

Telefone direto: +351 212 948 596
Extensão interna: 15301

Correio eletrónico:
div.ii.helpdesk@fct.unl.pt

Serviço:
Segurança

Assunto:
**Pedido de emissão ou revogação de
certificado de servidor TCS**

**Reservado à Divisão de
Infraestruturas Informáticas**
Data de registo:

___ / ___ / ____

Número de registo interno:

Assinatura:

Data de suspensão para execução
futura:

___ / ___ / ____

Data de conclusão:

___ / ___ / ____

Assinatura:

Este formulário deverá ser entregue,
individualmente, na secretaria da
Divisão de Infraestruturas
Informáticas da FCT/UNL.

Quando existam, a validade do
pedido implica a aceitação dos
termos e condições do serviço em
anexo.

Para informações adicionais,
consulte <http://www.div-i.fct.unl.pt>.

Última revisão: 2018.01.04

Secretaria da Divisão de Infraestruturas Informáticas
Faculdade de Ciências e Tecnologia
2829-516 Caparica
Portugal

Identificação do Requerente

Nome completo: _____

Identificador no CLIP: _____

Departamento ou Divisão: _____

Telefone: _____

Endereço de correio eletrónico: _____

Identificação do responsável pelo pedido

Nome completo: _____

Identificador no CLIP: _____

Função: _____

O responsável pelo pedido deverá ser um presidente de departamento, director de centro de investigação ou o administrador da FCT/UNL.

Descrição do pedido

☐ Emissão de certificado

Serviço prestado pelo servidor: _____

Validade: ☐ 1 ano ☐ 2 anos ☐ 3 anos

Nome DNS do servidor (FQDN): _____

Nomes DNS adicionais (para certificados multi-domínio): _____

☐ Revogação de certificado

Nome DNS do servidor (FQDN): _____

Observações

Faculdade de Ciências e Tecnologia, ___ / ___ / ____

O Requerente

O Responsável pelo pedido

Instruções para criação de um pedido de certificado para o servidor

Neste documento encontra-se demonstrado o processo para criação de um pedido de certificado digital.

Gerar pedido de Certificado (CSR – Certificate Signing Request)

O processo de requisição de certificados inicia-se com a geração de um CSR, que será posteriormente submetido à entidade certificadora.

Como primeiro passo, deve ser gerado um ficheiro de configuração para o respetivo servidor. Mude o nome do ficheiro para o FQDN (Fully Qualified Domain Name) do servidor para o qual o certificado vai ser emitido (exemplo `www.dep.fct.unl.pt.cnf`).

O ficheiro deverá conter o seguinte conteúdo:

```
[ req ]
```

```
default_bits = 2048
```

```
prompt = no
```

```
encrypt_key = no
```

```
default_md = sha1
```

```
distinguished_name = req_distinguished_name
```

```
[ req_distinguished_name ]
```

```
C = PT
```

```
O = Universidade Nova de Lisboa
```

```
CN = www.dep.fct.unl.pt
```

```
emailAddress = div.ii.secretariado@fct.unl.pt
```

```
OU = FCT
```

```
L = Lisboa
```

Deverão adaptar apenas os campos a negrito

Depois de criado com sucesso o ficheiro de configuração, passa-se à geração do CSR propriamente dito. Para efetuar esse processo, basta executar os seguintes comandos (somente para sistemas *NIXs):

```
openssl req -new -config www.dep.fct.unl.pt.cnf -keyout  
www.dep.fct.unl.pt.key -out www.dep.fct.unl.pt.csr
```

Executado o comando anterior, será criado um par de chaves RSA de 2048 bits. A chave privada deste par encontra-se no ficheiro `www.dep.fct.unl.pt.key` (deve guardar este ficheiro de modo a que ninguém tenha acesso) e a chave pública no ficheiro www.dep.fct.unl.pt.csr.

O ficheiro com a extensão CSR deverá ser submetido juntamente com este pedido.