En cuanto a la medida contra la vulnerabilidad de la generación de claves RSA

USRM3-1250-00 2022-03 es

Índice

Prefacio

Prefacio

Para actualizar una clave RSA creada con una biblioteca de cifrado vulnerable, deberá actualizar el firmware y realizar los procedimientos adicionales descritos en este documento.

En primer lugar, compruebe el modelo y la versión del equipo.
Si encuentra el modelo y la versión de su equipo en esta página, actualice el firmware y, a continuación, realice los procedimientos adicionales descritos en este documento. **Comprobación de si debe realizar procedimientos adicionales(P. 5)**
Para obtener información sobre la actualización del firmware, consulte el sitio web en el que obtuvo este documento.

Comprobación de la versión del equipo

Siga el procedimiento que se indica a continuación para comprobar la versión del equipo.

1 Inicie la IU remota.

2 Haga clic en [Monitor de estado/Cancelar] en la página del portal.

3 Haga clic en [Información de dispositivo] ▶ Compruebe [Controlador] en [Información de versión].

Modelos y versiones que requieren procedimientos adicionales

Modelos	Versiones
- iR-ADV 4545 / 4535 / 4525 - iR-ADV 715 / 615 / 525 - iR-ADV 6575 / 6565 / 6560 / 6555 - iR-ADV 8505 / 8595 / 8585 - iR-ADV C3530 / C3520 - iR-ADV C7580 / C7570 / C7565 - iR-ADV C5560 / C5550 / C5540 / C5535 - iR-ADV C355 / C255 - iR-ADV C356 / C256	Ver 59.39 a ver 67.30
- iR-ADV 4545 III / 4535 III / 4525 III - iR-ADV 715 III / 615 III / 525 III - iR-ADV 6575 III / 6565 III / 6560 III - iR-ADV 8505 III / 8595 III / 8585 III / 8505B III / 8595B III / 8585B III - iR-ADV C3530 III / C3520 III - iR-ADV C7580 III / C7570 III / C7565 III - iR-ADV C5560 III / C5550 III / C5540 III / C5535 III - iR-ADV C356 III - iR-ADV C475 III - iPR C165 / C170	Ver 29.39 a ver 37.30
- iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B - iR-ADV C3730 / C3720	Ver 17.44 a ver 27.30

Modelos	Versiones
- iR-ADV C7780 / C7770 / C7765	
- iR-ADV C357 - iR-ADV C477	Ver 19.34 a ver 27.30
- iR-ADV C5760 / C5750 / C5740 / C5735	Ver 19.40 a ver 27.30
- iR-ADV 6765 / 6780	Ver 17.44 a ver 27.33
- iR-ADV C5870 / C5860 / C5850 / C5840	Ver 03.11 a ver 17.32
- iR-ADV 6860 / 6870	Ver 05.25 a ver 17.32
- iR-ADV C3830 / C3826 / C3835	Ver 06.28 a ver 17.32
- iR-ADV C568	Ver 04.13 a ver 17.08
- iR C3226 / C3222	Ver 01.12 a ver 02.13
- iR2425	Ver 02.06 a ver 05.00
- iR2635 / iR2645 / iR2630 / iR2625	Ver 130.0.117 a ver 707.0.701

NOTA

- Las capturas de pantalla utilizadas en este documento pueden diferir de las que se ven en realidad en función del modelo del equipo. Para obtener detalles sobre las capturas de pantalla, consulte el manual de su equipo en el sitio web de manuales en línea.

  https://oip.manual.canon/

Comprobación de si debe realizar procedimientos adicionales

Comprobación de si debe realizar procedimientos adicionales

Realice las tres operaciones siguientes para comprobar si debe realizar procedimientos adicionales.
Es posible que no pueda realizar operaciones desde el panel de control, en función del modelo de su equipo. Si es el caso, realice las operaciones desde la IU remota.

Comprobación de la clave RSA(P. 5)
Comprobación de las opciones de Bluetooth(P. 8)
Comprobación de la configuración del sistema de gestión de acceso(P. 8)
Si en una clave registrada en el equipo aparece "Clave predeterminada" o "AMS", la comprobación de la clave RSA no es necesaria. Compruebe la configuración de Bluetooth y la configuración del sistema de gestión de acceso, y realice los procedimientos adicionales si es necesario.

NOTA

- Las capturas de pantalla utilizadas en este documento son solo un ejemplo. Pueden diferir de las que se ven en realidad, en función del modelo del equipo.

Comprobación de la clave RSA

Compruebe si existe una clave RSA. Si hay una clave RSA generada para el equipo, compruebe el uso de esta.

Uso del panel de control(P. 5)
Al utilizar la IU remota(P. 6)

■ Uso del panel de control

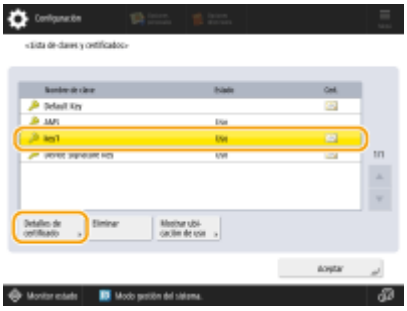
1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Lista de claves y certificados>.**

3 **Pulse <Lista claves y certificados para disposit.>.**

- <Lista claves y certificados para disposit.> no aparecerá a menos que la función de firma del usuario esté habilitada en el equipo. Si es el caso, proceda al siguiente paso.

