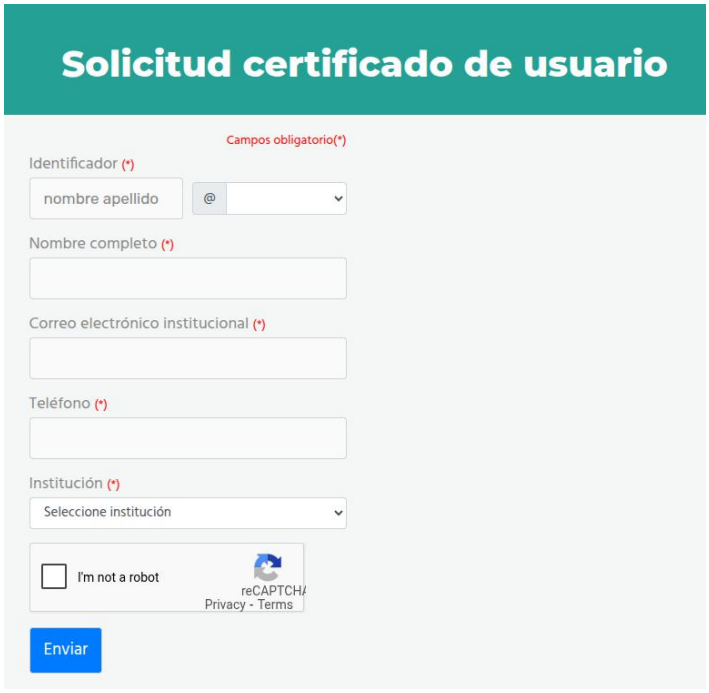
Cómo solicitar un certificado

Paso previo: Estar validado para solicitar un certificado, de acuerdo con lo establecido en la sección Validación del Solicitante disponible en https://reuna-ca-n.reuna.cl/procedimientos/

1. Ir a https://reuna-ca-n.reuna.cl/procedimientos/ y acceder a la sección Solicitud de Certificados y seleccionar el certificado que corresponde

2. Llenar el formulario con la información solicitada dependiendo del certificado a solicitar

a) En el caso de certificado de usuario
   i. Identificador: nombre.apellido@institución
   ii. Nombre completo del solicitante
   iii. Correo electrónico (este debe ser institucional)
   iv. Teléfono
   v. Institución

