
	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE		EXT-TEC-200006	
			VERSIÓN	1.0
			FECHA	13/06/01

EXT-TEC-200006
SOLICITUD DE
CERTIFICADO DE SERVIDOR SEGURO
PARA UN SERVIDOR ORACLE

AC CAMERFIRMA - NIF: A 82743287		USO: PÚBLICO	Página 1 de 6
CI Velázquez, 157 28002 - Madrid		PI Catedral, 11 05001 - Ávila	


	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE	EXT-TEC-200006	
		VERSIÓN	1.0
		FECHA	13/06/01

CONTROL DE ACTUALIZACIONES

EX-TEC-200006

SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE

VERSIÓN	FECHA	ELABORADO	REVISADO	APROBADO
1.0	13/06/2001	Dto. Técnico		

	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE	EXT-TEC-200006	
		VERSIÓN	1.0
		FECHA	13/06/01

Generar el CSR (Petición de Firma de Certificado) Certificate Signing Request

En este primer paso, generaremos una petición para Camerfirma para emitir un certificado.

Esto implica generar un par de claves e identificar el servidor, la organización que lo está utilizando, y la persona que lo maneja. La clave privada se encripta y nunca debe salir del servidor (salvo para copias de seguridad). La clave pública será parte del certificado, y consecuentemente se enviará a Camerfirma, junto con el resto de información que identifica a su organización y a su servidor.

Para generar una petición de certificado, es necesaria la herramienta interactiva *genreq* y proporcionarle a esta la información que solicita.


Vamos a ver un ejemplo del uso de *genreq*.

Antes de empezar, debemos crear un directorio para almacenar todos los ficheros relacionados con SSL, por ejemplo, `$ORACLE_HOME/ows2/ssl`. Para evitar teclear nombres y rutas demasiado largas, podemos arrancar *genreq* desde este directorio.

Para utilizar *genreq*:


- Arrancar *genreq*, localizado en `$ORACLE_HOME\OWS20\BIN` en NT (generalmente `c:\orant\ows20\bin`) y `$ORACLE_HOME/ows2/bin` en UNIX.
- Teclee G para empezar a crear la petición.
- Cuando se le pida, teclee una contraseña (mínimo 8 caracteres), que será utilizada para encriptar su clave privada. Recuerde esta contraseña.

AC CAMERFIRMA - NIF: A 82743287	USO: PÚBLICO	Página 3 de 6
CI Velázquez, 157 28002 - Madrid	PI Catedral, 11 05001 - Ávila	

	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE	EXT-TEC-200006	
		VERSIÓN	1.0
		FECHA	13/06/01

- Vuelva a teclear la contraseña para confirmarla. Si las contraseñas no concuerdan, *genreq* no le avisará, simplemente las volverá a solicitar.
- Elija el exponente público que desee utilizar para generar el par de claves. Los dos únicos exponentes reconocidos son 3 y 65537, también conocido como Fermat 4 o F4.
- Introduzca el tamaño en bits del módulo que desee utilizar para generar el par de claves. Dependiendo de las versiones el tamaño máximo varía. Para la mayoría versiones distribuidas en Europa, el tamaño máximo (y por defecto) es de 512 bits. Consulte la documentación de su servidor para establecer el tamaño máximo.
- Elija entre uno de los tres métodos para generar una semilla aleatoria para generar el par de claves.
 - Fichero Aleatorio: *genreq* le solicitará que introduzca el path completo de un fichero de su sistema de archivos local. Este puede ser cualquiera que al menos tenga un tamaño de 256 bytes, que no contenga ninguna información secreta y cuyo contenido no sea fácilmente "adivinable" (en UNIX, puede usar `/var/adm/messages`, en NT puede usar `\WINNT\System32\config\AppEvent.Evt`)
 - Secuencias de teclado aleatorias: *genreq* le solicita la entrada de una secuencia cualquiera de pulsaciones de teclado. *genreq* utiliza las diferencias de tiempo entre las pulsaciones para generar la semilla. No utilice las funciones del teclado para repetir texto, y no espere más de dos segundos entre cada pulsación. *genreq* le avisará cuando haya realizado un número de pulsaciones suficiente. Debe borrar cualquier carácter tecleado que no se haya utilizado después de este aviso.
 - Ambos métodos combinados: *genreq* le solicita el path de un fichero y una secuencia aleatoria de pulsaciones. Esta opción es la más recomendable.