4 **Seleccione una clave distinta de la <Default Key> y <AMS> en la que se indique <Uso> en <Estado> ▶ Pulse <Detalles de certificado>.**
Pantalla de ejemplo:



5 Compruebe <Clave pública>.

Pantalla de ejemplo:

Para un certificado que no sea RSA

No es necesario realizar procedimientos adicionales. Pulse <Aceptar> para cerrar la pantalla.

Para un certificado RSA

Continúe con el paso 6.

- No es necesario realizar procedimientos adicionales para las claves siguientes. Pulse <Aceptar> para cerrar la pantalla.
  - Se ha generado una clave RSA externamente y se ha registrado en el equipo
- Si debe realizar procedimientos adicionales, es posible que necesite información sobre el certificado para desactivarlo. Anote la información necesaria antes de eliminar la clave/certificado. Pregunte a la autoridad de certificación que ha emitido el certificado acerca de la información necesaria.

6 Pulse <Mostrar ubicación de uso> ▶ Compruebe el uso de la clave.

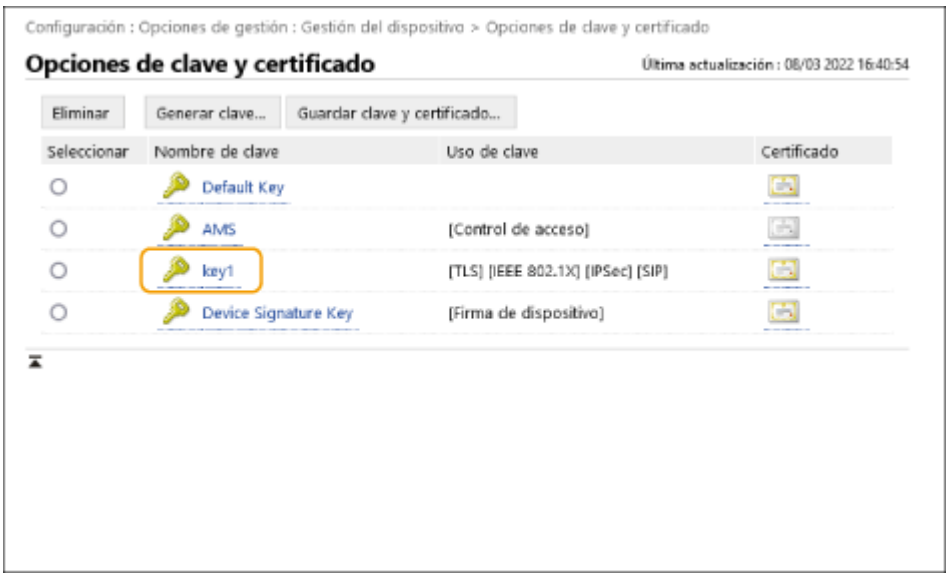
Pantalla de ejemplo:

Realice los procedimientos adicionales según lo que aparezca aquí. **Uso de la clave RSA y procedimiento adicional(P. 12)**

■Al utilizar la IU remota

1 Inicie la IU remota ▶ Haga clic en [Configuración] ▶ [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

2 Haga clic en una clave distinta de la [Default Key] y [AMS].



3 Compruebe [Clave pública].

Para un certificado que no sea RSA

No es necesario realizar procedimientos adicionales.

Para un certificado RSA

Haga clic en [Opciones de clave y certificado] en la parte superior de la pantalla ▶ Compruebe el uso de la clave.

- Realice los procedimientos adicionales según lo que aparezca aquí. **Uso de la clave RSA y procedimiento adicional(P. 12)**
- No es necesario realizar procedimientos adicionales para las siguientes claves.
  - Se ha generado una clave RSA externamente y se ha registrado en el equipo
- Si debe realizar procedimientos adicionales, es posible que necesite información sobre el certificado para desactivarlo. Anote la información necesaria antes de eliminar la clave/certificado. Pregunte a la autoridad de certificación que ha emitido el certificado acerca de la información necesaria.

Comprobación de las opciones de Bluetooth

Compruebe si el Bluetooth se ha establecido en <Sí>. Deberá realizar los procedimientos adicionales si se ha establecido en <Sí>.

Uso del panel de control(P. 8)
Al utilizar la IU remota(P. 8)

■ Uso del panel de control

1 Pulse (Configuración).

2 Pulse <Preferencias> ▶ <Red> ▶ <Opciones de Bluetooth>.

3 Compruebe <Usar Bluetooth>.

- Si <Usar Bluetooth> se ha establecido como <Sí>, realice los procedimientos siguientes. **Procedimientos adicionales para la configuración de Bluetooth(P. 89)**
- Si <Usar Bluetooth> se ha establecido como <No>, no es necesario que realice los procedimientos siguientes.

■ Al utilizar la IU remota

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Red] ▶ [Opciones de Bluetooth].

4 Compruebe [Usar Bluetooth].

- Si se ha seleccionado [Usar Bluetooth], realizar los procedimientos siguientes. **Procedimientos adicionales para la configuración de Bluetooth(P. 89)**
- Si se ha desmarcado [Usar Bluetooth], no es necesario que realice los procedimientos siguientes.

Comprobación de la configuración del sistema de gestión de acceso

Compruebe si el sistema de gestión de acceso se ha establecido en <Sí>. Deberá realizar los procedimientos adicionales si se ha establecido en <Sí>.