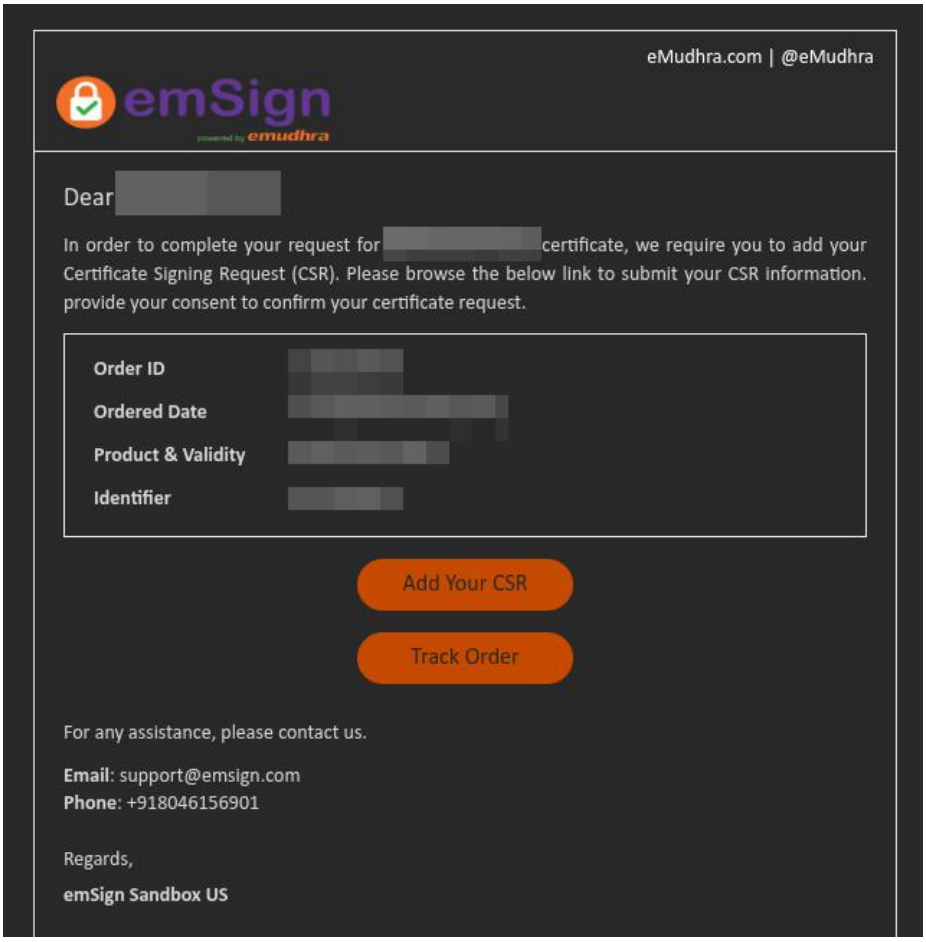


b) En el caso de certificado de servidor
   i. Identificador: nombre-servidor.institución
   ii. Nombre completo del solicitante
   iii. Correo electrónico (este debe ser institucional)
   iv. Teléfono

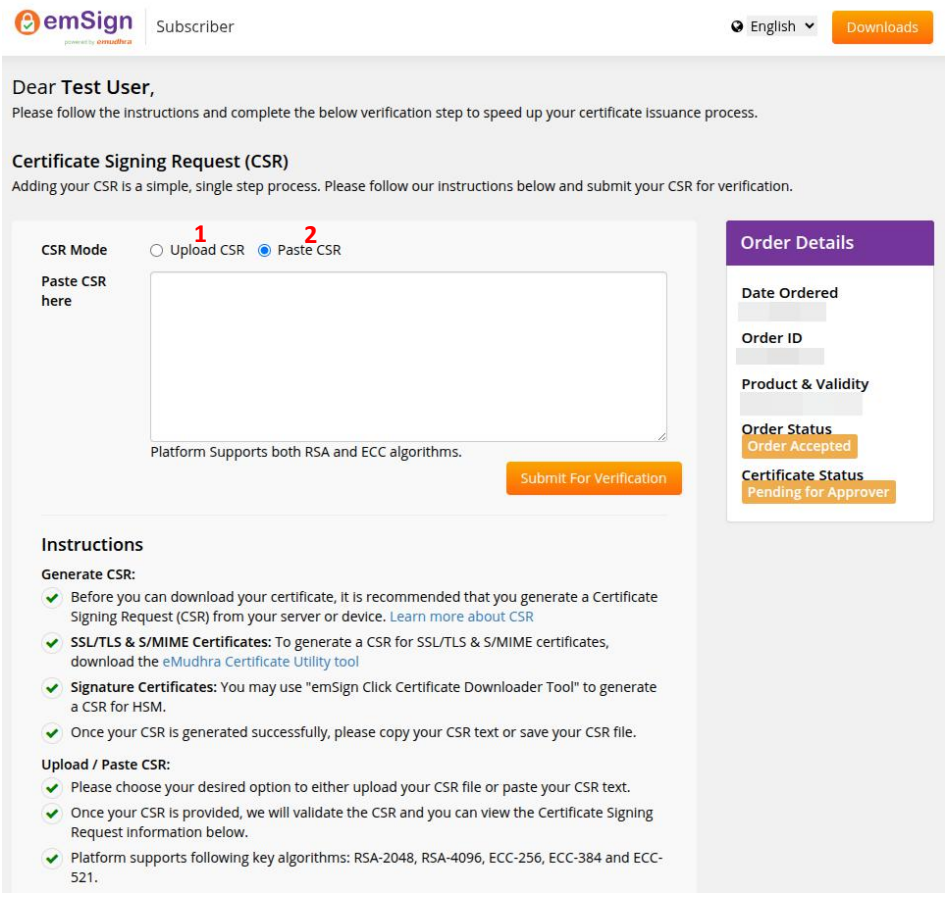
v. Institución

3. Una vez completado el formulario, completar el CAPTCHA y hacer clic en Enviar

4. Una vez aprobado el certificado, llegará un correo desde *emSign@emudhra.com* con el asunto - *ORDER #(número) - Add your Certificate Signing Request (CSR)*, el cual tiene el siguiente contenido

