ENTIDADE CERTIFICADORA
COMUM DO ESTADO

# Manual de Instruções
# para a
# Criação de Ficheiros CSR

## *Apache (OpenSSL)*

ceger
CENTRO DE GESTÃO
DA REDE INFORMÁTICA
DO GOVERNO
PORTUGAL

**CONTROLO DOCUMENTAL**

| REGISTO DE MODIFICAÇÕES | | | | |
|---|---|---|---|---|
| **Versão** | **Data** | **Motivo da Modificação** | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **PREPARADO** | | **REVISTO** | **APROVADO** | **ACEITE** |
| DUS/RS | | | | |
| | | | | |
| | | | | |
| | | | | |

| DISTRIBUIÇÃO DO DOCUMENTO | | |
|---|---|---|
| **Nome** | **Departamento** | **Entidade** |
| CERTIFICACAO | CERTIFICACAO | ECCE |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| VALIDADE E LOCALIZAÇÃO DO DOCUMENTO | | |
|---|---|---|
| **Versão** | **Entrada em vigor** | **Válido até** |
| 1.0 | 16/06/2014 | Próxima Revisão |
| | | |
| | | |
| | | |
| **Localização do Documento** | http://www.ecce.gov.pt/suporte/manuais.aspx | |

# Índice

## 1. Objetivo

Este manual tem como objetivo servir de guia aos utilizadores que vão solicitar certificados SSL à ***Entidade Certificadora Comum do Estado*** (*ECCE*). Em especial, neste manual, é abordada a criação de ficheiros de *Certificate Signing Request (CSR)* através de plataformas *Apache* utilizando *OpenSSL*, descrevendo-se os passos a seguir para o efeito.

## 2. Âmbito e Dever de Leitura

O âmbito deste documento é a geração de certificados SSL emitidos pela ***Entidade Certificadora Comum do Estado*** para a segurança de um ou mais *hostnames* (domínios, sites, …). Este manual deverá ser lido e conhecido por todos os utilizadores de certificados SSL que pretendam solicitar a emissão de certificados à ECCE.

## 3. Arquivo e Publicação

Este documento faz parte do repositório de documentação existente no *site* da *ECCE* em http://www.ecce.gov.pt/suporte/manuais.aspx, encontrando-se disponível em formato eletrónico para *download*. A responsabilidade pela manutenção, publicação e aprovação deste manual é da *Entidade Certificadora Comum do Estado*.

## 4. Referências

***OpenSSL***

http://www.ecce.gov.pt/media/2138/CSR-Apache.pdf

## 5. Instruções para a Criação do CSR (*Apache – OpenSSL*)

**IMPORTANTE**: Antes de proceder à criação do CSR, deverá sempre instalar previamente, na máquina que utilizar para a geração do ficheiro, os certificados intermédios da cadeia de certificação (ECCE e ECRaizEstado).

1. Faça login no servidor através do seu *terminal client* (*ssh*). Digite na *prompt*:

   ***openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr***

   Onde: ***server*** - é o nome do seu servidor;

2. Este comando inicia o processo de geração de dois ficheiros: o ficheiro da **chave privada** para a desencriptação do certificado SSL e o ficheiro de **CSR** (*certificate signing request*) (**CSR**) para a emissão do certificado SSL (com a*pache openssl*);

   Quando lhe for solicitado o ***Common Name*** (nome do domínio), deverá indicar o FQDN (*fully qualified domain name*) para o *site* em causa. Se está a gerar um *Apache CSR* para um certificado do tipo *Wildcard SSL*, o valor a introduzir neste campo deverá começar por um asterisco (ex.: *.organismo.com);

   Quanto à restante informação (*organizational information*), como é ocaso da informação geográfica, é habitual tratar-se de informação que já encontra por defeito definida;

   Este procedimento criará depois o ficheiro *openssl* *.csr;

3. Edite o texto do ficheiro *CSR* com um editor e verifique se gerou o *request* (incluindo as *tags* de BEGIN e END);

4. Faça *backup* do ficheiro *.key gerado, que será necessário mais tarde para a instalação do certificado emitido pela ECCE;

## 6. Importação do Ficheiro *.*pfx* para um Servidor *Apache*

Para mover um certificado SSL de um servidor *Apache* para outro servidor *Apache* basta efetuar um a cópia simples dos ficheiros da sua chave privada, do certificado do servidor e dos certificados intermédios da cadeia de certificação para o novo servidor, modificando depois o ficheiro de configurações apache para a utilização dos certificados copiados. É também possível mover certificados de servidores *windows* para *Apache* (ou outros servidores não *windows*) manipulando dos ficheiros dos certificados utilizando comandos *OpenSSL*. Esta secção explica como mover ficheiros de certificados *.pfx de um servidor *windows* para um servidor não *windows*. Os passos a realizar são:

1. Em primeiro lugar faça backup dos ficheiros dos certificados do servidor IIS para um ficheiro *.pfx, utilizando o seguinte comando *OpenSSL* seguinte:

   ***openssl pkcs12 -export -out backup.pfx -inkey ficheiro_chave_privada.txt -in dominio.crt -certfile certificado.crt***

   Este comando combina o certificado principal, certificados intermédios e a chave privada num ficheiro único *.*pfx*;

2. Utilize o seguinte comando *OpenSSL* para criar um ficheiro de texto individualizado com a chave privada:

   ***openssl pkcs12 -in ficheiro.pfx -out ficheiro_final.txt -nodes***

   Nota: O ficheiro *ficheiro.pfx* é o *backup* dos certificados do servidor IIS;

3. O passo anterior criará um ficheiro de texto *ficheiro_final.txt*. Abra-o com um editor de texto e verá a chave privada no início do ficheiro, com um formato aproximado ao seguinte:

   ```
   -----BEGIN RSA PRIVATE KEY-----

   < Bloco de texto >

   -----END RSA PRIVATE KEY-----
   ```

4. Copie e cole todo este texto, incluindo as *tags* de BEGIN e END para um novo ficheiro de texto. Guarde este ficheiro de texto como ***dominio.key***;

5. Instale os ficheiros gerados no seu novo servidor.