

Gestão de Certificados SSL

Certificados de Servidor, Certificados
Pessoais e Futuro da Automação



Agenda da Sessão

- Introdução
- HARICA - Novo fornecedor do serviço Certificados RCTS
- Q&A
- Esclarecimentos e Apoio
- Encerramento



Área de Serviços de Redes

Serviço de Identidade Digital e Sistemas (SIDS)

Emanuel Massano



Esmeralda Pires



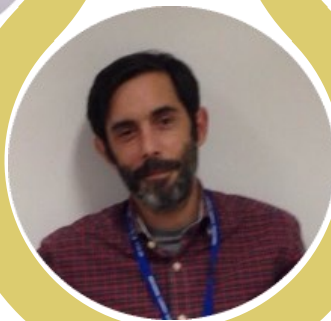
João Guerreiro



André Leite



António Coucelo



Pedro Simões



Filipe Santana



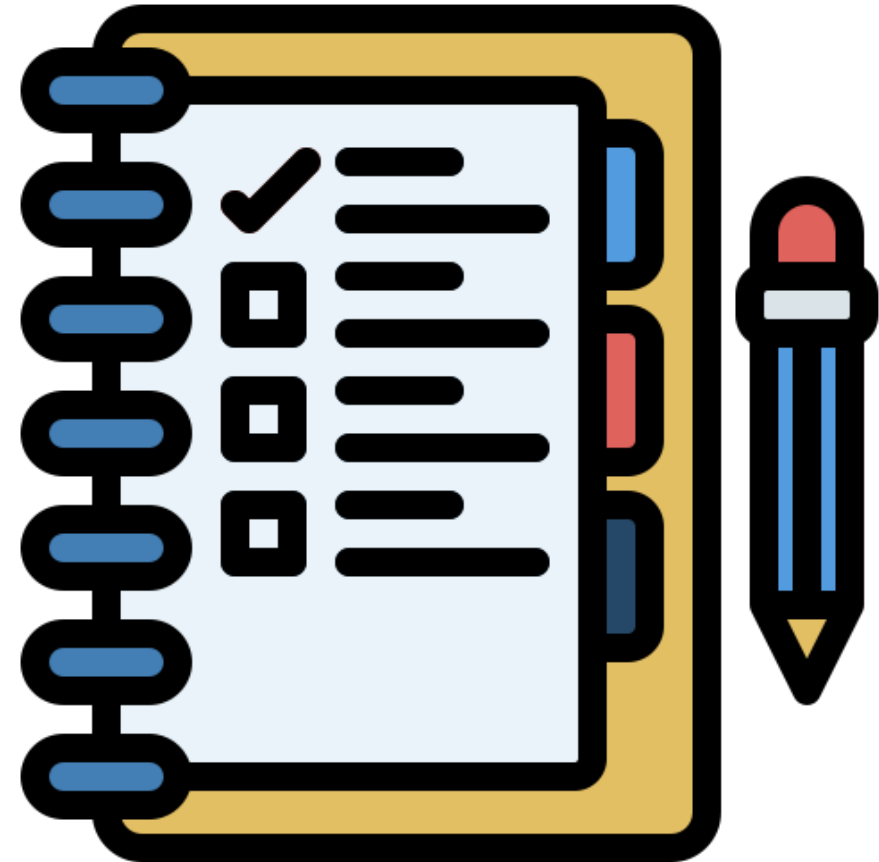
HARICA

Novo fornecedor do serviço de
certificados RCTS



HARICA - Agenda

- HARICA - Novo Fornecedor
- (1º) Acesso
- Validações
- Utilizadores: Perfis
- Certificados: Server
- Gerir certificados: Personal
- Considerações gerais



HARICA - Novo Fornecedor de Serviço

Quem é a HARICA?



“HARICA is the Hellenic Academic & Research Institutions Certification Authority. It participates in all major Global 'ROOT CA' Trust Programs, and operates as a 'Trust Anchor' in widely used Application Software and Operating Systems”

Moldes do serviço

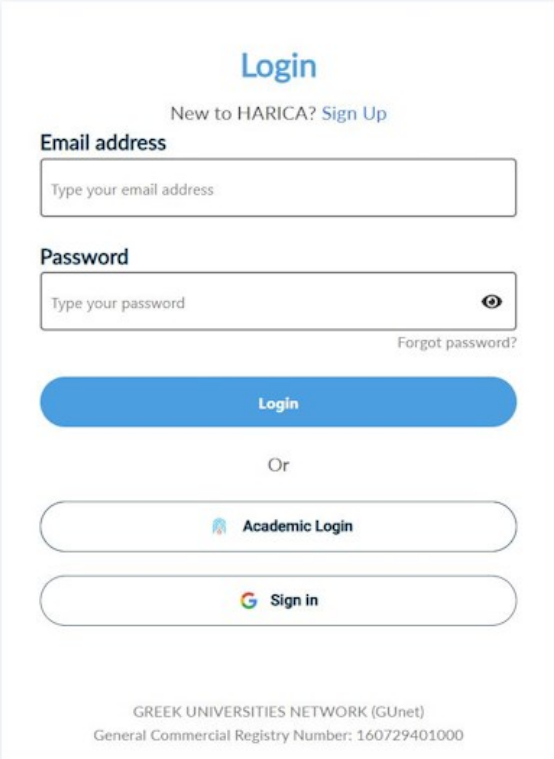
- Novo fornecedor de serviço
- Igual à Sectigo (no futuro)
- Integrações ainda a decorrer
- Ongoing - roadmap de funcionalidades



