Vulnerabilidad en la generación de claves RSA: comprobación y corrección de claves

Para imagePROGRAF series y PIXMA/MAXIFY series

1.ª edición

Contenido

1 Introducción

Esta guía explica cómo actualizar el firmware y registrar los certificados digitales.

Contenido:

Esta guía tiene los siguientes apartados:

- Inicio de la IU remota
- Actualización del firmware
- Actualización del certificado digital de comunicación SSL/TLS
- Registro de un certificado raíz

Las pantallas que se utilizan en esta guía pueden variar ligeramente de las que se muestran en su impresora. Para obtener más información, consulte el manual en línea de su modelo de impresora. https://ij.start.canon

2 Inicio de la IU remota

Puede utilizar la IU remota para actualizar el firmware a través de la red. Acceda a la impresora desde el navegador web de su ordenador, tableta o smartphone.

Nota

Antes de usar la IU remota, conecte la impresora a su red.

Consulte el manual en línea de su modelo de impresora para conocer los sistemas operativos y los navegadores web compatibles.

Panel

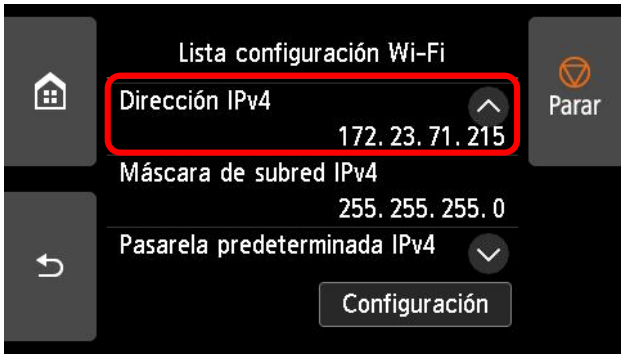
1. Compruebe la dirección IP de la impresora

(1) En la pantalla de inicio, seleccione [Configuración de LAN]

(2) Seleccione una LAN activada

Cualquier LAN desactivada aparecerá tachada.

(3) Compruebe la [Dirección IPv4] en la pantalla mostrada



Importante

El método para comprobar la dirección IP de su impresora puede diferir ligeramente de las instrucciones anteriores.

Para obtener más detalles sobre cada pantalla, consulte el manual en línea de su modelo de impresora.

