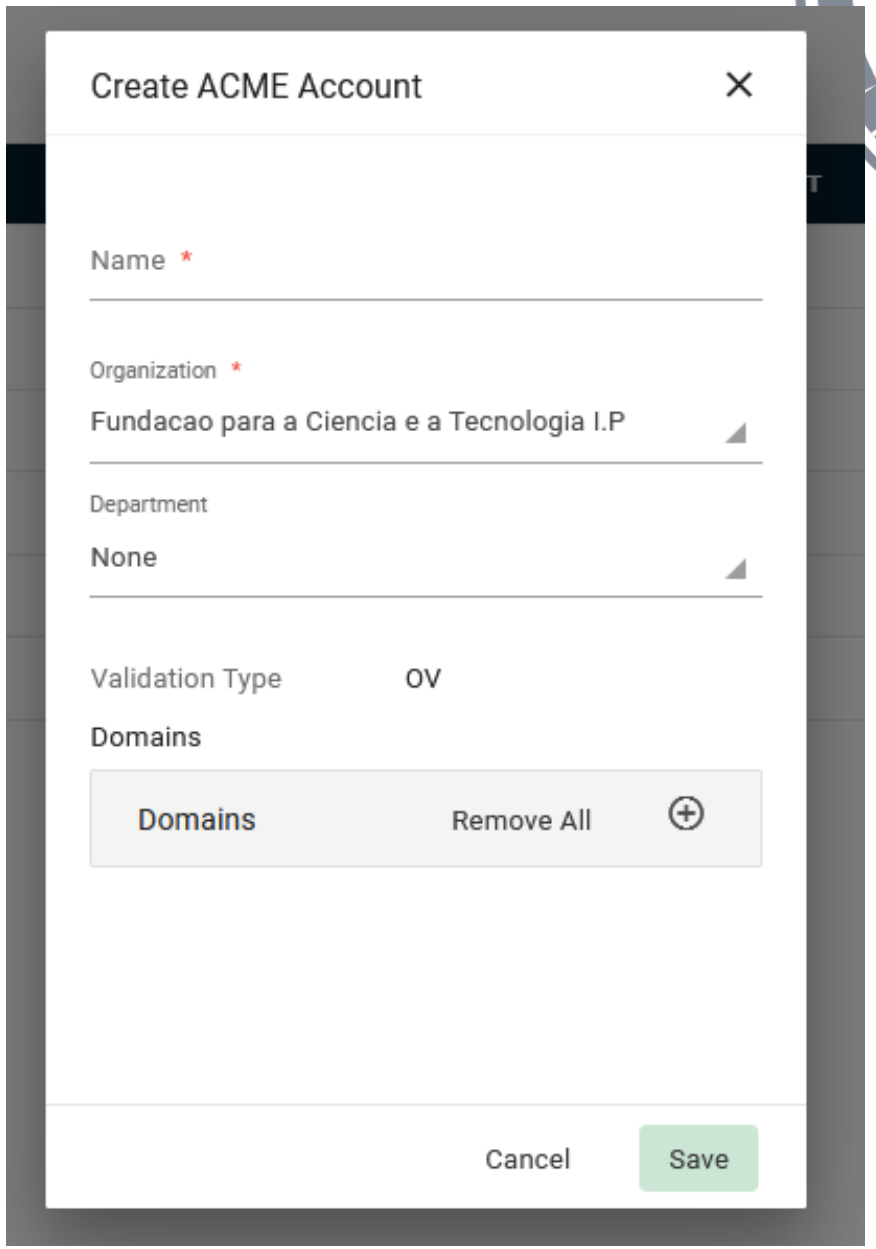
ACME Accounts

Add

NAME	ORGANIZATION	DEPARTMENT
FCCN	Fundacao para a Ciencia e a Tecnologia I.P	FCT|FCCN
ACME FCCN - RCTSaai	Fundacao para a Ciencia e a Tecnologia I.P	FCT|FCCN
ACME FCCN eduroam - psimoes	Fundacao para a Ciencia e a Tecnologia I.P	FCT|FCCN
ACME FCCN ASA	Fundacao para a Ciencia e a Tecnologia I.P	FCT|FCCN
ACME FCCN	Fundacao para a Ciencia e a Tecnologia I.P	FCT|FCCN
ACME Ciencia-ID	Fundacao para a Ciencia e a Tecnologia I.P	