Puede que este ajuste no aparezca en función del equipo. En ese caso, no es necesario realizar procedimientos adicionales.

Uso del panel de control(P. 9)

Al utilizar la IU remota(P. 9)

■Uso del panel de control

1 Pulse (Configuración).

2 Pulse <Opciones de gestión> ▶ <Licencias/Otros> ▶ <Usar ACCESS MANAGEMENT SYSTEM>.

3 Compruebe <Usar ACCESS MANAGEMENT SYSTEM>.

- Si <Usar ACCESS MANAGEMENT SYSTEM> se ha establecido como <Sí>, realice los procedimientos siguientes.
Procedimientos adicionales para la configuración del sistema de gestión de acceso(P. 94)
- Si <Usar ACCESS MANAGEMENT SYSTEM> se ha establecido como <No>, no es necesario que realice los procedimientos siguientes.

■Al utilizar la IU remota

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Licencias/Otros] ▶ [Opciones de ACCESS MANAGEMENT SYSTEM].

4 Compruebe [Usar ACCESS MANAGEMENT SYSTEM].

- Si se ha seleccionado [Usar ACCESS MANAGEMENT SYSTEM], realizar los procedimientos siguientes.
Procedimientos adicionales para la configuración del sistema de gestión de acceso(P. 94)
- Si se ha desmarcado [Usar ACCESS MANAGEMENT SYSTEM], no es necesario que realice los procedimientos siguientes.

Uso de la clave RSA y procedimiento adicional

Uso de la clave RSA y procedimiento adicional

Consulte "Procedimientos adicionales" y realícelos según el uso de la clave.

Uso de la clave RSA	Condiciones	Procedimientos adicionales
TLS	Deberá realizar los procedimientos adicionales en todos los casos.	**Procedimiento para TLS(P. 13)**
IEEE 802.1X	Deberá realizar los procedimientos adicionales si el método de autenticación IEEE 802.1X está establecido como EAP-TLS.	**Procedimiento para IEEE 802.1X(P. 28)**
IPSec	Deberá realizar los procedimientos adicionales si el método de autenticación IKE está establecido como método de firma digital.	**Procedimiento para IPSec(P. 46)**
SIP	Deberá realizar los procedimientos adicionales si se utiliza TLS.	**Procedimiento para SIP(P. 64)**
Firma de dispositivo	Debe realizar los procedimientos adicionales en los casos siguientes: • Cuando se ha añadido una firma digital a los archivos enviados utilizando una clave para firmas de dispositivos • Cuando el cifrado está habilitado en la configuración de cifrado de S/MIME	**Procedimiento para las firmas de dispositivo(P. 81)**

NOTA

- Las capturas de pantalla utilizadas en este documento son solo un ejemplo. Pueden diferir de las que se ven en realidad, en función del modelo del equipo.

Procedimiento para TLS

Paso 1: Regeneración de la clave y el certificado (para TLS)

Puede generar tres tipos de certificados para una clave generada con el equipo: un certificado autofirmado, un certificado CSR y un certificado SCEP. El procedimiento difiere según el tipo de certificado.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Para un certificado autofirmado(P. 14)
Para un certificado CSR(P. 17)
Para un certificado SCEP(P. 19)

Para un certificado autofirmado

Uso del panel de control(P. 14)
Al utilizar la IU remota(P. 15)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Generar clave> ▶ <Generar clave de comunicaciones por red>.**

3 **Configure los ajustes necesarios y pase a la pantalla siguiente.**

Pantalla de ejemplo:

a <Nombre de clave>

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b <Algoritmo de firma>

Seleccione el algoritmo hash a utilizar para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512. Si se selecciona <RSA> para c, y se establece <Longitud de clave (bits)> para <1024> o más para d, se pueden seleccionar los algoritmos hash SHA384 y SHA512.

c <Algoritmo de clave>

Seleccione el algoritmo de clave. Si se selecciona <RSA>, aparecerá <Longitud de clave (bits)> como elemento de configuración para d. Si se selecciona <ECDSA>, aparecerá en su lugar <Tipo de clave>.

d <Longitud de clave (bits)>/<Tipo de clave>

Especifique la longitud de la clave si se selecciona <RSA> para c, o especifique el tipo de clave si se selecciona <ECDSA>. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

4 Configure los elementos necesarios para el certificado ▶ Pulse <Generar clave>.

Pantalla de ejemplo:

a <Válido desde>/<Fecha de caducidad>

Introduzca la fecha de inicio y los datos de finalización del periodo de validez del certificado.

b <País/región>/<Estado>/<Ciudad>/<Organización>/<Unidad organiz.>

Seleccione el código de país de la lista e introduzca la ubicación y el nombre de la organización.