https://ij.start.canon

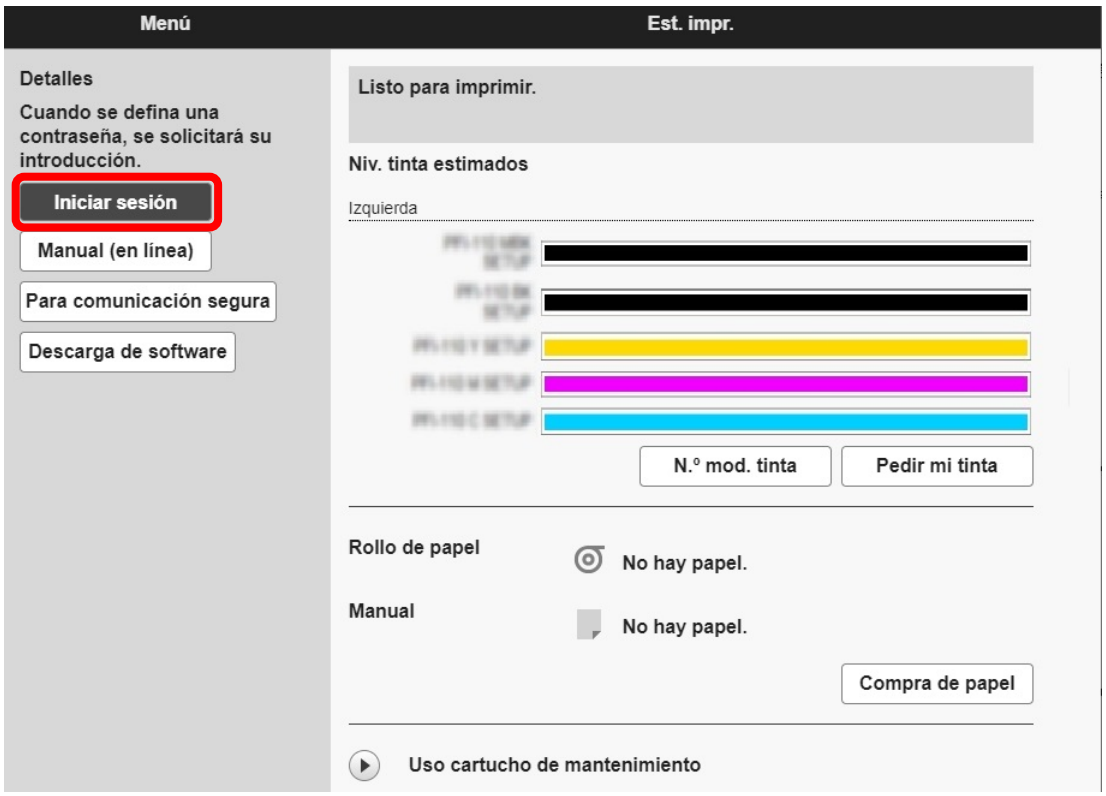
IU remota

2. Abra el navegador web e introduzca la dirección IP de la impresora en la barra de direcciones

Introduzca la dirección IP en el siguiente formato.

http://XXX.XXX.XXX.XXX

Tras obtener acceso, se iniciará la IU remota y se mostrará una pantalla de inicio de sesión en el navegador web.



3. Seleccione [Iniciar sesión]

Se mostrará una pantalla de autenticación de contraseña.

4. Introduzca la contraseña y haga clic en [OK]

Se mostrará la pantalla principal de la IU remota.

3 Actualización del firmware

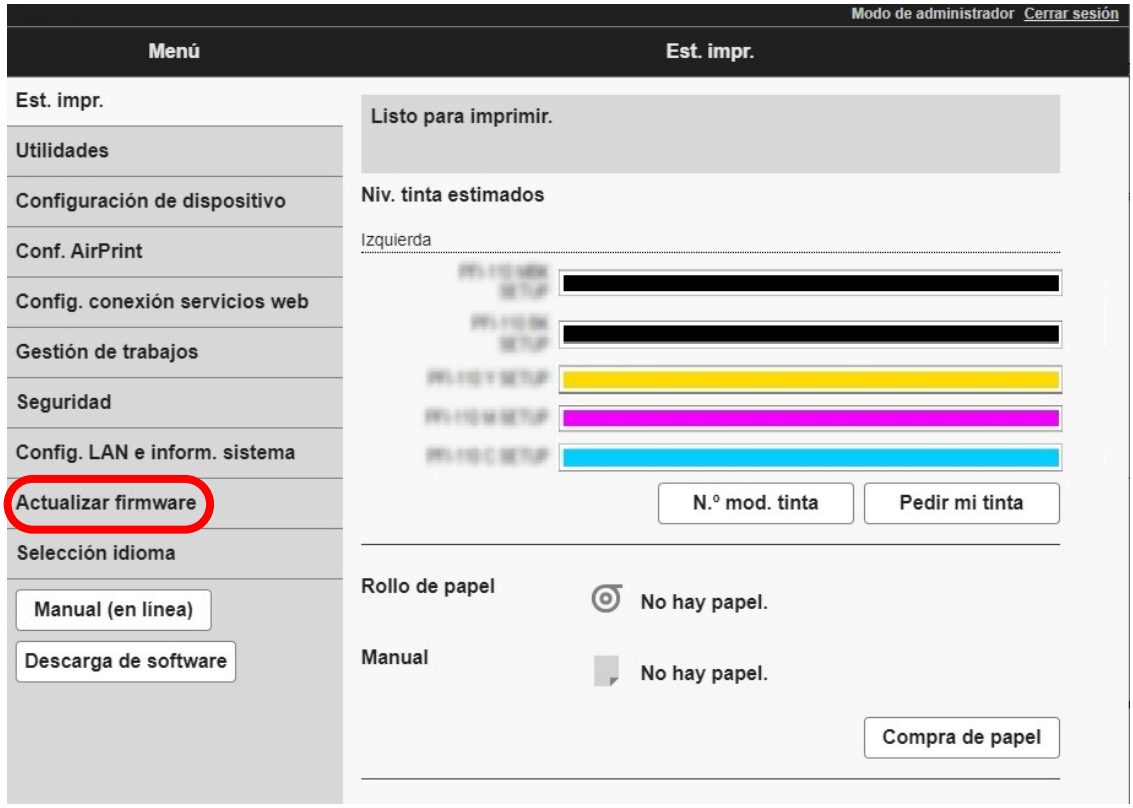
Una vez que la IU remota esté funcionando, actualice el firmware de la impresora.