HARICA - (1º) Acesso

Como aceder

- Portal: <https://cm.harica.gr>
- Autenticação federada
- Usar login Federado



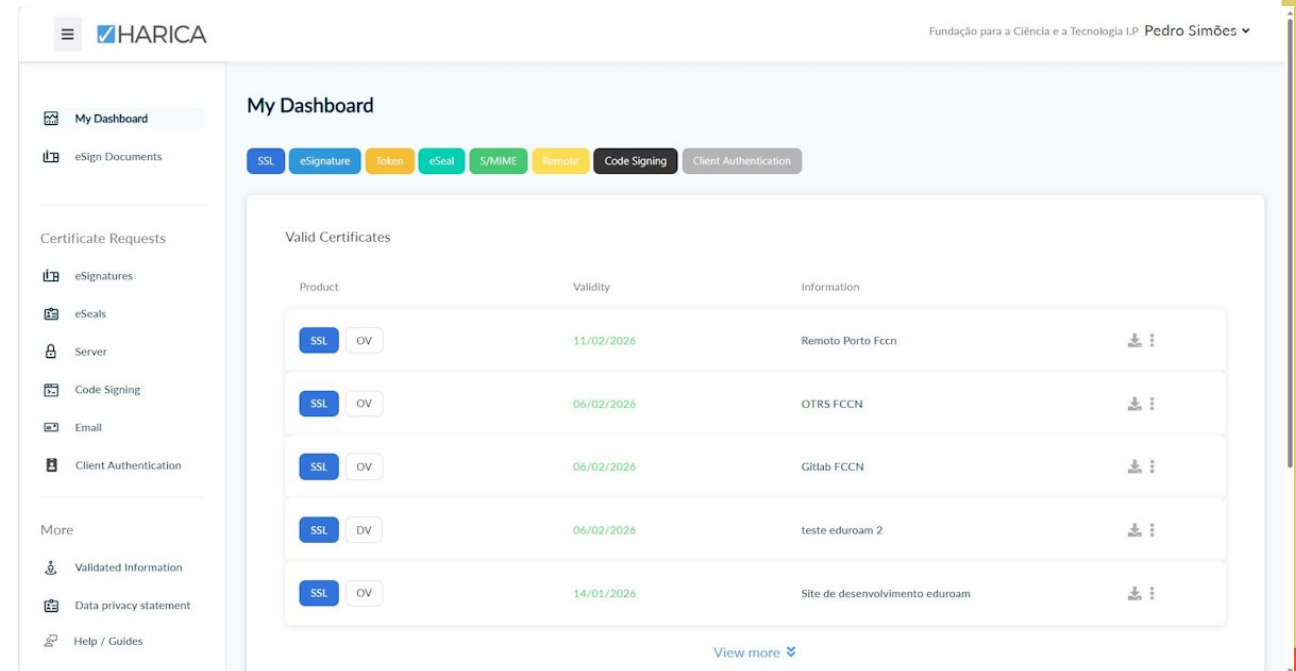
The screenshot shows the HARICA Login interface. At the top, the word "Login" is displayed in blue. Below it, a link "New to HARICA? Sign Up" is visible. The form consists of two main input fields: "Email address" with a placeholder "Type your email address" and "Password" with a placeholder "Type your password" and a toggle icon. A "Forgot password?" link is located below the password field. A prominent blue "Login" button is centered below the inputs. Below this button, the word "Or" is displayed. Two alternative login options are provided: "Academic Login" with a person icon and "Sign in" with the Google logo. At the bottom of the page, the text "GREEK UNIVERSITIES NETWORK (GUnet)" and "General Commercial Registry Number: 160729401000" is displayed.



HARICA - (1º) Acesso

Certificate Manager (CM)

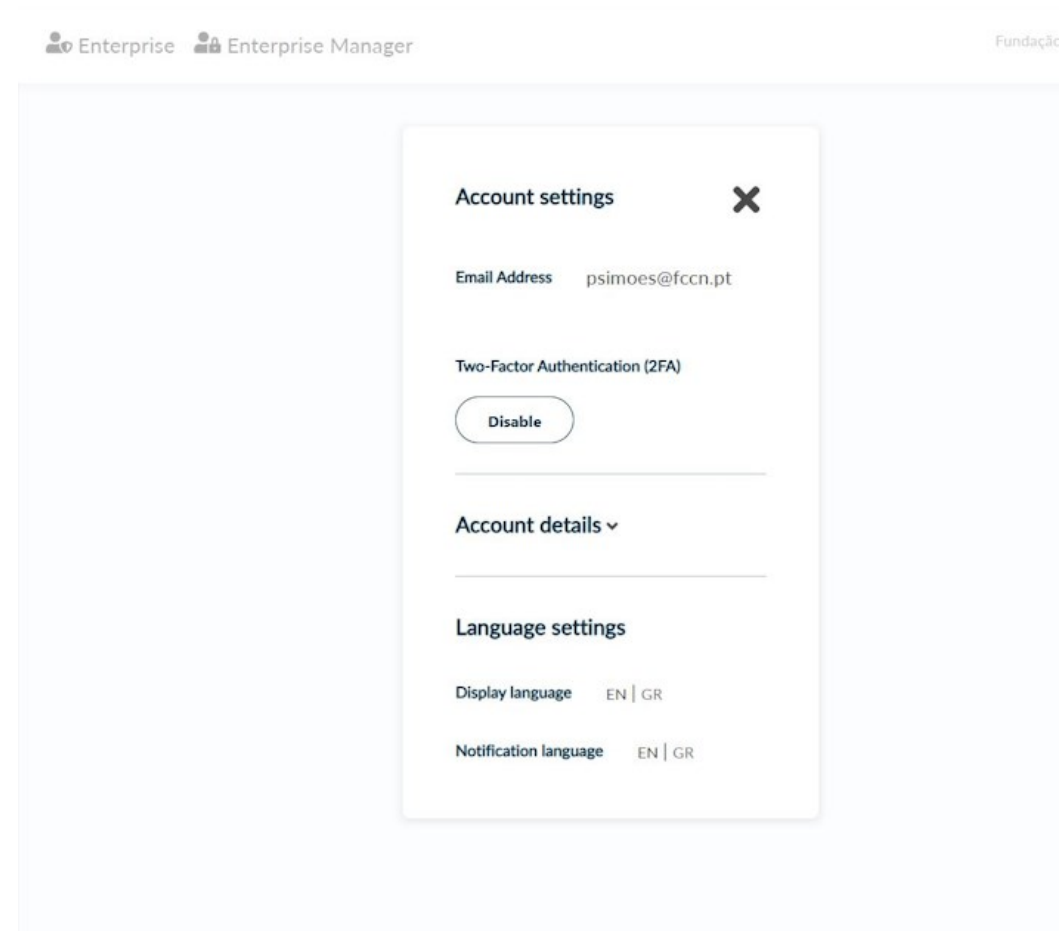
- Gerir Organização/Users
- Pedir novos certificados
- Aceder aos certificados
- Revogar os certificados



HARICA - (1º) Acesso

Segurança

- Onboarding realizado
- Autenticação federada
- Ativar 2FA por admin



HARICA – Validações: DCV

Domain Control Validation

- Autorização domínios

- Métodos:
 - DNS record
 - Email

- Renovação anual

The screenshot displays the HARICA DCV (Domain Control Validation) interface. It features a form for selecting a validation type and providing an email for validation. Below the form, there is a list of domains and their expiration dates, with a 'Validate Domain' button for each.

