



ENTIDADE CERTIFICADORA
COMUM DO ESTADO

Manual de Instruções para a Criação de Ficheiros CSR

Microsoft IIS 5/6



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>Internet Information Services 5/6</i>)	4
6. Transferência de Ficheiros de Certificados do IIS 5/6	5
6.1. Exportação/<i>Backup</i> para um Ficheiro .pfx	5
6.2. Importação de um Ficheiro .pfx	6
6.3. Ativação de um Novo Certificado num Servidor	7

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 Internet Information Services (IIS) 5 ou IIS 6*, 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

IIS 5/6


<http://www.ecce.gov.pt/media/2105/CSR-IIS56.pdf>

	<p>Manual de Instruções para a Criação de Ficheiros CSR</p> <p>Microsoft IIS 5/6</p>	<p>Página 4 de 8</p>
---	--	----------------------

5. Instruções para a Criação do CSR (*Internet Information Services 5/6*)

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. Clique em **Start, Administrative Tools** e abra depois o **Internet Information Services (IIS)**;
 2. Com o botão direito do rato sobre o *website*, selecione **Properties**. Clique no separador **Directory Security** e depois no botão **Server Certificate**;
 3. Clique em **Next**.
 4. Escolha **Create a new certificate** e faça **Next**;
No caso de pretender renovar um certificado já existente, as opções disponíveis serão **Renew, Remove e Replace**. Escolha a opção **Renew** e ignore os passos 5 a 8.
 5. Escolha a opção **Prepare the request now, but send it later** e faça **Next**;
 6. Escolha um nome para o certificado e um *bit-length* mínimo de 2048 (Deixe as restantes *checkboxes* desmarcadas);
 7. Preencha a informação necessária nos campos:
Company – Nome do Ministério/Organização;
Organizational unit – Nome do Departamento/Entidade;
FQDN – *Fully-qualified domain name* do site (Ex.: [www.dominio.gov.pt](#));
Location – Dados da Localização (*Country, State e City*);
 8. Escolha o nome a atribuir ao ficheiro de CSR a gerar (o ficheiro deverá ser de texto - .txt);
 9. Faça **Next** (o ficheiro é gerado);
 10. Para a emissão do certificado, remeta uma cópia do ficheiro gerado para a ECCE (certificacao@ecce.gov.pt).
-

 <p>ceger CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO PORTUGAL</p>	<p>Manual de Instruções para a Criação de Ficheiros CSR</p> <p>Microsoft IIS 5/6</p>	<p>Página 5 de 8</p>
--	--	----------------------

Nota: Com a criação do ficheiro CSR é também criado um *pending request* no respetivo *website*, que não deve nunca apagar. Mais tarde, já na posse do novo certificado, é através deste pedido pendente que irá importar o novo certificado.

6. Transferência de Ficheiros de Certificados do IIS 5/6

Os servidores Windows utilizam ficheiros com a extensão *.pfx* para o armazenamento dos ficheiros de chaves públicas (ficheiros dos certificados SSL) e dos correspondentes ficheiros das chaves privadas que são geradas pelo servidor como parte do ficheiro de CSR. Dado que, quer as chaves públicas, quer as chaves privadas, são necessárias para o bom funcionamento do certificado SSL é necessário criar um *backup* do ficheiro *.pfx para transferir os certificados de segurança SSL de um servidor para outro(s).

Esta secção descreve os passos a dar para efetuar o *backup* de um certificado que está a funcionar num servidor em produção (com o SSL a funcionar) para que possa ser utilizado noutra servidor.


6.1. Exportação/*Backup* para um Ficheiro .pfx

1. No menu **Start** escolha **Run** e escreva *mmc*;
 2. Clique em **File > Add/Remove Snap-in**;
 3. Em seguida clique em **Add > Certificates > Add**;
 4. Selecione a conta do computador e clique em **Next**;
 5. Selecione **Local Computer** clique em **Finish**. Feche as janelas **add standalone snap-in** e **add/remove snap-in**;
 6. Clique em “+” para expandir a árvore da consola dos certificados (**local computer**) e pesquise a diretoria/pasta **personal**. Expanda a pasta dos Certificados;
-

7. Clique com o botão direito do rato no certificado que pretende fazer backup e seleccione **ALL TASKS > Export**;
8. Escolha **Yes**, exporte a chave privada e, se possível, inclua todos os certificados da cadeia de certificação (**certificate path**). Certifique-se de que a opção **delete private key** não está seleccionada;
9. Deixe ficar as definições por defeito e insira a sua *password* se necessário;
10. Escolha salvar o ficheiro e depois clique em **Finish**. Deverá ser notificado do sucesso da exportação.

6.2. Importação de um Ficheiro .pfx

1. Através do menu Start, clique em **run** e escreva *mmc*. Faça **Enter**;
 2. Clique em **File > Add/Remove Snap-in**;
 3. Clique em **Add > Certificates > Add**;
 4. Seleccione **Computer Account** e faça **Next**. Seleccione **Local Computer** e faça **Finish**. Feche as janelas de **add standalone snap-in** e de **add/remove snap-in**;
 5. Expanda os certificados, clicando em “+” na árvore da consola em **local computer** e localize a diretoria/pasta pessoal. Expanda a pasta dos certificados;
 6. Clique com o botão direito do rato sobre o certificado que pretende fazer backup e seleccione **All Tasks > Import**;
 7. Siga as instruções do *wizard* para importar o seu certificado primário a partir do ficheiro pfx. Quando lhe for solicitado, escolha a colocação
-

 <p>ceger CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO PORTUGAL</p>	<p>Manual de Instruções para a Criação de Ficheiros CSR</p> <p>Microsoft IIS 5/6</p>	<p>Página 7 de 8</p>
--	--	----------------------

automática dos certificados nas *stores* de certificados com base no tipo de certificado.

6.3. Ativação de um Novo Certificado num Servidor

1. No menu **Start** clique em **Administrative Tools > Internet Information Services (IIS Manager)**;
 2. No *IIS manager*, clique com o botão direito do rato sobre o site em que pretende utilizar o certificado e seleccione **Properties**;
 3. Faça **Directory Security > Server Certificate**. O *wizard* de certificado deverá iniciar-se;
 4. Escolha, caso possível, a designação de um certificado existente ao *site* e seleccione o certificado que pretende importar;
 5. Caso essa opção não esteja disponível, ser-lhe-á perguntado o que pretende fazer com o certificado atual do *site*. Escolha a opção para substituir o certificado atual;
 6. Procure o ficheiro pfx que criou previamente e conclua o *wizard* seguindo as instruções do mesmo. Reinicie o serviço IIS no servidor e verifique se o novo certificado é reconhecido pela máquina.
-