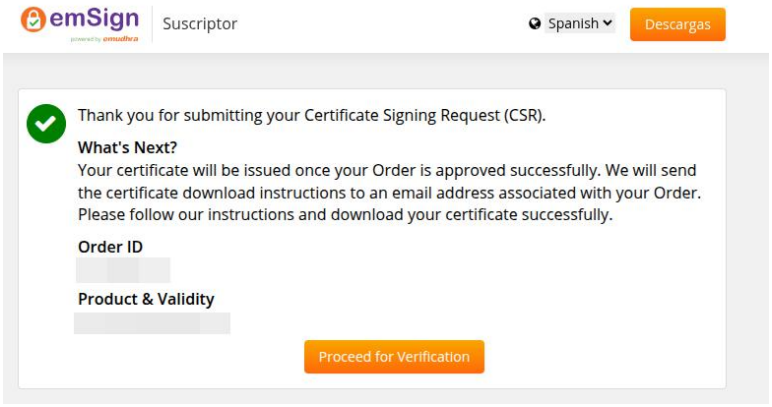


5. Hacer clic en Add Your CSR para subir la solicitud de firma del certificado, a lo que se abrirá el siguiente sitio en el navegador

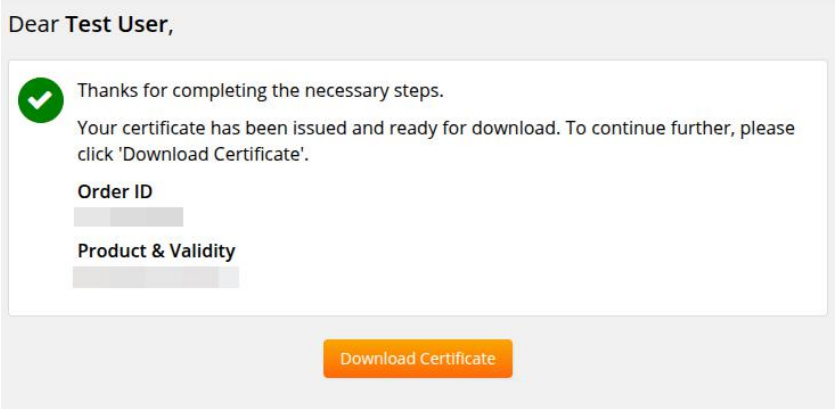


6. Para subir un archivo CSR, seleccionar la opción *Upload CSR* (Ver 1 en la imágen anterior) y seleccionar el archivo. Para pegar el contenido del CSR, seleccionar *Paste CSR* (Ver 2 en la imágen anterior), pegar el contenido del CSR en el cuadro de texto y hacer clic en *Submit For Verification*.
NOTA: Considerar que cuando se genera el CSR, se genera también la llave privada del certificado, por lo que se **solicita guardar todos los archivos generados**. Para generar un CSR ir al anexo al final de este documento

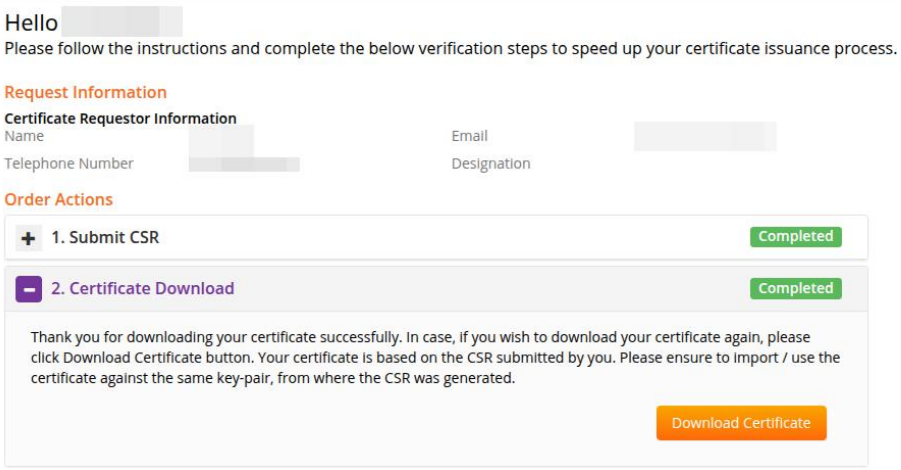
7. Una vez que el CSR ha sido verificado, aparecerá un mensaje que indica que para obtener el certificado solicitado se debe hacer una verificación, con la cual se enviará el certificado al correo indicado en la solicitud. Para realizar dicha verificación, hacer clic en *Proceed for Verification*