Validation Type

Constructed Email to Domain Contact - 3.2.2.4.4 ▼

Email of user that will validate the Enterprise

Email

admin ▼ @ study-research.pt ▼

Submit

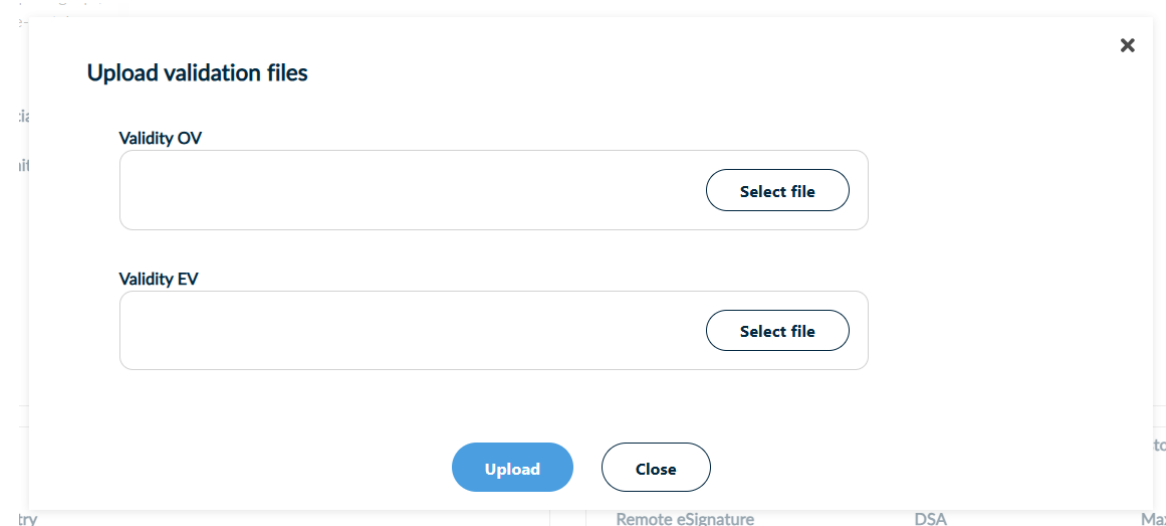
Domains and Expiration Dates:

gigapix.pt	08/01/2025	Validate Domain
ticsociedade.pt	08/01/2025	Validate Domain
eduroam.pt	10/02/2026	Validate Domain
cienciaid.pt	08/01/2025	Validate Domain
gridcomputing.pt	08/01/2025	Validate Domain
fct.pt	17/02/2026	Validate Domain

HARICA – Validações: Organização

Organization Validation

- Validar dados Organização
- Documentos (PDF):
 - Link do site DGES
 - Diário República
 - Outros (fora da org)
- Renovação anual



The screenshot shows a web-based dialog box titled "Upload validation files" with a close button (X) in the top right corner. Inside the dialog, there are two sections for file uploads:

- Validity OV:** A text input field with a "Select file" button to its right.
- Validity EV:** A text input field with a "Select file" button to its right.

At the bottom of the dialog, there are two buttons: a blue "Upload" button and a white "Close" button with a blue border. The dialog is overlaid on a background that shows parts of a table with headers like "Remote eSignature", "DSA", and "Max".

HARICA – Utilizadores: Perfis

- Perfis (cumulativos) (1)
 - Admin: Gerir dados da Org
 - Aprovador: Tratar certificados
- Promover só com 2FA
- Associar Organização (2)
- Domínio de email registado

The screenshot shows the 'Account info' tab of a user profile in the HARICA system. The interface includes tabs for 'Personal info', 'Requests', and 'Account info'. Under 'Account info', the 'Account created' date is 'Wednesday, January 8, 2025'. The 'Two-Factor Authentication (2FA)' status is 'Enabled' with a 'Disable' button. The 'Roles' section shows the user is associated with the 'Organization' 'Fundação para a Ciência e a Tecnologia'. Two roles are listed: 'Enterprise Admin' and 'Enterprise Approver', both with toggle switches. A dropdown menu for the 'Enterprise Approver' role is open, showing two checked options: 'SSL Enterprise Approver' and 'SMIME Enterprise Approver'. A red arrow labeled '(1)' points to this dropdown menu. The 'Validator groups' section shows the group 'Fundação para a Ciência e a Tecnologia' with a 'Manage Groups' button. A red arrow labeled '(2)' points to this button. A 'Save' button is located at the bottom right of the form.

HARICA – Certificados: Server

Tipos de certificados

- DV – “Domain Validation”
- OV – “Organization Validation”
- **Não existem certificados EV**
- **ACME chega em maio (previsto)**

Select the type of your certificate

Domain-only (DV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains

Select

Free

For enterprises or organizations (OV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains

Select

Free

For enterprises or organizations (EV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains
- Official registry information of your organization

Select

from 275€ year



HARICA – Certificados: Personal

Tipos de certificados

- “Email-only”
 - E-mail

- “Enterprises or organizations”
 - E-mail
 - Informação pessoal
 - Informação da Organização

Sistema de self-service

Select the type of your certificate

Email-only
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)

Select

Free

For individuals or sole proprietorships (IV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information

Select

from
33€ year

For enterprises or organizations (OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Information of your organization

Select

from
71.5€ year

For enterprises or organizations (IV+OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
• Information of your associated organization