c <Nombre común>

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

■Al utilizar la IU remota

1 Inicie la IU remota.

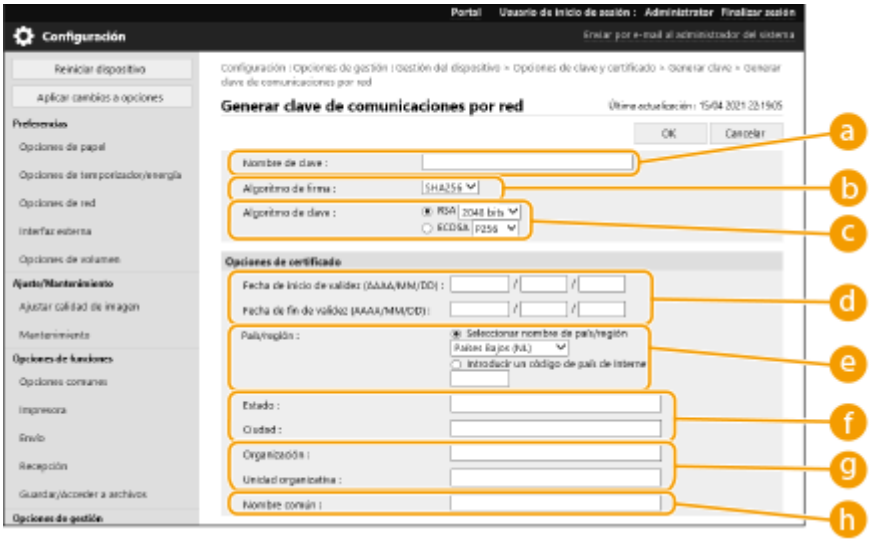
2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 Haga clic en [Generar clave].

5 Haga clic en [Comunicación de red].

6 Configure la clave y los ajustes del certificado.



a [Nombre de clave]

Introduzca un nombre de clave utilizando caracteres alfanuméricos. Utilice un nombre que sea fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash que se utilizará para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512.

c [Algoritmo de clave]

Seleccione [RSA] o [ECDSA] como el algoritmo de generación de clave. Especifique la longitud de la clave si se selecciona [RSA] o indique el tipo de clave si se selecciona [ECDSA]. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

NOTA:

- Si se selecciona [SHA384] o [SHA512] para [Algoritmo de firma], no se podrá establecer la longitud de la clave en [512 bits] al seleccionar [RSA] para [Algoritmo de clave].

d [Fecha de inicio de validez (AAAA/MM/DD)]/[Fecha de fin de validez (AAAA/MM/DD)]

Introduzca la fecha de inicio y los datos de finalización del período de validez del certificado. La [Fecha de fin de validez (AAAA/MM/DD)] no puede ajustarse a una fecha anterior a la fecha en [Fecha de inicio de validez (AAAA/MM/DD)].

e [País/región]

Haga clic en [Seleccionar nombre de país/región] y seleccione el país/región en la lista desplegable. También puede hacer clic en [Introducir un código de país de Internet] e introducir el código el país, como por ejemplo "US" para Estados Unidos.

f [Estado]/[Ciudad]

Introduzca la ubicación utilizando los caracteres alfanuméricos que sean necesarios.

g [Organización]/[Unidad organizativa]

Introduzca el nombre de la organización utilizando los caracteres alfanuméricos que sean necesarios.

h [Nombre común]

Introduzca el nombre común del certificado utilizando los caracteres alfanuméricos que sean necesarios. "Nombre común" suele abreviarse como "CN".

7 Haga clic en [Bien].

- Generar una clave y un certificado puede llevar cierto tiempo.
- Las claves y certificados generados se registran automáticamente en el equipo.

Para un certificado CSR

Genere una clave y una CSR en el equipo. Utilice los datos de CSR que aparecen en la pantalla o que se envían a un archivo para solicitar a la autoridad de certificación que emita un certificado. A continuación, registre el certificado emitido para la clave.
Este ajuste solo se puede configurar desde la IU remota.

■1. Generación de una clave y una CSR

1 **Inicie la IU remota.**

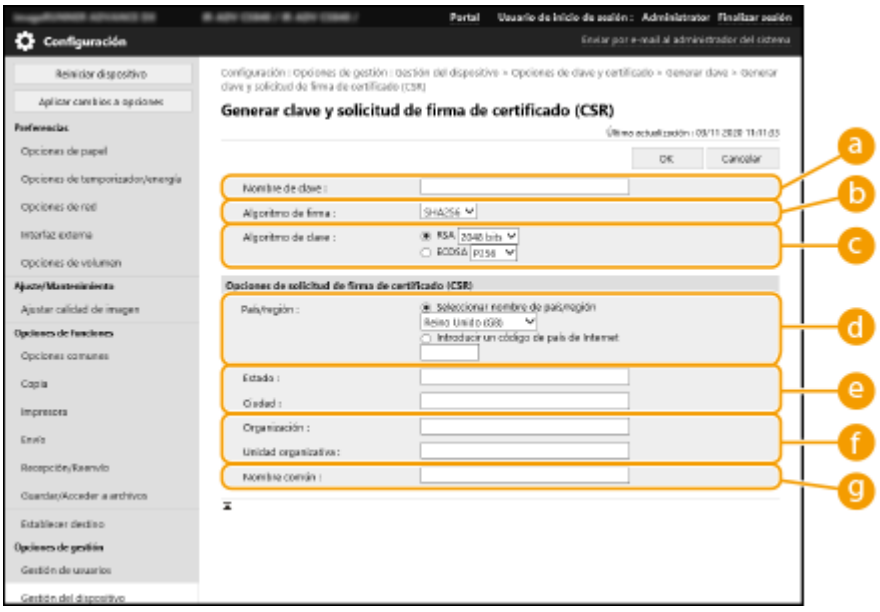
2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Haga clic en [Generar clave].**

5 **Haga clic en [Clave y solicitud de firma de certificado (CSR)].**

6 **Configure la clave y los ajustes del certificado.**



a [Nombre de clave]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash para utilizar para la firma.

c [Algoritmo de clave]

Seleccione el algoritmo de clave y especifique la longitud de la clave si se selecciona [RSA], o bien especifique el tipo de clave si se selecciona [ECDSA].

