

## 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

The screenshot shows a light gray background with a dark blue header bar at the top containing the text "SOLICITUD DE CERTIFICADOS". Below the header, there is a message in Spanish: "Si ya te encuentras validado como usuario, puedes hacer tu solicitud de certificado ingresando a los siguientes enlaces". Underneath this message are two main options: "Solicitar certificado de usuario" on the left and "Solicitar certificado de servidor" on the right. Each option has an associated icon: a shield-like shape with a person icon for the user certificate and two server racks for the server certificate.

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

The screenshot shows a teal header bar with the text "Solicitud certificado de usuario". Below the header is a section titled "Campos obligatorio(\*)". The form contains five input fields: "Identificador (\*)" (with a dropdown menu for selecting an institution), "Nombre completo (\*)", "Correo electrónico institucional (\*)", "Teléfono (\*)", and "Institución (\*)" (with a dropdown menu). At the bottom of the form is a reCAPTCHA verification box with the text "I'm not a robot" and a checkbox, followed by a link "reCAPTCHA Privacy - Terms". A large blue "Enviar" button is located at the bottom left of the form area.

- 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

## Solicitud certificado de servidor

Campos obligatorio(\*)

Identificador (\*)

nombre del servicio

Nombre completo (\*)

Correo electrónico institucional (\*)

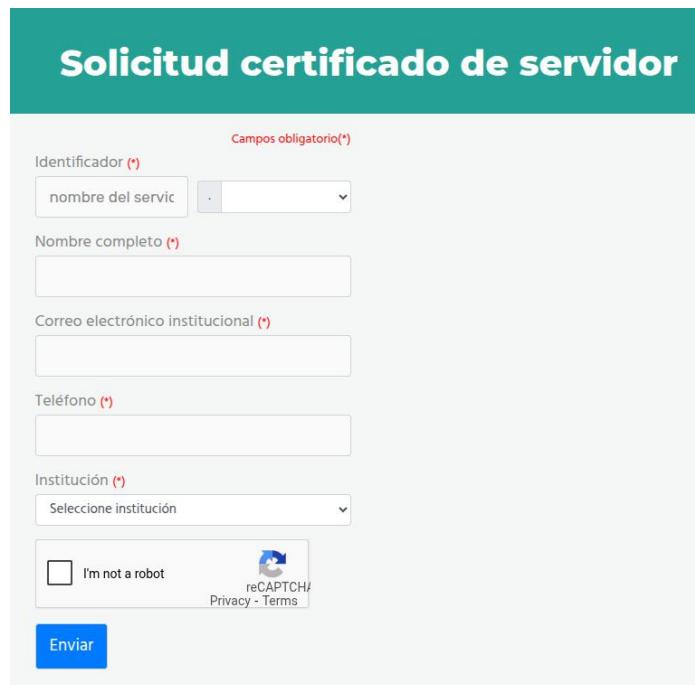
Teléfono (\*)

Institución (\*)

Seleccione institución

I'm not a robot  reCAPTCHA  
[Privacy](#) - [Terms](#)

**Enviar**



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

**emSign** | Subscriber      English | Downloads

Dear Test User,  
Please follow the instructions and complete the below verification step to speed up your certificate issuance process.

**Certificate Signing Request (CSR)**  
Adding your CSR is a simple, single step process. Please follow our instructions below and submit your CSR for verification.

CSR Mode       **1 Upload CSR**     **2 Paste CSR**

Paste CSR here

Platform Supports both RSA and ECC algorithms.

**Submit For Verification**

**Order Details**

- Date Ordered
- Order ID
- Product & Validity
- Order Status **Order Accepted**
- Certificate Status **Pending for Approver**

**Instructions**

**Generate CSR:**

- Before you can download your certificate, it is recommended that you generate a Certificate Signing Request (CSR) from your server or device. [Learn more about CSR](#)
- SSL/TLS & S/MIME Certificates:** To generate a CSR for SSL/TLS & S/MIME certificates, download the [eMudhra Certificate Utility tool](#)
- Signature Certificates:** You may use "emSign Click Certificate Downloader Tool" to generate a CSR for HSM.
- Once your CSR is generated successfully, please copy your CSR text or save your CSR file.