Select

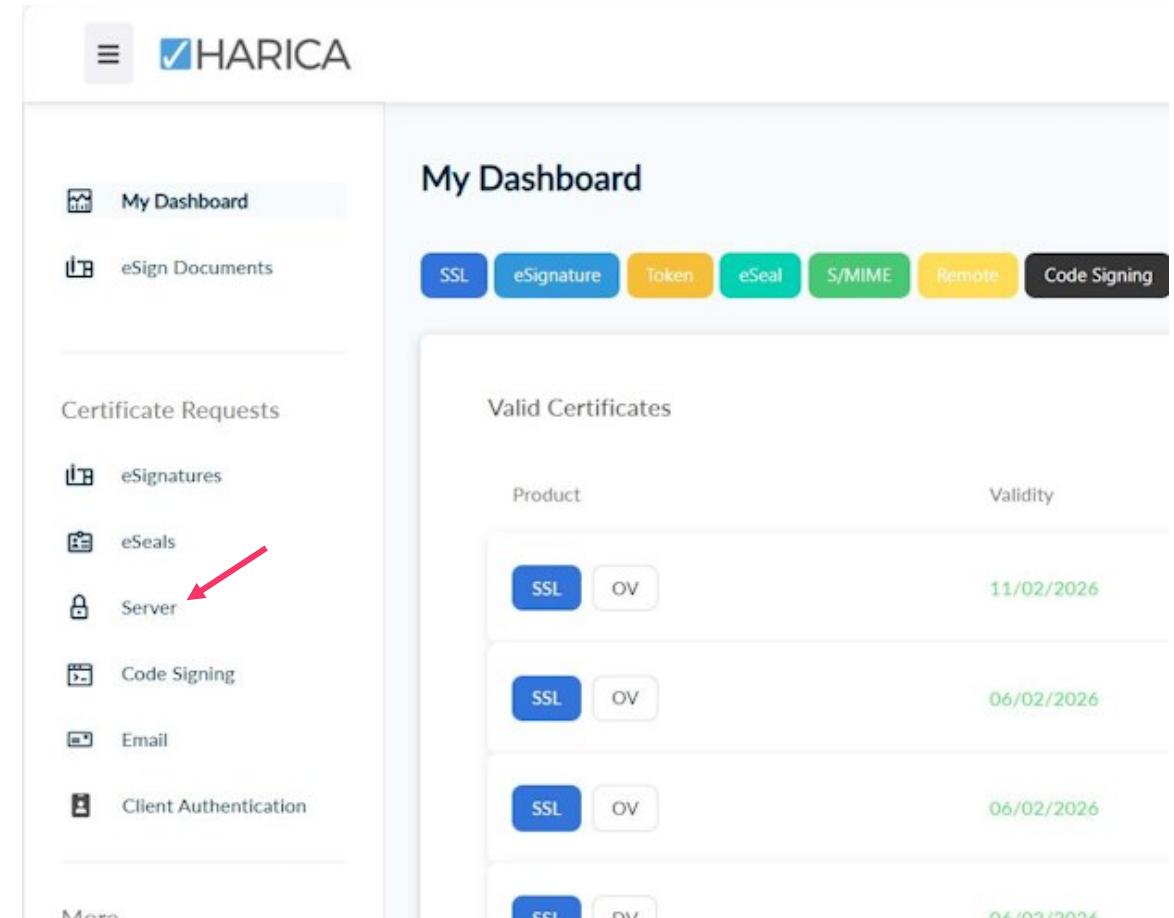
Free



HARICA – Certificados: Server

Pedir 1 certificado

- Gerar Key e CSR
- Aceder ao CM
- Opção “Server” no menu



HARICA – Certificados: Server

Pedir 1 certificado

- Definir “Friendly Name”
- Definir domínio(s)
- **Domínio do CSR tem de constar**

My Dashboard

eSign Documents

Certificate Requests

eSignatures

eSeals

Server

Code Signing

Email

Client Authentication

More

Validated Information

Data privacy statement

Help / Guides

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Friendly name (optional)
A custom label to help you identify this certificate in your dashboard

e.g. "Webserver", "my certificate", etc

Add Domains Manually or via Import
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

e.g. harica.gr

+ Add more domains

The maximum number of domains allowed per request is 100.

Next

HARICA – Certificados: Server

Pedir 1 certificado

- Validar informação
- Carregar o CSR
- **Não usar a geração automática de CSR**

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Submit Request

What is a CSR?

Auto-generate CSR Submit CSR manually

or

Create your Private Key directly in your browser, and your CSR will be auto-generated Use your (already created) CSR and submit it here.

☐ I, Pedro Simões, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

< Back Submit request

HARICA – Certificados: Server

Fluxo de aprovação

- Pedido de certificado
- Aprovação por Org
- Verificar informação
 - Requerente, Domínio, etc
- Comunicar por email

The screenshot displays the HARICA eSignatures interface for a certificate request. At the top, the user information is shown: "Tiago^Sousa - tiagosousa@uevora.pt" and the certificate details "f8559f50-ef11-490d-b9f1-ac9a337f4ae6 SSL DV".

The main form is divided into several sections:

- Consent:** Indicated by a red 'X' icon.
- Domains:** Indicated by a green checkmark icon.
- Validated:** A table showing the status of the request:

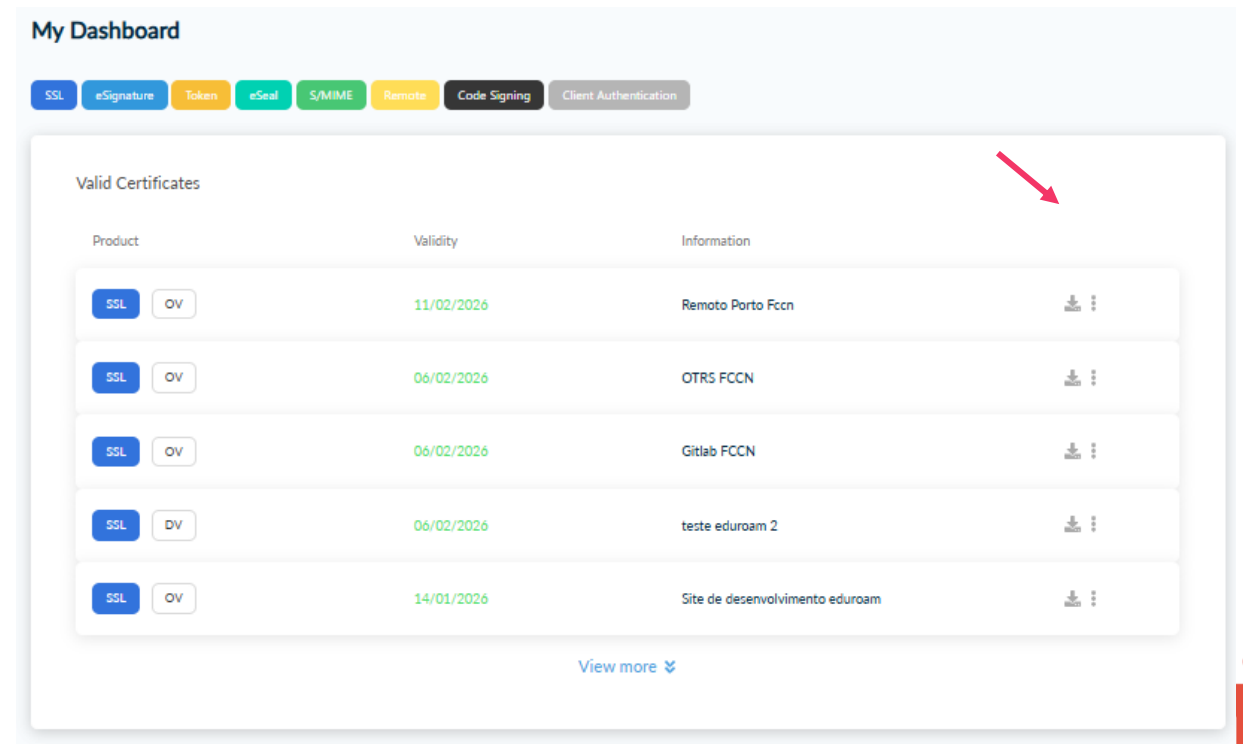
Validated	Reviewed	Created
X	0	2025-03-10T11:24:29.739114
- Value:** A section for uploading a file, with buttons for "Open file", "Escolher Ficheiro", and "Não foi escolhido nenhum ficheiro".
- Message:** A text area for entering a message, with a "Message" label and a "uevora.pt" domain specified.
- Inform user:** A checkbox labeled "Inform user" with an "Accept" button and an "Update" button.