[País/región]

Seleccione el código de país de la lista o introdúzcalo directamente.

[Estado]/[Ciudad]

Introduzca la ubicación.

[Organización]/[Unidad organizativa]

Escriba el nombre de la organización.

[Nombre común]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

7 Haga clic en [Bien].

➡ Aparecen los datos de CSR.

- Si desea guardar los datos de CSR en un archivo, haga clic en [Guardar en archivo] y especifique la ubicación de almacenamiento.

NOTA:

- La clave que ha generado la CSR aparece en la pantalla de lista de claves y certificados, pero no puede usarla por sí sola. Para utilizar esta clave, tiene que registrar el certificado que se emite luego a partir de la CSR.

8 Solicite a la autoridad de certificación que emita un certificado en base a los datos de la CSR.

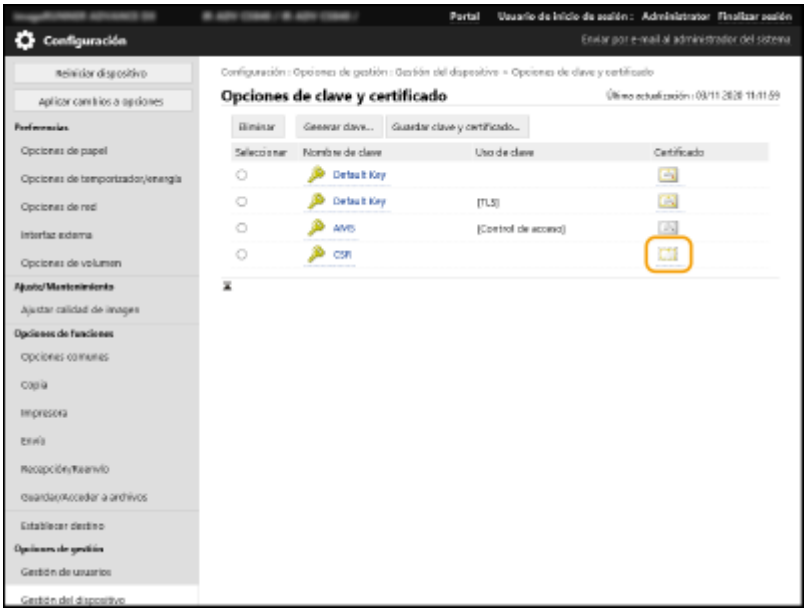
■2. Registro del certificado emitido en la clave

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 En la lista [Certificado], haga clic en para el certificado que desee registrar.



5 **Haga clic en [Guardar certificado...].**

6 **Registre el certificado.**

- Haga clic en [Examinar...] ▶ Especifique el archivo (certificado) para registrar ▶ Haga clic en [Guardar].

Para un certificado SCEP

Solicite manualmente al servidor SCEP que emita un certificado.
Solo puede configurar este ajuste desde la IU remota.

NOTA

- No podrá enviar una solicitud manual de emisión de un certificado si se selecciona [Habilitar el temporizador para la solicitud automática de emisión de certificado]. Desmarque esta opción si está seleccionada.

Inicie la IU remota ▶ Haga clic en [Configuración] ▶ [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)] ▶ [Opciones para la solicitud automática de emisión de certificado] ▶ Desmarque [Habilitar el temporizador para la solicitud automática de emisión de certificado] ▶ Haga clic en [Actualizar].

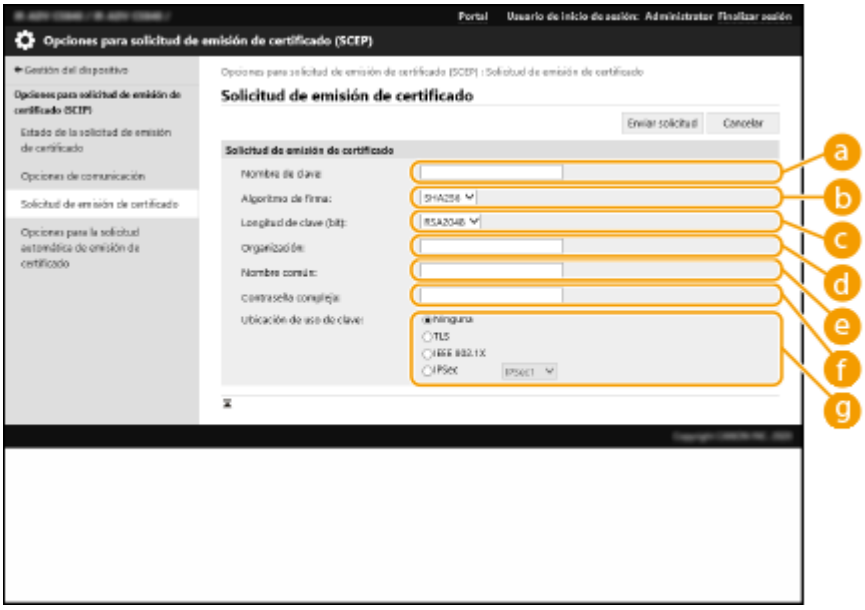
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)].**

4 **Haga clic en [Solicitud de emisión de certificado].**

5 Configure los ajustes necesarios para solicitar un certificado.



a [Nombre de clave:]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b [Algoritmo de firma:]

Seleccione el algoritmo hash para utilizar para la firma.

c [Longitud de clave (bit):]

Seleccione la longitud de la clave.

d [Organización:]

Escriba el nombre de la organización.

e [Nombre común:]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

f [Contraseña compleja:]

Cuando se configure una contraseña en la parte del servidor SCEP, introduzca la contraseña de comprobación incluida en los datos de solicitud (PKCS#9) para solicitar un certificado para emitirse.

g [Ubicación de uso de clave:]

Seleccione [TLS].

