



Esta Secretaría General da su conformidad al procedimiento para la emisión de certificados electrónicos en la Universidad de Murcia, que se recoge en Anexo, propuesto desde el Área de Tecnología de la Información y las Comunicaciones Aplicadas, con objeto de adecuarlo al nuevo procedimiento establecido por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM).

El citado procedimiento deberá ser publicado en la Sede Electrónica de esta Universidad.

## EL SECRETARIO GENERAL

Santiago Manuel Álvarez Carreño

Firmado con certificado electrónico reconocido.  
La información sobre el firmante, la fecha de  
firma y el código de verificación del documento  
se encuentra disponible en los márgenes  
izquierdo e inferior



# Procedimiento de emisión de certificados en la Universidad de Murcia

## Motivación

El presente documento pretende describir la propuesta de procedimiento de emisión de certificados electrónicos, a falta de aprobar, en su caso, por parte de responsables del equipo rectoral de la Universidad de Murcia.

Dado que se emiten certificados de diferentes prestadores y en diferentes soportes (TUI, móvil...) el documento se ha dividido en apartados específicos para cada caso.

### Emisión de certificados electrónicos de la FNMT-RCM

Desde el 1 de Marzo de 2015 la FNMT-RCM utiliza un nuevo procedimiento de emisión para sus certificados. El proceso está descrito de forma detallada en <https://www.sede.fnmt.gob.es/certificados/persona-fisica> y puede resumirse en:

1. En la Sede de la FNMT-RCM, el usuario solicita la emisión de un certificado, indicando DNI, primer apellido y correo electrónico
2. El usuario recibe un correo electrónico con un código de solicitud
3. El usuario se presenta ante una autoridad de registro para acreditar su identidad
4. Tras la acreditación y una pequeña demora para la generación del mismo, el usuario podrá descargar su certificado desde la Sede de la FNMT-RCM y en el mismo equipo y navegador en el que lo solicitó el certificado

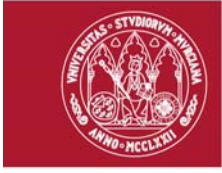
### Problemática de emisión de certificado en la TUI

Si el usuario desea generar el certificado dentro de la TUI, con el objetivo de alcanzar el grado de *firma reconocida*, tal y como recoge la Ley 59/2003, es necesario realizar una serie de pasos y comprobaciones técnicas:

- Verificar que la parte criptográfica de la tarjeta ha sido inicializada
- Comprobar que la tarjeta tiene el espacio suficiente para albergar el certificado
- Realizar el procedimiento utilizando Mozilla Firefox, puesto que es el único navegador que actualmente permite seleccionar la ubicación donde generar el certificado

Es importante destacar que los nuevos certificados tienen un tamaño de clave de 2048 bits, superior al límite de 1024 bits que tenía la **anterior tarjeta universitaria (conocida internamente como tarjeta "roja")** por lo que estas tarjetas **NO** son válidas para albergar los nuevos certificados.

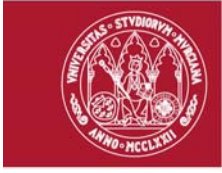
Por otro lado, es probable que en un futuro próximo los propios navegadores y sistemas dejen de permitir la utilización de certificados de 1024 bits, por lo que la **anterior tarjeta universitaria (roja)** previsiblemente dejará de ser válida para la realización de firma electrónica.



## Procedimiento técnico completo para la emisión en la TUI

De lo indicado en los párrafos anteriores, se obtiene la siguiente **lista detallada de pasos que, debiendo de ser realizados previamente a la solicitud de un certificado en la TUI, podrían resultar impracticables para los usuarios que no estén acompañados durante el proceso de un técnico de soporte:**

1. Introducir la TUI e iniciar Mozilla Firefox.
  - a. Comprobar que ha detectado la tarjeta: Firefox>Opciones>Avanzado>Certificados>Dispositivos de Seguridad:  
El módulo UMU PKCS#11 tiene debajo una entrada con nombre *GemP15-1*.
2. Abrir el Gestor de certificados en: <https://sede.um.es/sede/gestor/>.
  - a. Al iniciar el Gestor solicitará el PIN de la parte criptográfica. Si fallase, es posible que no esté inicializado. Para inicializar el PIN, será necesario actualizarlo en un TPS.
  - b. Tras solicitar el PIN, el Gestor comprueba si la parte criptográfica está correctamente inicializada (es posible que la inicialización fuese incompleta).  
En caso de fallo, habría que introducir la tarjeta en un TPS.
  - c. En el Gestor, pulsar *Verificar* para asegurar que la TUI no tiene datos corruptos, como solicitudes interrumpidas o fallos en la TUI que dejan basura en la misma impidiendo un correcto uso.
3. Acceder a <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/solicitar-certificado>.
4. Rellenar el formulario, aceptar las condiciones y enviar (Es necesario permitir **TODAS** las cookies).
  - a. En la ventana de generación de claves que se debería mostrar, elegir GemP15-1. Es posible que le pida meter el PIN o "Contraseña maestra del dispositivo GemP15". Si Firefox no muestra la ventana para elegir el dispositivo, ha sucedido un problema y tendrá que repetirse el proceso desde el inicio.
  - b. Esperar para confirmar el éxito de la operación.
5. Extraer la TUI y cerrar Mozilla Firefox.
6. Acceder al correo electrónico del usuario, esperar la recepción de un mensaje de la FNMT-RCM y anotar el código de solicitud.
7. Acreditar la identidad del suscriptor ante la RA (Debe usar Internet Explorer).
8. Tras la acreditación esperar la recepción de un correo electrónico para confirmar la generación del certificado.
9. Introducir la TUI e iniciar Mozilla Firefox.
10. Acceder a <https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/descargar-certificado>.
  - a. Comprobar que ha detectado la tarjeta: Firefox>Opciones>Avanzado>Certificados>Dispositivos de Seguridad