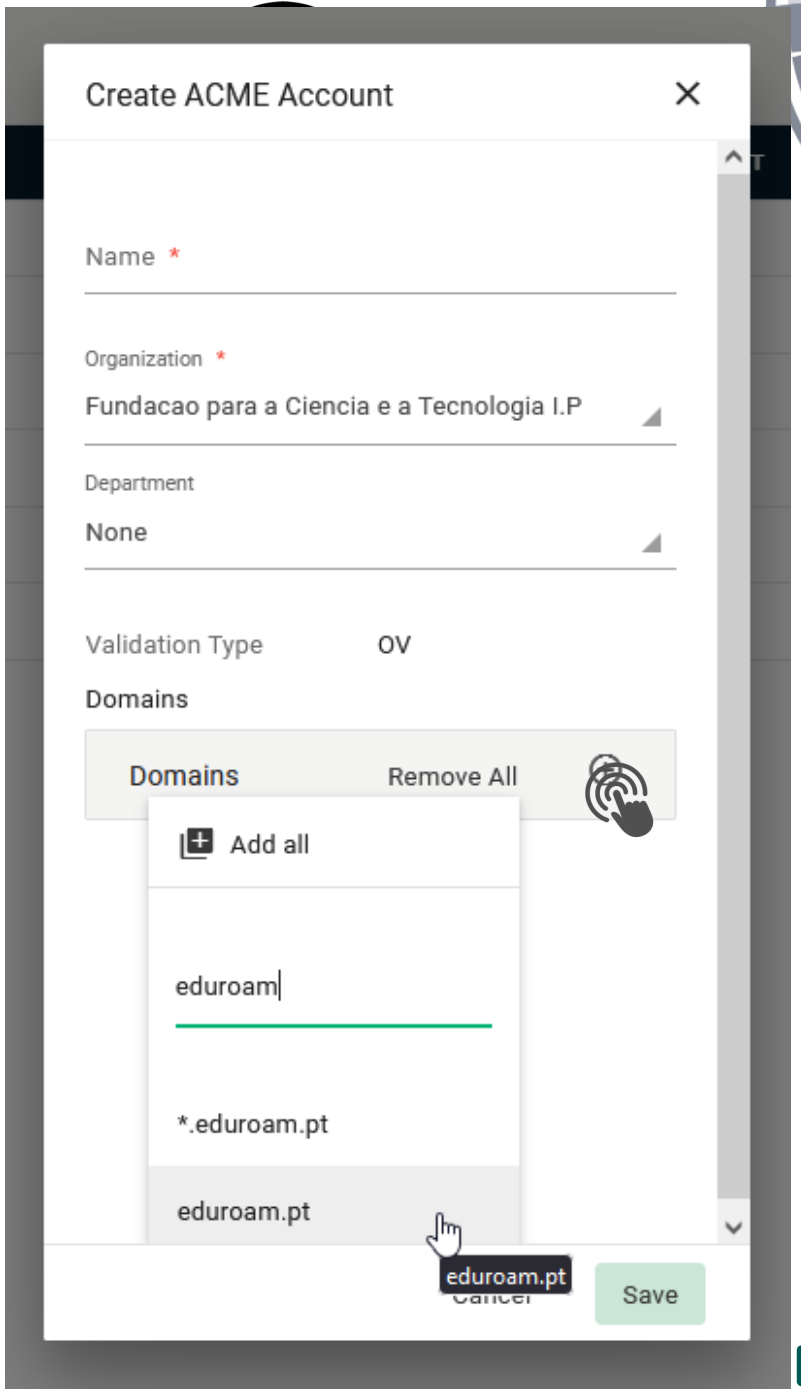
Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME



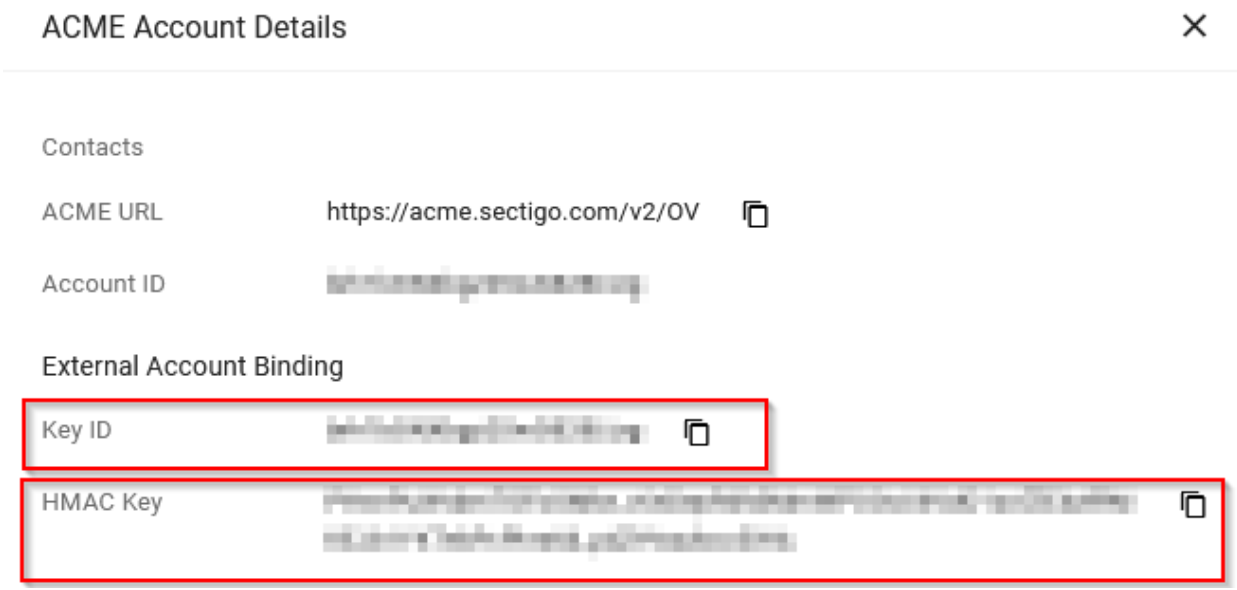
Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME
   - **Associar domínios da instituição ligados a uma conta**



Como utilizar?

1. **<u>Administradores de Certificados da Instituição</u>**
   - Criar conta(s) ACME
   - Associar domínios da instituição ligados a uma conta
   - **Obter credenciais da conta**



Como utilizar?

1. Administradores de Certificados da Instituição
2. **Administradores de sistemas dos serviços da Instituição**

ANSIBLE

Como utilizar?

1. Administradores de Certificados da Instituição
2. **Administradores de sistemas dos serviços da Instituição**
   - **Com credenciais de conta ACME**
     - Cifradas (*e.g., Ansible-Vault*)

credentials.yml:

```yaml
---

sectigo_customerUri: fccn
sectigo_organizationId: 11606
contact: joao.guerreiro@fccn.pt

acme_server: https://acme.sectigo.com/v2/OV

acme_accounts:
  - name: "eduroam"
    macId: XXXXXXXXXXXXXXXXX
    macKey: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Como utilizar?

1. Administradores de Certificados da Instituição
2. **Administradores de sistemas dos serviços da Instituição**
   - Com credenciais de conta ACME
   - **Ansible Playbook *Certbot***
     - **Instala ferramenta**
     - **Regista Cliente ACME na CA**
     - **Faz pedido de certificado**
     - **Transfere o certificado**

credentials.yml:

```yaml
---

sectigo_customerUri: fccn
sectigo_organizationId: 11606
contact: joao.guerreiro@fccn.pt

acme_server: https://acme.sectigo.com/v2/OV

acme_accounts:
  - name: "eduroam"
    macId: XXXXXXXXXXXXXXXX
    macKey: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```shell
shell> ansible-playbook acme.yml \
          --extra-vars \
            "option_acme_account_name='eduroam' \
            option_common_names_list='teste-acme.eduroam.pt'"
```

Pacote Ansible - ACME

- **Resumo**
  - Instala e configura *certbot*
  - Depois, **periodicamente**:
    - Confirma se certificados ainda estão válidos
    - **Se necessário, pede e transfere novo certificado**
    - **Pode reiniciar aplicações** (*apache, nginx, etc.*)
  - A disponibilizar brevemente

Pacote Ansible será disponibilizado às instituições aderentes ao RCTS Certificados

Questões?

Feedback Instituições:

- ACME?
- API?

João Guerreiro - joao.guerreiro@fccn.pt
Pedro Simões - psimoes@fccn.pt

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