NOTA:

- Al seleccionar una opción que no sea [Ninguna], active cada función con antelación. Si se obtiene correctamente un certificado con todas las funciones desactivadas, el certificado se asigna a la ubicación de uso de la clave, pero las funciones no se activan de forma automática.

6 Haga clic en [Enviar solicitud].

7 **Haga clic en [Reiniciar].**

Paso 2: Restablecimiento de la clave y el certificado (para TLS)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.
Este procedimiento no es necesario para un certificado SCEP.

Para un certificado autofirmado/CSR

Uso del panel de control(P. 22)
Al utilizar la IU remota(P. 23)

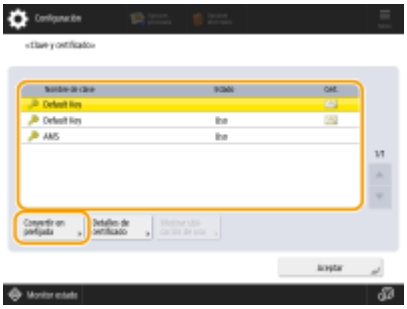
■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de TLS>.**

3 **Pulse <Clave y certificado>.**

4 **Seleccione la clave y el certificado para a con comunicación cifrada TLS ▶ Pulse <Convertir en prefijada> ▶ <Sí>.**
Pantalla de ejemplo:



- Si desea utilizar una clave y un certificado preinstalados, seleccione <Default Key>.

NOTA:

- La comunicación cifrada TLS no puede utilizar <Device Signature Key>, que se utiliza para las firmas de dispositivo, o <AMS>, que se utiliza para las restricciones de acceso.

5 **Pulse <Aceptar>.**

6 **Pulse (Configuración) ▶ <Aplicar cambios a opciones> ▶ <Sí>.**

➠ El equipo se reinicia y las opciones se aplican.

■Al utilizar la IU remota

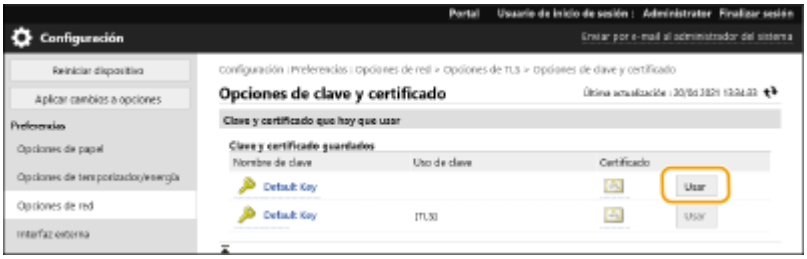
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Red] ▶ [Opciones de TLS].**

4 **Haga clic en [Clave y certificado].**

5 **Haga clic en [Usar] para la clave y el certificado para utilizar con comunicación cifrada TLS.**



- Si desea utilizar una clave y un certificado preinstalados, seleccione [Default Key].

6 **Haga clic en [Aplicar camb. a opc.] para reiniciar el equipo.**

➠ El equipo se reinicia y las opciones se aplican.

Paso 3: Eliminación de una clave/certificado generado en el pasado (para TLS)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

NOTA

- Es posible que tenga que transmitir información a la autoridad de certificación cuando desactive el certificado. Consulte **Comprobación de si debe realizar procedimientos adicionales(P. 5)** , y anote la información necesaria antes de borrar la clave/certificado.

Uso del panel de control(P. 24)
Al utilizar la IU remota(P. 25)

■ Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Lista de claves y certificados> ▶ <Lista claves y certificados para disposit.>.**

- <Lista claves y certificados para disposit.> no aparecerá a menos que la función de firma del usuario esté habilitada en el equipo. Si es el caso, proceda al siguiente paso.

3 **Seleccione la clave y el certificado ▶ Pulse <Eliminar> ▶ <Sí>.**

Pantalla de ejemplo:

NOTA:

- Si aparece , la clave está corrupta o no es válida.
- Si no aparece , el certificado de la clave no existe.
- Si selecciona una clave y certificado y pulsa <Detalles de certificado>, aparecerá información detallada sobre el certificado. También puede pulsar <Verif. certif.> en esta pantalla para comprobar si el certificado es válido.

■Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Seleccione la clave y el certificado ▶ Haga clic en [Eliminar] ▶ [Aceptar].**

NOTA

- Si aparece , la clave está corrupta o no es válida.
- Si aparece , el certificado de la clave no existe.
- Haga clic en un nombre de clave para ver la información detallada del certificado. También puede hacer clic en [Verificar certificado] en esta pantalla para comprobar si el certificado es válido.

Paso 4: Desactivación del certificado (para TLS)

Desactive los certificados generados en el pasado. El procedimiento difiere según el tipo de certificado.

■ Para un certificado autofirmado

Si tiene algún certificado con clave que requiera procedimientos adicionales registrado en algún ordenador o navegador web como certificado de confianza, elimínelo.