Cuando haya un nuevo firmware dispon ble, este se mostrará en la IU remota. La nuevas versiones del firmware incluyen mejoras en la seguridad, por lo que es conveniente actualizarlo a la última versión.

Actualización del firmware desde la IU remota

IU remota

1. Seleccione [Actualizar firmware]



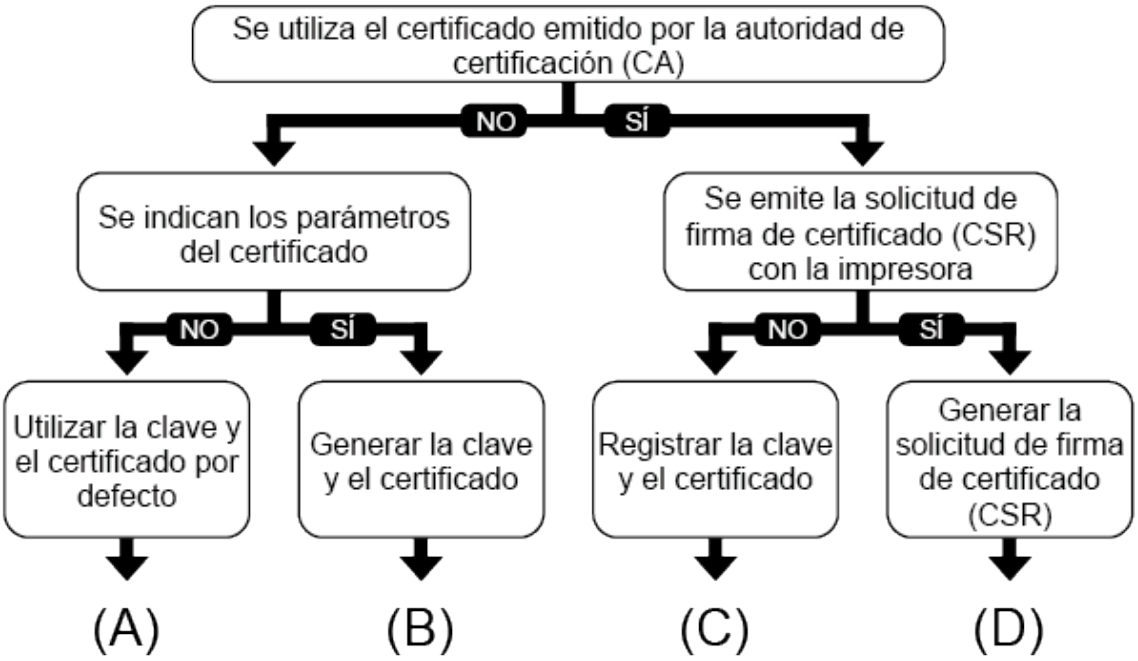
2. Seleccione [Instalar actualización]

3. Compruebe el mensaje en pantalla y seleccione [Actualización]

4 Actualización del certificado digital de comunicación SSL/TLS

Una vez completada la actualización del firmware, consulte la siguiente tabla a fin de determinar el patrón correcto para registrar su certificado digital de comunicación SSL/TLS. Actualice el certificado digital de comunicación SSL/TLS si es necesario.

Patrones de registro de certificados digitales SSL/TLS:



Determine el patrón apropiado y siga las instrucciones para ese patrón.