A "Close" button is located at the bottom right of the form.

HARICA – Gerir Certificados: Server

Obter o certificado e CA

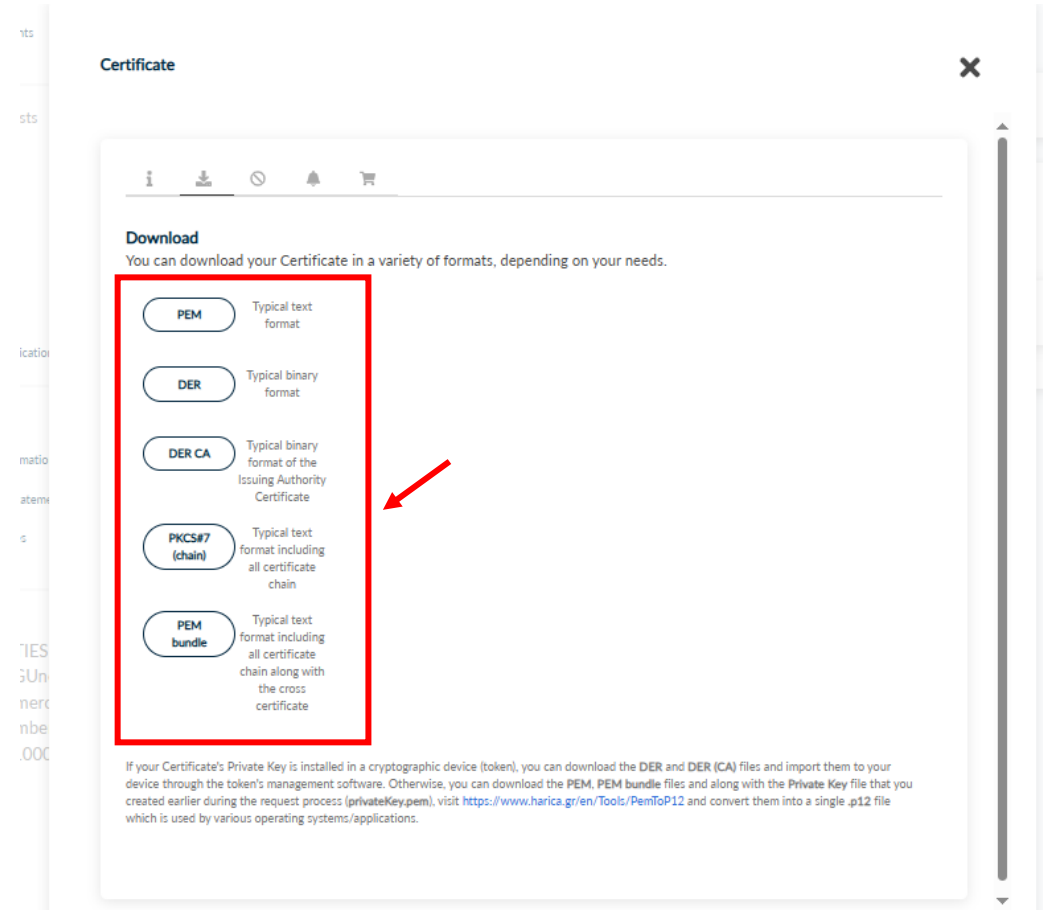
- Aceder ao CM HARICA
- Certificados no dashboard



HARICA – Gerir Certificados: Server

Obter o certificado e CA

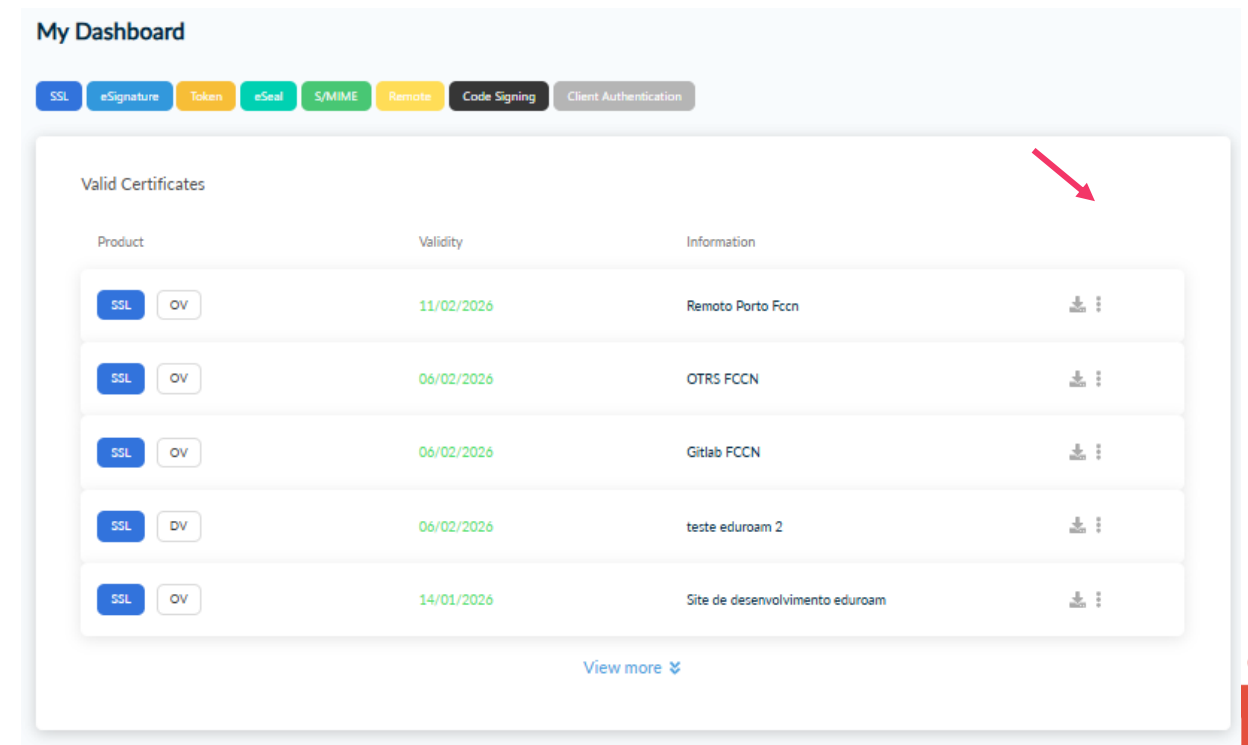
- Escolher formato
- Nova CA – Aplicar nos serviços
- **Adaptar CA ao serviço**



