



ENTIDADE CERTIFICADORA
COMUM DO ESTADO

Manual de Instruções para a Criação de Ficheiros CSR

Tomcat com Keystore e Keytool



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>Tomcat com Keystore</i>)	4
5.1. Criação de uma Nova <i>Keystore</i>	4
5.2. Geração do CSR para a Nova <i>Keystore</i>	4
6. Instruções para a Criação do CSR (<i>Webservers baseados em Java</i>)	5
Como gerar o CSR utilizando o <i>Java Keytool</i>	5
6.1. Criação de uma Nova <i>Keystore</i>	5
6.2. Geração do Ficheiro de CSR para a Nova <i>Keystore</i>	5

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 *Tomcat* e *keystore* e servidores baseados em *Java* utilizando a ferramenta *keytool*, 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

Keytool

<http://www.ecce.gov.pt/media/2144/CSR-Tomcat.pdf>

	<p>Manual de Instruções para a Criação de Ficheiros CSR</p> <p><i>Tomcat com Keystore e Keytool</i></p>	<p>Página 4 de 6</p>
---	---	----------------------

5. Instruções para a Criação do CSR (*Tomcat com Keystore*)

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).

5.1. Criação de uma Nova *Keystore*

1. Deverá utilizar o comando *keytool* para criar e gerir a sua nova *Keystore*. Poderá necessitar de adicionar a diretoria *java /bin/* à sua *path* para que o comando *keytool* seja reconhecido. Quando estiver em condições de criar a *keystore*, dê o comando seguinte (na diretoria onde pretende gerir a *keystore* e os certificados):

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore o_seu_site.jks
```

2. Ser-lhe-á solicitada uma *password* para a sua *keystore*. Em seguida deverá inserir a informação referente à sua Organização;

Quando for solicitado o ***first and last name***, deverá inserir o ***Fully Qualified Domain Name (FQDN)*** do site em causa (ex.: *www.dominio.gov.pt*). No caso de pretender emitir um certificado do tipo *Wildcard*, o FQDN deverá começar por um asterisco (ex.: **.dominio.pt*);

3. Depois de ter inserido a informação necessária, confirme quando solicitado com um 'y' ou 'yes'. Em seguida ser-lhe-á solicitada a *password* para confirmação;

O ficheiro da sua nova *keystore*, com o nome ***o_seu_site.jks***, foi criado na diretoria atual (diretoria de trabalho);

5.2. Geração do CSR para a Nova *Keystore*

1. Para a criação do ficheiro de CSR (*Certificate Signing Request*) para a nova *Keystore*, deverá utilizar a aplicação *keytool*, inserindo o comando seguinte:

```
keytool -certreq -alias server -file csr.txt -keystore o_seu_site.jks
```

2. Insira a *password* da *keystore* que escolheu previamente e faça **Enter**;
3. O CSR foi criado na diretoria corrente com o nome **csr.txt**. Este é o ficheiro a remeter à ECCE para emissão do certificado respetivo.

6. Instruções para a Criação do CSR (*webservers baseados em Java*)

Como gerar o CSR utilizando o *Java Keytool*

NOTA: Para seguir este processo terá de criar uma nova *keystore*. Se for instalado um novo certificado numa *keystore* já existente, é muito provável que o certificado não funcione bem.

6.1. Criação de uma Nova *Keystore*

1. Para utilizar o comando *keytool* para a criação de um novo par **chave-CSR**, digite a seguinte linha de comando:

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore dominio.jks
```

2. Ser-lhe-á solicitada a informação acerca do nome do domínio (**DN**). Quando for solicitado o **first and last name**, o que deverá inserir é o nome do domínio e respetiva extensão (ex.: *www.organismo.gov.pt*);

Nota: No caso de pretender a emissão de um *wildcard* deverá começar por * (ex.: **.organismo.pt*);

3. Confirme a inserção da informação requerida digitando 'y' ou 'yes' quando pedido. Ser-lhe-á solicitada a *password* para confirmação.

6.2. Geração do Ficheiro de CSR para a Nova *Keystore*

1. A criação do ficheiro de CSR utilizando *keytool* é efetuada através do comando seguinte:

```
keytool -certreq -alias server -keyalg RSA -file dominio.csr -keystore dominio.jks
```

2. Insira a *password* da *keystore* assim que solicitado;
 3. O ficheiro CSR criado deverá ser remetido à ECCE para emissão do certificado.
-