8. Finalmente aparecerá un mensaje donde se podrá descargar el certificado solicitado. Para ello, hacer clic en *Download Certificate*.



9. También llegará un correo de confirmación donde se podrá hacer seguimiento a la orden y acceder a descargar el certificado.



Anexo: Generar un CSR

Windows

1. Descargar OpenSSL para Windows de https://slproweb.com/products/Win32OpenSSL.html

2. Instalar siguiendo el asistente de instalación (Nota: Para saltar la parte de donación, desmarcar las opciones que estén con ticket)
3. Abrir cmd y escribir cd C:\Archivos de Programa\OpenSSL-Win64\bin\
4. En el directorio ejecutar `openssl.exe req -out` **<nombre-csr>** `-new -sha256 -newkey rsa:2048 -nodes -keyoout` **<nombre-key>**

   Donde:

   <nombre-csr>: Nombre del archivo con extensión csr. E.g.: Certificado de usuario Juan Perez juan-perez.csr

   <nombre-key>: Nombre del archivo de llave privada. E.g.: Certificado de usuario Juan Perez juan-perez.key
5. Seguir el asistente interactivo e ir respondiendo:

   Country Name: Código del país, para Chile corresponde CL

   State or Province Name: Región del país, sin acentos ni ñ o ü.

   Locality Name: Cuidad, sin acentos ni ñ o ü.

   Organization Name: Nombre de la institución, sin acentos ni ñ o ü.

   Organization Unit Name: Sección dentro de la institución, sin acentos ni ñ o ü.

   Common Name: Nombre de red (e.g. servidor.institucion.cl) o identificador del solicitante (nombre.apellido@institucion.cl).

   Email address: Correo institucional del solicitante.

   A challenge password: Opcional, si se usa, favor recordar. Para dejar en blanco, presionar Enter

   An optional Company Name: Opcional. Para dejar en blanco, presionar Enter
6. Para ver el archivo, abrir con notepad el CSR, en el directorio C:\Archivos de Programa\OpenSSL-Win64\bin\ y pegar el contenido en el punto 5 del manual.

Linux

1. Abrir una consola y ejecutar el siguiente comando: `openssl req -out` **<nombre-csr>** `-new -sha256 -newkey rsa:2048 -nodes -keyoout` **<nombre-key>**

   Donde:

   <nombre-csr>: Nombre del archivo con extensión csr. E.g.: Certificado de usuario Juan Perez juan-perez.csr

   <nombre-key>: Nombre del archivo de llave privada. E.g.: Certificado de usuario Juan Perez juan-perez.key
2. Seguir el asistente interactivo e ir respondiendo:

   Country Name: Código del país, para Chile corresponde CL

   State or Province Name: Región del país, sin acentos ni ñ o ü.

   Locality Name: Cuidad, sin acentos ni ñ o ü.

   Organization Name: Nombre de la institución, sin acentos ni ñ o ü.

   Organization Unit Name: Sección dentro de la institución, sin acentos ni ñ o ü.

   Common Name: Nombre de red (e.g. servidor.institucion.cl) o identificador del solicitante (nombre.apellido@institucion.cl).

   Email address: Correo institucional del solicitante.

   A challenge password: Opcional, si se usa, favor recordar. Para dejar en blanco, presionar Enter

   An optional Company Name: Opcional. Para dejar en blanco, presionar Enter
3. Para ver el archivo, abrir con un editor de texto, ya sea por consola (nano, vim, etc.) o con editor de texto (gedit, mousepad, etc.)