



ENTIDADE CERTIFICADORA
COMUM DO ESTADO

Manual de Instruções para a Criação de Ficheiros CSR

Microsoft Exchange 2007



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.....	3
2. Âmbito e Dever de Leitura.....	3
3. Arquivo e Publicação	3
4. Referências	3
5. Instruções para a Criação do CSR (<i>Microsoft Exchange 2007</i>)	4
6. Importação/Exportação do Certificado SSL no <i>Exchange 2007</i>	4
6.1. Exportação/<i>Backup</i> para um Ficheiro *.pfx	5
6.2. Importação a Partir de um Ficheiro *.pfx.....	5
6.3. Ativação do Certificado no Servidor.....	6

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 do *Microsoft Exchange 2007*, 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

Exchange 2007

<http://www.ecce.gov.pt/media/2168/CSR-Exch2007.pdf>

5. Instruções para a Criação do CSR (*Microsoft Exchange 2007*)

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. Dê o comando seguinte a partir da linha de comandos do **Exchange Management Shell**:

```
New-ExchangeCertificate -GenerateRequest -KeySize 2048 -Path c:\CSR.txt  
-SubjectName "c=PT, l=Cidade, s=Localidade, o=Organização,  
cn=primeiroDominio.pt" -DomainName segundoDominio.pt, terceiroDominio.pt  
-PrivateKeyExportable:$true
```

Notas: Este comando deverá ser uma linha única, devendo substituir os dados adaptando-os à sua Organização;

O primeiro nome de domínio é indicado na secção **-SubjectName** em **cn=** e os nomes de domínio adicionais são acrescentados depois do parâmetro **-DomainName** entre vírgulas (poderá adicionar tantos quantos os necessários);

2. O seu novo ficheiro de CSR com o nome CSR.txt está localizado na raiz da *drive* C. Este é o ficheiro a remeter à ECCE para posterior emissão do certificado SSL.

6. Importação/Exportação do Certificado SSL no *Exchange 2007*

Os servidores *Windows* utilizam ficheiros *.pfx para o armazenamento de ficheiros de chaves públicas (ficheiros de certificados SSL) e de chaves privadas a eles associados (gerados pelo servidor, fazendo parte integrante do CSR). Dado que, quer as chaves públicas, quer as chaves privadas, são essenciais para o correto funcionamento do certificado SSL, a transferência de certificados SSL de um servidor para outro(s) é feita através de um ficheiro *.pfx.

Esta secção descreve os passos necessários para efetuar o *backup* do certificado a partir de um servidor em produção, importá-lo para outro servidor e depois proceder à respetiva ativação no novo servidor.

6.1. Exportação/Backup para um Ficheiro *.pfx

1. No menu **Start**, clique em **Run** e escreva *mmc*;
2. Clique em **File** e depois **Add/Remove Snap-in**;
3. Faça **Certificates** e depois **Add** e feche depois a janela **Add Standalone Snap-in window**. Clique em **OK**;
4. Selecione **Computer Account** e clique em **Next**. Selecione **Local Computer** e faça **Finish**. Feche depois as janelas **add standalone snap-in** e **add/remove snap-in**;
5. Clique em '+' para expandir a árvore da consola dos certificados (**local computer**) e procure a pasta pessoal (**personal directory/folder**). Expanda a pasta dos certificados;
6. Clique com o botão direito do rato no certificado de que se pretende fazer **backup** e selecione **ALL TASKS** e depois **Export**;
7. Siga as instruções do **wizard** para a exportação do certificado para um ficheiro *.pfx. Escolha a opção **Yes, export the private key**;
8. Deixe as configurações de **default** e insira a sua **password** se solicitado. Escolha a localização para salvar o ficheiro e clique depois em **Finish**. Receberá uma mensagem de exportação com sucesso.

6.2. Importação a Partir de um Ficheiro *.pfx

1. No menu **Start** clique em **Run** e escreva *mmc*;
 2. Clique em **File** e depois em **Add/Remove Snap-in**;
 3. Clique em **Certificates** e depois em **Add**, fechando em seguida a janela **Add Standalone Snap-in**. Clique em **OK**;
 4. Selecione **Computer Account** e clique depois em **Next**. Selecione **Local Computer** e clique depois em **Finish**. Em seguida feche as janelas **Add Standalone Snap-in** e **Add/Remove Snap-in**;
-

5. Clique no '+' para expandir a árvore da consola dos certificados (**local computer**) e procure a pasta pessoal (*personal directory/folder*). Expanda a pasta dos certificados;
6. Clique com o botão direito do rato na pasta *Personal Certificates Store* e selecione **ALL TASKS** e depois **Import**;
7. Siga as instruções do *wizard* para importar o certificado a partir do ficheiro *.pfx. Quando solicitado, indique que os certificados deverão ser automaticamente colocados nas *stores* com base no tipo de certificado.

6.3. Ativação do Certificado no Servidor

1. Para obter o **thumbprint** do certificado, corra o seguinte comando, adaptando o nome do **domínio** para o seu caso:

```
C:\> Get-ExchangeCertificate -DomainName oseudominio
```

Thumbprint	Services	Subject
-----	-----	-----
123449A1911919F2753354AEP76C7D5DB1E4A123	N=oseudominio

2. Para a ativação do certificado para utilização no Exchange, corra o comando seguinte, alterando os serviços de acordo com o *thumbprint* do certificado:

```
Enable-ExchangeCertificate -ThumbPrint -Services "SMTP, IMAP, POP, IIS"
```

3. Poderá correr de novo o comando **Get-ExchangeCertificate** para verificar se o certificado foi devidamente instalado;

Nota: Na coluna **Services**, **SIP** e **W** representam SMTP, IMAP, POP3 e IIS.

4. Deverá efetuar testes ao seu certificado utilizando o *Internet Explorer*, o *ActiveSync* ou o *Outlook* (se está a utilizar o *ISA 2004* ou o *ISA 2006* poderá ter de reiniciar o servidor).