

1º Passo - Gerar o Certificate Signing Request (CSR)

O pedido de um certificado do tipo EV ou OV implica sempre que tenha sido criado previamente os ficheiros KEY e CSR.



Exemplo de CSR:

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBnTCCAQYCAQAwXTElMAkGA1UEBhMCU0cxETAPBgNVBAoTCE0yQ3J5cHRvMRIwEAYDVQQDEwlsb2NhbGhvc3QxJzAIBGkqhkiG9w0BCQEWGGFkbWluQHNIcnZici5IeGFtcGxhLnRvbnRzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArl1r
uB/FqICRRr5nvupdIN+3wF7q915tvEQoc74bnu6b8lbbGRMhgzdmvQ4SzFfVEAuM
MuTHeybPq5th7YDrTNizKKxOBnqE2KYuX9X22A1Kh49soJJFg6kPb9MUgiZBiMlv
tb7K3CHfgw5WagWnLI8Lb+ccvKZZI+8CAwEAAaAAMA0GCSqGSIb3DQEBAUA4GB
AHpoRp5YS55CZpy+wdigQEwjL/wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o8oEwi
PdrrliKNknFmHKlaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd09D1K
9rsQkRc9Urv9mRBlsredGnYECNeRaK5R1yzpOowninXC
-----END CERTIFICATE REQUEST-----
```

Campos a preencher no CSR (**Opcionais** / **Obrigatórios**):

C (country): PT

L (locality): Localidade

ST (state or province): Distrito

O (organization): Nome da organização de acordo com o protocolo

OU (organizational unit): Departamento

CN (common name): Deve corresponder ao FQDN ou lista de Domain Names

STREET (street address): Morada

E (E-mail address): Email Genérico (departamento@instituição)

Nota: Os campos opcionais quando preenchidos devem corresponder à informação do protocolo

A criação de certificados em Linux pressupõe que esteja instalada uma versão recente do software openssl.

Criar e/ou editar o ficheiro Openssl.conf

Devem criar ou editar, caso já existe, o ficheiro openssl.conf. Tipicamente este ficheiro está localizado na pasta /etc/ssl/.

```
vi /etc/ssl/openssl.cnf
```

Adicionar os campos

Devem adicionar os seguintes campos ao ficheiro openssl.conf.

Os campos referentes ao DN devem ser alterados a ajustados para a instituição que está a requerer o certificado.

De notar que os múltiplos domínios a serem usados devem ser definidos usando o campo **subjectAltName**. Deve sempre existir pelo menos um campo **CN**, onde é definido o domínio principal associado ao certificado, e os restantes devem seguir uma lógica numérica: DNS.1, DNS.2, DNS.3, etc.

```
[ req ]
default_bits = 2048
prompt = no
encrypt_key = no
default_md = sha256
distinguished_name = dn
req_extensions = v3_req

[ dn ]
C = pais
ST = rua
L = localidade
O = nome_da_organizacao
OU = nome_unidade_organica
CN = a.teste.fccn.pt
emailAddress = endereco@inst.pt

[ v3_req ]
# Extensions to add to a certificate request
subjectAltName = @alt_names

[alt_names]
DNS.1 = b.teste.fccn.pt
DNS.2 = c.teste.fccn.pt
DNS.3 = d.teste.fccn.pt
```

Gerar o CSR

Gerar a Chave Privada

```
openssl genrsa -des3 -out myserverkey.key 2048
```

Gerar o CSR com base na Chave Privada

```
openssl req -new -out server.csr -key myserverkey.key -config /etc/ssl/openssl.cnf
```

Validar o CSR e os vários domínios

```
openssl req -text -noout -in server.csr
```

Criar o ficheiro request.inf com os parâmetros necessários ao novo certificado. Devem alterar os valores dos seguintes campos:

- **O** = Colocar o nome da Entidade, conforme consta do serviço TCS
- **CN** = Colocar o FQDN da máquina
- **SAN** = Colocar os restantes nomes a serem usados no certificado. Este campo é também definido pelo OID 2.5.29.17 e deve aí contar os domínios adicionais.
- **OID** = Colocar o OID referente ao propósito para o qual o certificado é gerado. Pode ser consultada [aqui](#) uma lista completa dos OID's e respectivos propósitos

Server 2008 ou posterior

Para Windows Server 2008, Windows Server 2008 R2, Windows Vista ou Windows 7 deve ser usado o modelo abaixo para o ficheiro request.inf

```

;----- request.inf -----
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=a.teste.fccn.pt, OU=RCTSAAI, O=Fundacao para a Computacao Cientifica Nacional, L=Lisboa, S=Lisboa, C=PT" ; replace attributes in this line using example below
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
FriendlyName = "vdm"
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

[Extensions]
2.5.29.17 = "{text}"
_continue_ = "dns=b.teste.fccn.pt&dns=c.teste.fccn.pt"

[RequestAttributes]

;-----

```

Para Server 2003 ou anterior

Para Windows Server 2003, Windows Server 2003 R2 ou Windows XP deve ser usado o modelo abaixo para o ficheiro request.inf.

No caso desta versão do Windows, por não suportar os SAN na forma de texto, este valor deve ser convertido para Base64-encoded.

A string deve ser gerada no formato: [b.teste.fccn.pt,c.teste.fccn.pt](#)

Existem vários sites disponíveis na Internet para fazer esta codificação. A título de exemplo deixamos [este](#).

```

;----- request.inf -----

[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=a.teste.fccn.pt, OU=RCTSAAI, O=Fundacao para a Computacao Cientifica Nacional, L=Lisboa, S=Lisboa, C=PT" ; replace attributes in this line using example below
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

[Extensions]
; 2003 Server
2.5.29.17=Yi50ZXN0ZS5mY2NuLnB0LGMudGVzdGUuZmNjbi5wdA==
Critical=2.5.29.17
[RequestAttributes]
;-----

```

? Anexo Desconhecido

Gerar o CSR

Gerar Certificado

Numa janela de DOS executar o seguinte comando para gerar o certificado. Este comando deve ser executado na mesma directoria onde o ficheiro request.inf foi guardado.

```
certreq -new request.inf request.csr
```

Este comando deve ser executado numa janela de DOS com permissões de Administrador ou com um user com essas permissões.

? Anexo Desconhecido



Digicert Tools - CSR Generators

No portal Digicert está disponível mais informação como gerar um CSR: [Digicert Tools - CSR Generator](#)



Próximo Passo

Realizar o pedido no portal da digicert: [Preencher Formulário do Pedido](#)