(A) Utilizar la clave y el certificado por defecto:

Se pueden utilizar la clave y el certificado por defecto ya instalados en la impresora. La clave y el certificado no necesitan actualizarse.

Cuando haya terminado, instale el certificado raíz en su navegador. > Registro de un certificado raíz

(B) Generar la clave y el certificado:

En primer lugar, debe eliminar la clave y el certificado actuales. Siga las instrucciones que se indican a continuación para eliminar la clave y el certificado actuales y generar otros nuevos.

1. Elimine la clave y el certificado

Acción: [Seguridad] > [Configuración SSL/TLS] > [Eliminar clave y certificado]

Elimine la clave y el certificado mostrados.

2. Genere la clave y el certificado

Acción: [Seguridad] > [Configuración SSL/TLS] > [Generar clave y certificado] > [Generar certif. autofirmado]

(1) Configure los elementos necesarios

- Algoritmo de firma: seleccione uno de entre [SHA256], [SHA384] y [SHA512].
- Longitud de bits de la clave pública: Seleccione [2048 bits].
- Validez:

  Introduzca la fecha de creación del certificado del servidor en [Válida desde].

  Introduzca la fecha de caducidad del certificado del servidor en [Válida hasta].
- Nombre común: Introduzca letras y números.

(2) Seleccione [Sig.]

- También se pueden introducir los campos [País], [Estado o provincia], [Localidad], [Organización] y [Unidad organizativa].
- Seleccione [Generar]: A continuación, se generará el certificado del servidor.
- Seleccione [Reiniciar LAN].

El certificado del servidor firmado se creará con el certificado raíz generado con la impresora.

Según el tipo y la versión del navegador web, puede aparecer una alerta que indique que no es posible establecer una comunicación segura.

Cuando haya terminado, instale el certificado raíz en su navegador. > Registro de un certificado raíz

(C) Registrar la clave y el certificado (utilizar un certificado creado externamente):

Se puede utilizar la misma clave y el mismo certificado que antes de la actualización del firmware, y no se necesitará ninguna acción después de la actualización. Tampoco será necesario instalar un certificado raíz en el navegador.

(D) Generar una solicitud de firma de certificado (CSR):

En primer lugar, debe eliminar la clave y el certificado actuales. Siga las instrucciones que se indican a continuación para eliminar la clave y el certificado actuales y generar otros nuevos.

1. Elimine la clave y el certificado

Acción: [Seguridad] > [Configuración SSL/TLS] > [Eliminar clave y certificado]

Elimine la clave y el certificado mostrados.

2. Genere la clave y el certificado

Acción: [Seguridad] > [Configuración SSL/TLS] > [Generar clave y certificado] > [Generar CSR (solicitud cert.)]

Si se muestra [Ya existe una CSR generada. Si inicia la generación, la CSR actual se eliminará. ¿Generar?], seleccione [Sí]

(1) Configure los elementos necesarios

- Algoritmo de firma: seleccione uno de entre [SHA256], [SHA384] y [SHA512].
- Longitud de bits de la clave pública: Seleccione [2048 bits].
- Nombre común

(2) Seleccione [Sig.]

- También se pueden introducir los campos [País], [Estado o provincia], [Localidad], [Organización] y [Unidad organizativa].
- Seleccione [Generar]
- Seleccione [Descargar]
- Especifique dónde guardar la CSR y guárdela

Envíe el archivo CSR guardado a una autoridad de certificación, y haga que se emita un certificado firmado por la autoridad de certificación.

3. Cargue el certificado

Acción: [Seguridad] > [Configuración SSL/TLS] > [Cargar clave y certificado]

Siga las instrucciones que se indican a continuación para cargar un certificado firmado por una autoridad de certificación.

(1) Seleccione el formato de archivo

Seleccione [PKCS#12] o [DER].