- El módulo UMU PKCS#11 tiene debajo una entrada con nombre *GemP15-1*.
11. Rellenar el formulario, aceptar las condiciones y enviar (Es necesario permitir **TODAS** las cookies).
    - a. En caso de éxito, pulsar el botón *Instalar Certificado*. Si no solicita el PIN o no funciona, es posible que haya sucedido un error y sea necesario repetirse el proceso desde el inicio. Es posible que si el PIN de la TUI es incorrecto, el certificado se considere (erróneamente) descargado, lo que implicaría tener que repetir el proceso desde el inicio.
  12. Si todo es correcto, tras esperar unos segundos debería indicar "Su certificado se ha instalado satisfactoriamente".
  13. Extraer la TUI y cerrar Mozilla Firefox.
  14. Insertar la TUI y abrir Internet Explorer para realizar una prueba de firma en: <https://sede.um.es/sede/soporte/test.seam>.
    - a. El icono de UMU-Shell debería haber cargado el certificado de forma correcta. Al pulsar el botón *Prueba de firma* debería indicar "Prueba de firma correcta", en caso contrario es posible que haya sucedido un error lo que implicaría tener que repetir el proceso desde el inicio.

### Emisión de certificados FNMT-RCM en la TUI para miembros de la comunidad universitaria

De acuerdo a la Declaración de prácticas de Certificación de la FNMT-RCM, la acreditación de la identidad del usuario ante la Autoridad de Registro no es exclusivamente mediante personación, como puede observarse en el siguiente párrafo extraído de aquella:

*"Cuando existan garantías suficientes para la confirmación de la identidad y demás datos personales necesarios para la gestión de certificados, las operaciones de registro podrán tener carácter telemático"*

Como entendemos que existen suficientes garantías para la confirmación de la identidad del solicitante, proponemos un procedimiento telemático, de tal forma que para esta operativa solo será necesario contar con la colaboración del operador de zona y la Autoridad de Registro del CAU de Espinardo, simplificando y centralizando el proceso con el correspondiente beneficio para todos los usuarios.

El procedimiento propuesto es:

1. El usuario realiza la solicitud de emisión de un certificado a través de <https://dumbo.um.es> a la aplicación por zonas "**Certificado en TUI**" o enviando un correo electrónico a [dumbo@um.es](mailto:dumbo@um.es) (del que CAU generará el DUMBO).
2. Un operador de zona (excepto Juniors) se desplazará al equipo del usuario para:
  - a. Solicitar al usuario su TUI y DNI para confirmar su identidad.
  - b. Hacer las comprobaciones previas de la TUI.
  - c. Realizar la solicitud de emisión del certificado.
  - d. Contactar telefónicamente y crear una **subtarea** a la Autoridad de Registro, indicando el código de solicitud.
3. La Autoridad de Registro tendrá que:
  - a. Recuperar y actualizar -si procede- la información en la base de datos de la Universidad.



- b. Utilizar dicha información en la página de registro de la FNMT-RCM.
  - c. Aprobar la emisión del certificado.
  - d. Resolver la **subtarea**.
4. El operador esperará la llegada del correo confirmación y procederá a la descarga.
  5. El operador realizará una prueba de firma y resolverá la tarea.

### **Emisión de certificados FNMT-RCM para usuarios ajenos a la Universidad**

El resto de personas y entidades deberán seguir las indicaciones de la Sede de la FNMT-RCM, <https://www.sede.fnmt.gob.es/certificados>, acudiendo a las diferentes Oficinas de Registro de la Universidad listadas en: <https://sede.um.es/sede/soporte/acreditar.seam>.

### **Procedimiento de emisión de certificados en móvil/tablet/otros**

Todos aquellos certificados que no vayan a ser alojados en la TUI se emitirán utilizando el prestador ACCV/ATCE, tal y como describe <http://www.accv.es/ciudadanos/certificados/certificados-en-soporte-software/>