HARICA – Gerir Certificados: Server

Revogar certificados

- Aceder ao CM HARICA
- Certificados no dashboard
- Escolher “Revoke”



HARICA – Gerir Certificados:

Server

Revogar certificados

- Definir a causa
- Adicionar detalhes
- Escolher “Revoke”

my Dashboard

Certificate

Details Download Revocation Notifications Order

Revocation code: cf37e8cd34ce102939ee297534c929d4

Submit a request to revoke this certificate. Your certificate will become invalid.

Revocation reason

Unspecified reason

Revocation Details

Revoke



HARICA – Certificados: Personal

Pedir 1 certificado

- Aceder ao CM
- Opção “Email” no menu
- Escolher “Email only”

Review the application before submitting

Certificate Type	Service Duration
S/MIME email-only	2 years

Emails
1. psimoes@fccn.pt

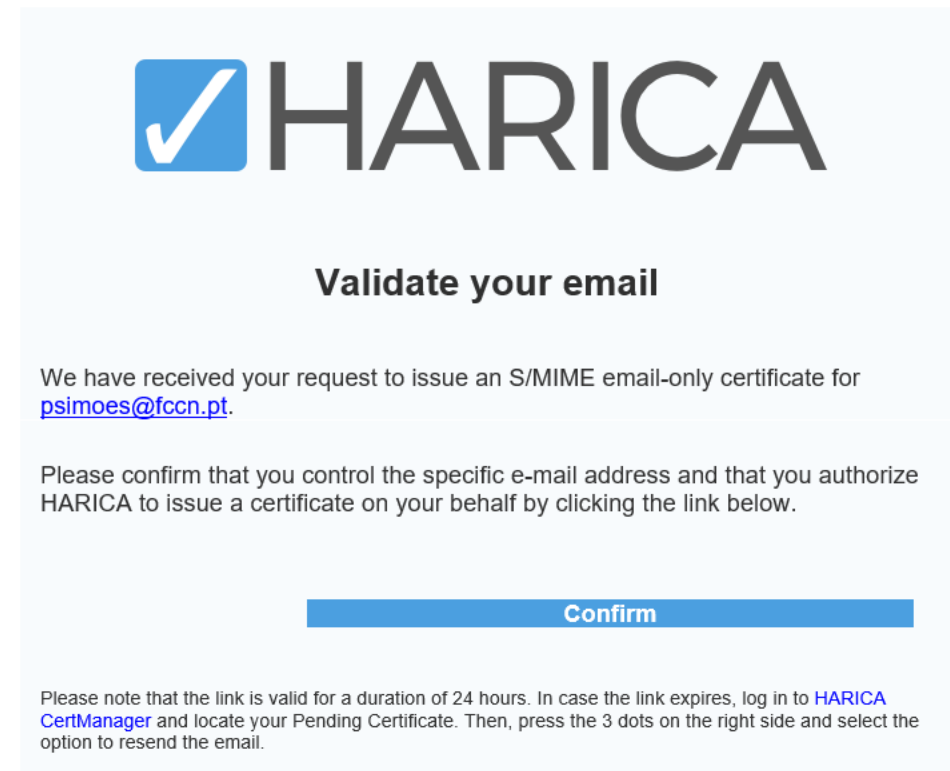
☒
I, Pedro Simões , declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

< Back
Submit

HARICA – Certificados: Personal

Validar pedido

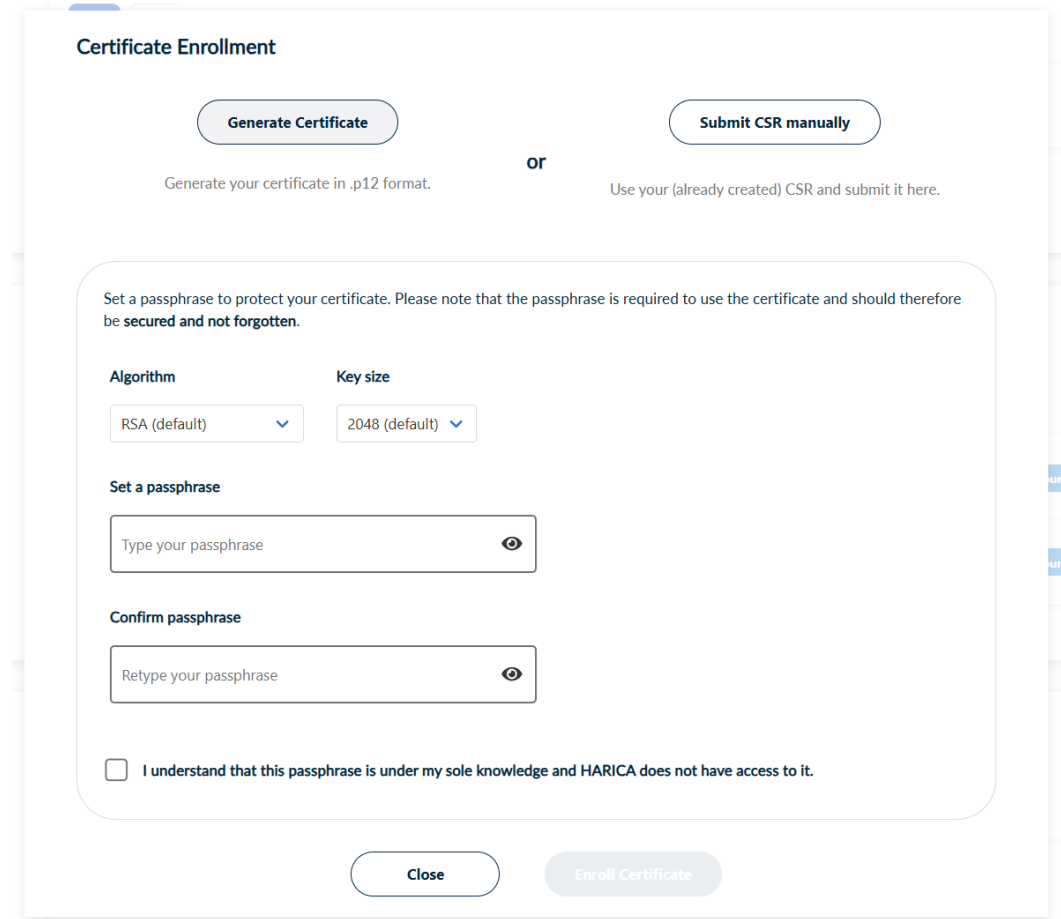
- Aceder ao email
- Clicar em “Confirm”
- Autorizar pedido na página