AC CAMERFIRMA - NIF: A 82743287	USO: PÚBLICO	Página 4 de 6
Cl Velázquez, 157 28002 - Madrid	Pl Catedral, 11 05001 - Ávila	

	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE	EXT-TEC-200006	
		VERSIÓN	1.0
		FECHA	13/06/01

En los siguientes tres pasos, habrá que indicarle a *genreq* dónde debe crear ciertos ficheros. Si ha creado un directorio para SSL y ha arrancado *genreq* desde este directorio, puede aceptar los valores por defecto. De otro modo, debe indicar los paths completos, o en un futuro, mover los archivos creados por *genreq*.

- Proporcione el nombre del fichero en el que vaya a almacenar su "distinguished name" (nombre distintivo) del servidor web. Puede elegir uno por defecto o introducir cualquier nombre con la extensión **.der**. La herramienta *genreq* crea este fichero en el directorio actual, posteriormente se puede mover a cualquier otra localización.
- Proporcione el nombre del fichero en el que vaya a almacenar la clave privada del servidor web. Al igual que en el caso anterior el archivo ha de tener la extensión **.der**.
- Proporcione el nombre del fichero en el cual vaya a almacenar la solicitud de certificado. En este caso la extensión debe ser **.pkc**.
- Introduzca la información de identificación de su organización o empresa que se le solicita:
 - o CN - Common Name: o nombre común, el nombre completo del punto de presencia en internet definido por el servicio de nombres de dominio (DNS). Ejemplo: www.camerfirma.com
 - o OU - Organizational Unit (opcional): o unidad organizacional, el nombre del grupo, división, u otra unidad de su organización responsable de su presencia en internet. Ejemplo: Departamento Técnico.

AC CAMERFIRMA - NIF: A 82743287	USO: PÚBLICO	Página 5 de 6
Cl Velázquez, 157 28002 - Madrid	Pl Catedral, 11 05001 - Ávila	

	SOLICITUD DE CERTIFICADO DE SERVIDOR SEGURO PARA UN SERVIDOR ORACLE	EXT-TEC-200006	
		VERSIÓN	1.0
		FECHA	13/06/01

- O - Organization : u organización, el nombre oficial o legal de su compañía u organización. Ejemplo: AC Camerfirma
- Locality (opcional). La ciudad donde se encuentra localizada su organización. Ejemplo: Ávila
- State or Province: estado o provincia en el que se encuentre localizada su organización. Ejemplo: Ávila
- CO – Country: los dos caracteres de la abreviación ISO del nombre del país en el que está localizada su organización. Ejemplo: ES
- WebMaster´s Name: o nombre del Web Master responsable del sitio web. Esta persona será el contacto técnico. Ejemplo: Luis Duque.
- WebMaster´s Email Address: o correo electrónico del Web Master. Ejemplo: luis_duque@camerfirma.com
- Server Software Versión: o versión del software del servidor. El nombre y la versión del software para el cual está solicitando el certificado. (generalmente, deberá aceptar el valor por defecto)

Una vez que ha generado el fichero CSR, debe pegar su contenido en el formulario de petición de certificado de servidor en la web de Camerfirma.

www.camerfirma.com

AC CAMERFIRMA - NIF: A 82743287	USO: PÚBLICO	Página 6 de 6
Cl Velázquez, 157 28002 - Madrid	Pl Catedral, 11 05001 - Ávila	