**Upload / Paste CSR:**

- Please choose your desired option to either upload your CSR file or paste your CSR text.
- Once your CSR is provided, we will validate the CSR and you can view the Certificate Signing Request information below.
- Platform supports following key algorithms: RSA-2048, RSA-4096, ECC-256, ECC-384 and ECC-521.

6. Para subir un archivo CSR, seleccionar la opción *Upload CSR* (Ver 1 en la imagen anterior) y seleccionar el archivo. Para pegar el contenido del CSR, seleccionar *Paste CSR* (Ver 2 en la imagen 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*

**emSign** | Suscriptor      Spanish | Descargas

Thank you for submitting your Certificate Signing Request (CSR).

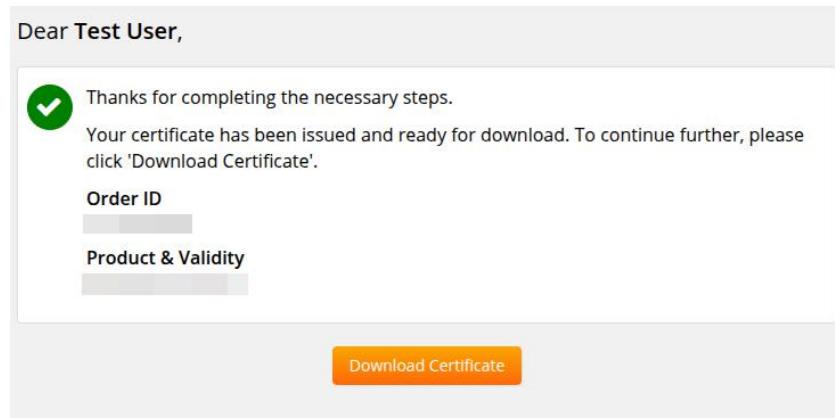
**What's Next?**  
Your certificate will be issued once your Order is approved successfully. We will send the certificate download instructions to an email address associated with your Order. Please follow our instructions and download your certificate successfully.

Order ID

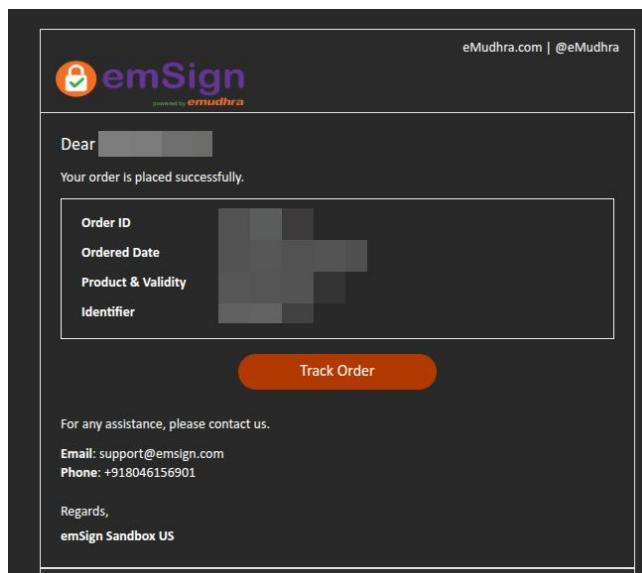
Product & Validity

**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.



Hello [REDACTED]

Please follow the instructions and complete the below verification steps to speed up your certificate issuance process.

#### Request Information

##### Certificate Requestor Information

Name [REDACTED]

Email [REDACTED]

Telephone Number [REDACTED]

Designation [REDACTED]

#### Order Actions

+ 1. Submit CSR

Completed

- 2. Certificate Download

Completed

Thank you for downloading your certificate successfully. In case, if you wish to download your certificate again, please click Download Certificate button. Your certificate is based on the CSR submitted by you. Please ensure to import / use the certificate against the same key-pair, from where the CSR was generated.

Download Certificate

## 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 -keyout <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: Ciudad, 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 -keyout <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: Ciudad, 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.)