HARICA – Certificados: Personal

Gerar/Obter certificado

- CM → Ready Certificates
- Clicar em “Enrol Certificate”
- Preencher dados
- Descarregar certificado



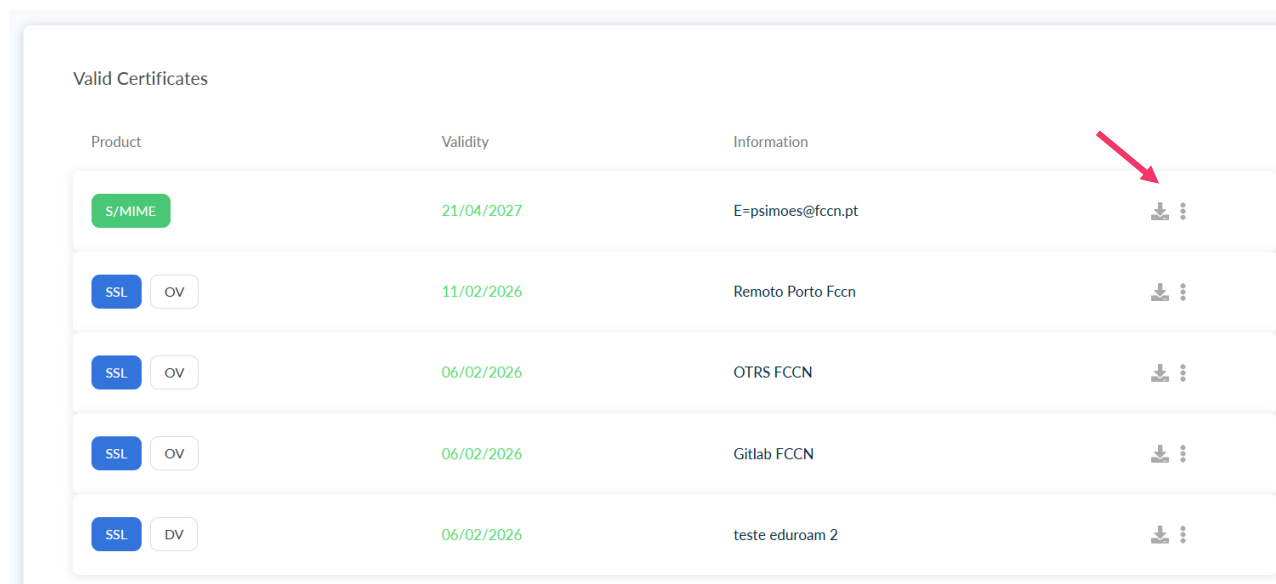
The screenshot shows the 'Certificate Enrollment' form. At the top, there are two buttons: 'Generate Certificate' and 'Submit CSR manually', separated by the word 'or'. Below these buttons, there are two instructions: 'Generate your certificate in .p12 format.' and 'Use your (already created) CSR and submit it here.' The main section of the form is titled 'Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be secured and not forgotten.' This section contains two dropdown menus: 'Algorithm' (set to 'RSA (default)') and 'Key size' (set to '2048 (default)'). Below these are two text input fields: 'Type your passphrase' and 'Retype your passphrase', each with a toggle icon for password visibility. At the bottom of the form, there is a checkbox labeled 'I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.' and two buttons: 'Close' and 'Enroll Certificate'.



HARICA – Gerir Certificados: Personal

Revogar certificados

- Aceder ao CM HARICA
- Certificados no dashboard
- Escolher “Revoke”