■ Para un certificado CSR/SCEP

Solicite a la autoridad de certificación que ha emitido el certificado que lo revoque. Consulte el [Emisor] en el certificado para que la autoridad de certificación lo solicite.

NOTA

- Si está comprobando la revocación de un certificado mediante una CRL en un ordenador o navegador web que se comunique con el equipo, registre la CRL actualizada en el ordenador o navegador web después de que el certificado sea revocado.
- Si utiliza un método distinto a la CRL (por ejemplo, OCSP) para comprobar la revocación de certificados, realice el procedimiento correspondiente a ese método.

Paso 5: Activación del nuevo certificado (para TLS)

Active el certificado que se acaba de generar en el equipo.

■ Para un certificado autofirmado

Registre el nuevo certificado como certificado de confianza en el ordenador o en el navegador web.

■ Para un certificado CSR/SCEP

No es necesario realizar procedimientos adicionales.

Procedimiento para IEEE 802.1X

Paso 1: Comprobación del método de autenticación (para IEEE 802.1X)

Debe realizar los procedimientos siguientes si el método de autenticación IEEE 802.1X está establecido como EAP-TLS. Siga el procedimiento siguiente para comprobar el método de autenticación.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Uso del panel de control(P. 29)
Al utilizar la IU remota(P. 29)

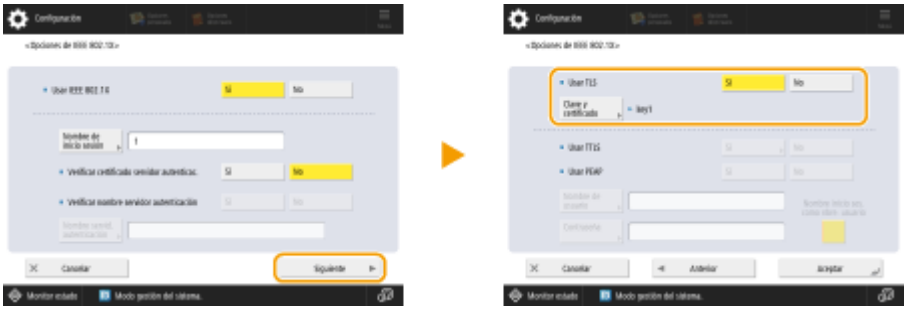
Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de IEEE 802.1X>.**

3 **Pulse <Siguiente> ▶ Compruebe <Usar TLS>.**

Pantalla de ejemplo:



- Si <Usar TLS> está establecido como <Sí> y aparece un nombre clave para <Clave y certificado>, realice los procedimientos siguientes.
- Si <Usar TLS> se ha establecido como <No>, no es necesario que realice los procedimientos siguientes.

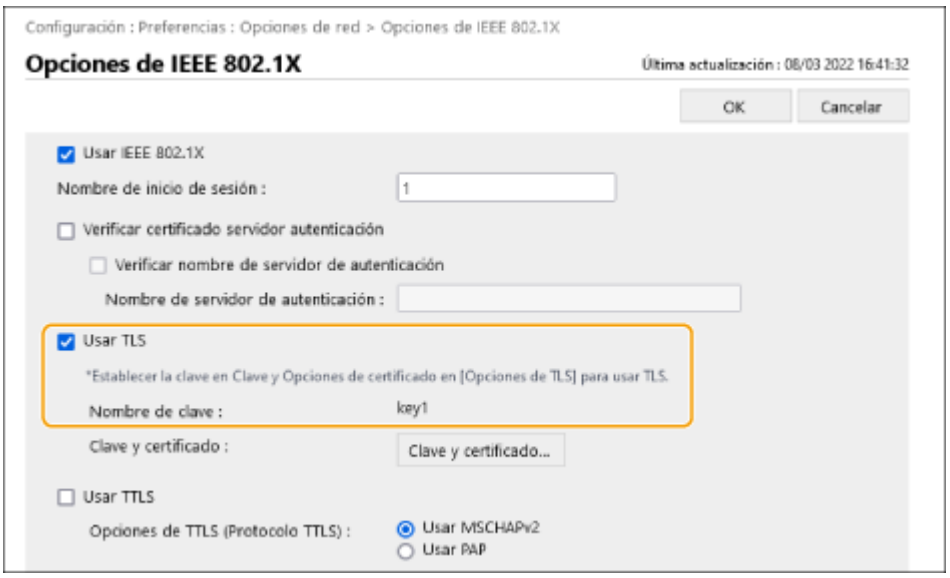
Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Red] ▶ [Opciones de IEEE 802.1X].**

4 Compruebe [Usar TLS].



- Si se ha seleccionado [Usar TLS] y aparece un nombre clave, realice los procedimientos siguientes.
- Si se ha desmarcado [Usar TLS], no es necesario que realice los procedimientos siguientes.