(2) Seleccione los archivos e introduzca la contraseña

(3) Seleccione el botón [Cargar]

(4) Si se solicita la contraseña del administrador, introdúzcala

(5) Seleccione el botón [Reiniciar LAN]

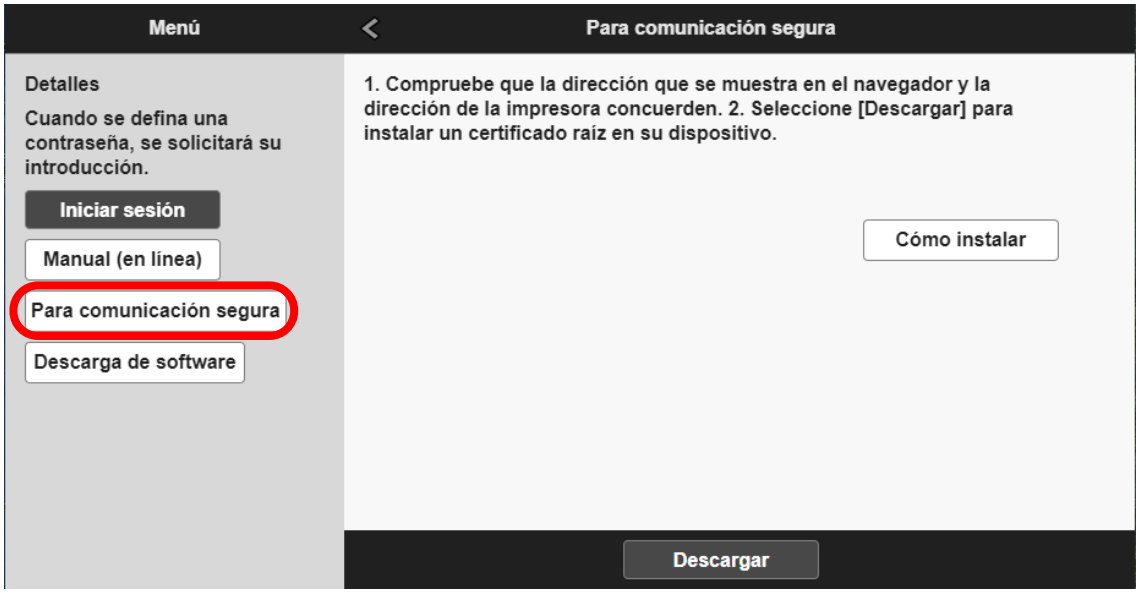
No es necesario instalar el certificado raíz en su navegador.

5 Registro de un certificado raíz

Si no se instala un certificado raíz en el navegador, puede aparecer una alerta indicando que no es posible establecer una comunicación segura. La primera vez que abra la IU remota, descargue el certificado raíz e instálelo en el navegador. Se confirmará la comunicación segura y la alerta desaparecerá. Sin embargo, en algunos navegadores seguirá apareciendo una alerta incluso después de instalar un certificado raíz.

La forma de instalar un certificado raíz depende del tipo y la versión del navegador. En esta guía se describe Microsoft Edge como ejemplo.

1. Seleccione [Para comunicación segura]



2. Seleccione [Descargar]

Se empezará a descargar el certificado raíz.

3. Después de que aparezca la pantalla de confirmación de la descarga, seleccione [Abrir]

Aparecerá la pantalla [Certificado].

4. Seleccione [Instalar certificado]

Se mostrará la pantalla [Asistente para importar certificados].

5. Seleccione [Siguiente]

6. **Seleccione [Colocar todos los certificados en el siguiente almacén]**
7. **Seleccione [Examinar]**

   Aparecerá la pantalla [Seleccionar almacén de certificados].
8. **Seleccione [Entidades de certificación raíz de confianza] y luego [Aceptar]**
9. **En la pantalla [Asistente para importar certificados], seleccione [Siguiente]**
10. **Después de que aparezca el [Finalización del Asistente para importar certificados], seleccione [Finalizar]**

    Aparecerá la pantalla [Advertencia de seguridad].
11. **Seleccione [Sí] en la pantalla [Advertencia de seguridad]**
12. **En la pantalla [Asistente para importar certificados], seleccione [Aceptar]**

    El certificado raíz ya estará instalado.

La actualización se habrá completado.