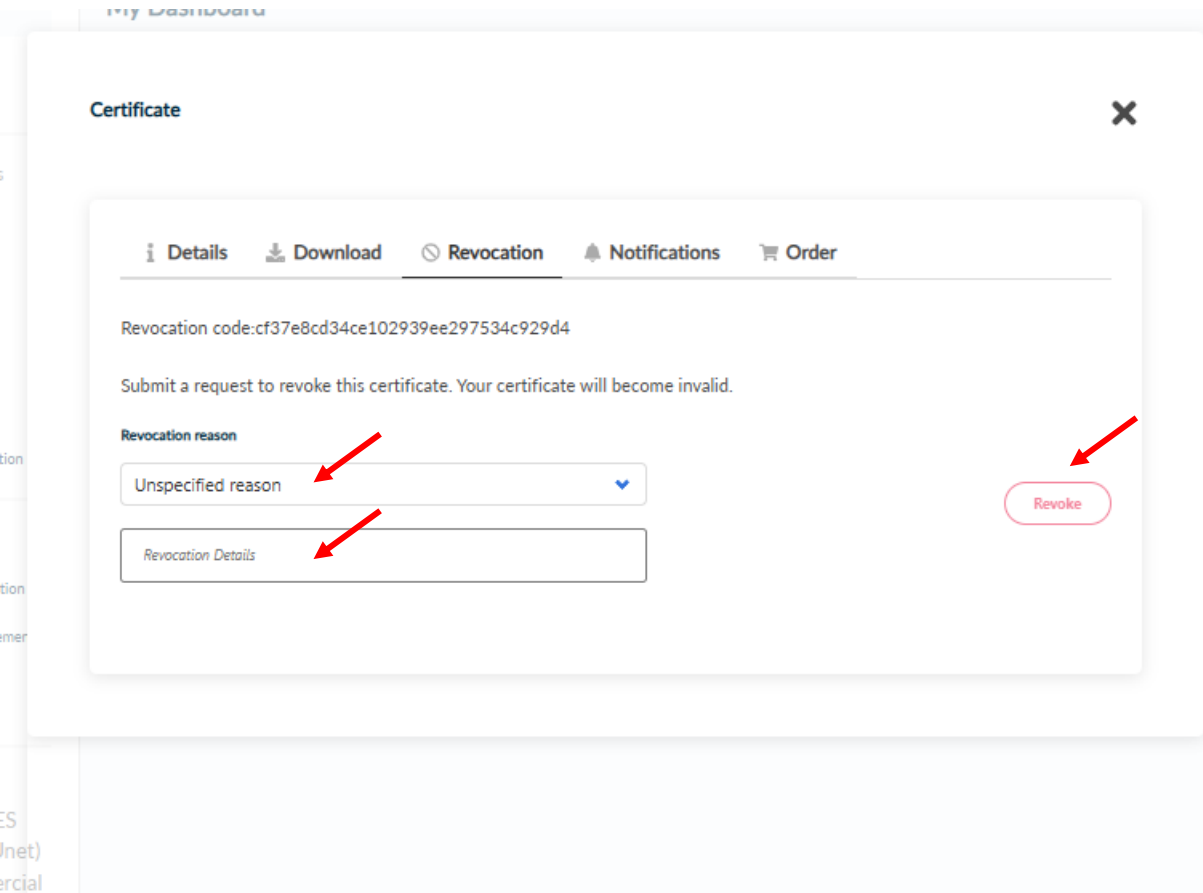


Product	Validity	Information	
S/MIME	21/04/2027	E=psimoes@fccn.pt	 
SSL OV	11/02/2026	Remoto Porto Fccn	 
SSL OV	06/02/2026	OTRS FCCN	 
SSL OV	06/02/2026	Gitlab FCCN	 
SSL DV	06/02/2026	teste eduroam 2	 

HARICA – Gerir Certificados: Pessoas

Revogar certificados

- Definir a causa
- Adicionar detalhes
- Escolher “Revoke”



My Dashboard

Certificate

Details Download Revocation Notifications Order

Revocation code:cf37e8cd34ce102939ee297534c929d4

Submit a request to revoke this certificate. Your certificate will become invalid.

Revocation reason

Unspecified reason

Revocation Details

Revoke

HARICA – Considerações gerais

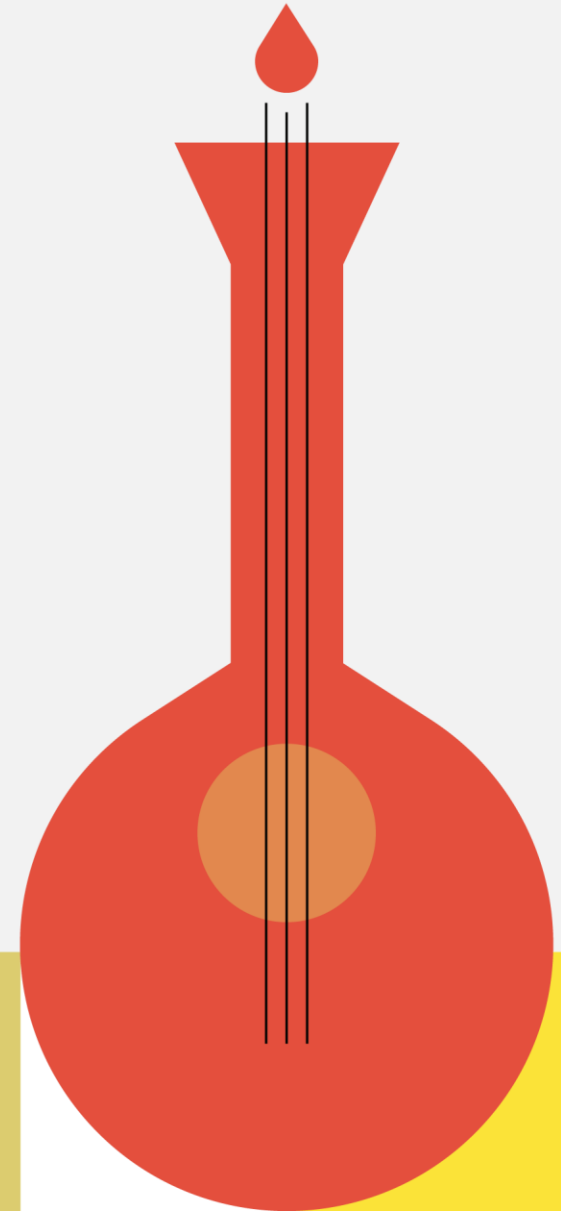
Considerações gerais

 **Segurança – 2FA**

 **Aprovação “por pares”**

 **Processo ongoing!!!!**

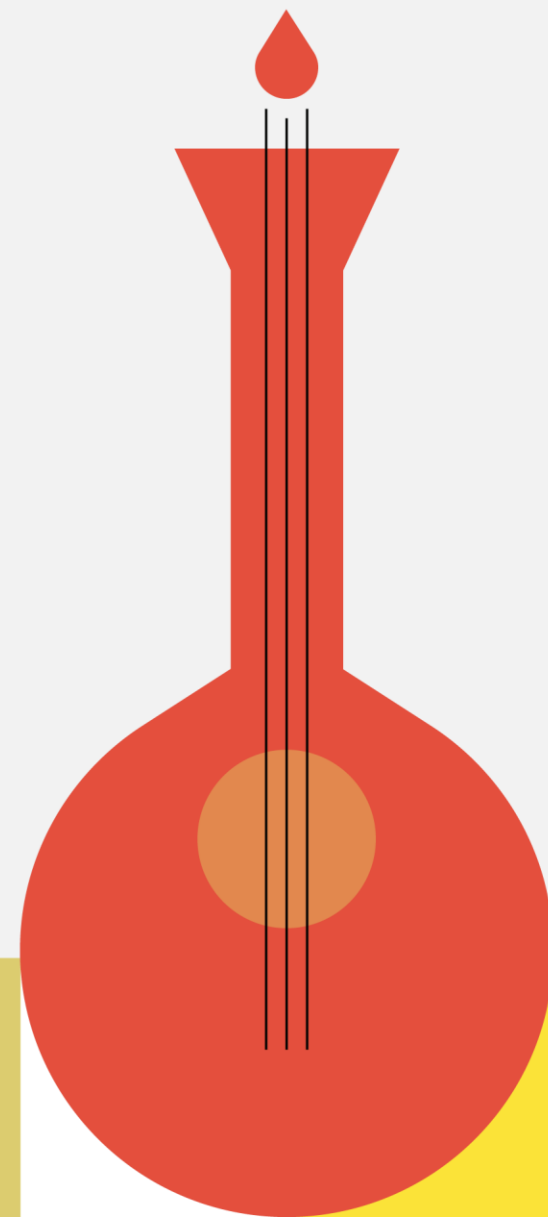




Apoio e Esclarecimentos

Estamos disponíveis, venham falar connosco!

Aqui e agora, ou mais tarde via noc@fccn.pt



Obrigado!

jornadas.fccn.pt

fccn.pt