Paso 2: Regeneración de la clave y el certificado (para IEEE 802.1X)

Puede generar tres tipos de certificados para una clave generada con el equipo: un certificado autofirmado, un certificado CSR y un certificado SCEP. El procedimiento difiere según el tipo de certificado.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Para un certificado autofirmado(P. 31)
Para un certificado CSR(P. 34)
Para un certificado SCEP(P. 36)

Para un certificado autofirmado

Uso del panel de control(P. 31)
Al utilizar la IU remota(P. 32)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Generar clave> ▶ <Generar clave de comunicaciones por red>.**

3 **Configure los ajustes necesarios y pase a la pantalla siguiente.**

Pantalla de ejemplo:

a <Nombre de clave>

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b <Algoritmo de firma>

Seleccione el algoritmo hash a utilizar para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512. Si se selecciona <RSA> para c, y se establece <Longitud de clave (bits)> para <1024> o más para d, se pueden seleccionar los algoritmos hash SHA384 y SHA512.

c <Algoritmo de clave>

Seleccione el algoritmo de clave. Si se selecciona <RSA>, aparecerá <Longitud de clave (bits)> como elemento de configuración para d. Si se selecciona <ECDSA>, aparecerá en su lugar <Tipo de clave>.

d <Longitud de clave (bits)>/<Tipo de clave>

Especifique la longitud de la clave si se selecciona <RSA> para c, o especifique el tipo de clave si se selecciona <ECDSA>. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

4 Configure los elementos necesarios para el certificado ▶ Pulse <Generar clave>.

Pantalla de ejemplo:

a <Válido desde>/<Fecha de caducidad>

Introduzca la fecha de inicio y los datos de finalización del periodo de validez del certificado.

b <País/región>/<Estado>/<Ciudad>/<Organización>/<Unidad organiz.>

Seleccione el código de país de la lista e introduzca la ubicación y el nombre de la organización.

c <Nombre común>

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

■Al utilizar la IU remota

1 Inicie la IU remota.

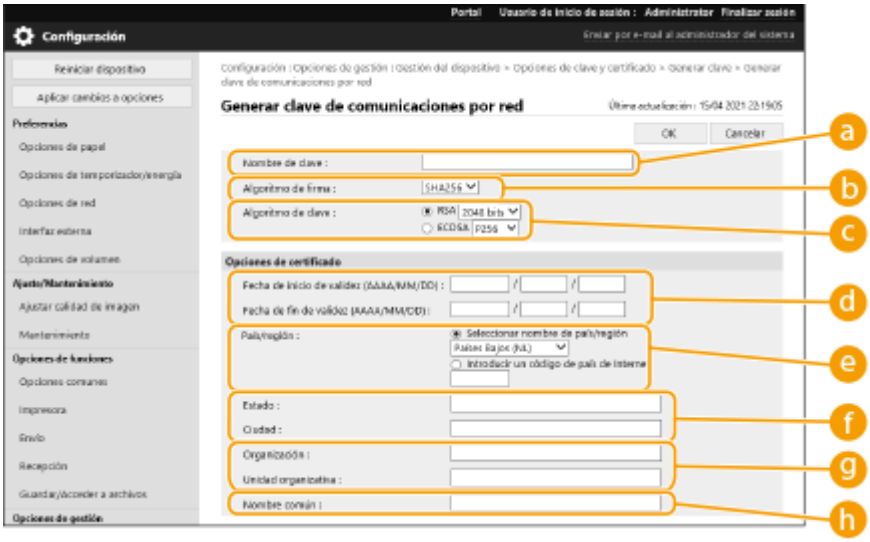
2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 Haga clic en [Generar clave].

5 Haga clic en [Comunicación de red].

6 Configure la clave y los ajustes del certificado.



a [Nombre de clave]

Introduzca un nombre de clave utilizando caracteres alfanuméricos. Utilice un nombre que sea fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash que se utilizará para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512.

c [Algoritmo de clave]

Seleccione [RSA] o [ECDSA] como el algoritmo de generación de clave. Especifique la longitud de la clave si se selecciona [RSA] o indique el tipo de clave si se selecciona [ECDSA]. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

NOTA:

- Si se selecciona [SHA384] o [SHA512] para [Algoritmo de firma], no se podrá establecer la longitud de la clave en [512 bits] al seleccionar [RSA] para [Algoritmo de clave].

d [Fecha de inicio de validez (AAAA/MM/DD)]/[Fecha de fin de validez (AAAA/MM/DD)]

Introduzca la fecha de inicio y los datos de finalización del período de validez del certificado. La [Fecha de fin de validez (AAAA/MM/DD)] no puede ajustarse a una fecha anterior a la fecha en [Fecha de inicio de validez (AAAA/MM/DD)].

e [País/región]

Haga clic en [Seleccionar nombre de país/región] y seleccione el país/región en la lista desplegable. También puede hacer clic en [Introducir un código de país de Internet] e introducir el código el país, como por ejemplo "US" para Estados Unidos.

f [Estado]/[Ciudad]

Introduzca la ubicación utilizando los caracteres alfanuméricos que sean necesarios.

g [Organización]/[Unidad organizativa]

Introduzca el nombre de la organización utilizando los caracteres alfanuméricos que sean necesarios.

h [Nombre común]

Introduzca el nombre común del certificado utilizando los caracteres alfanuméricos que sean necesarios. "Nombre común" suele abreviarse como "CN".

7 Haga clic en [Bien].

- Generar una clave y un certificado puede llevar cierto tiempo.
- Las claves y certificados generados se registran automáticamente en el equipo.

Para un certificado CSR

Genere una clave y una CSR en el equipo. Utilice los datos de CSR que aparecen en la pantalla o que se envían a un archivo para solicitar a la autoridad de certificación que emita un certificado. A continuación, registre el certificado emitido para la clave.
Este ajuste solo se puede configurar desde la IU remota.

■1. Generación de una clave y una CSR

1 **Inicie la IU remota.**

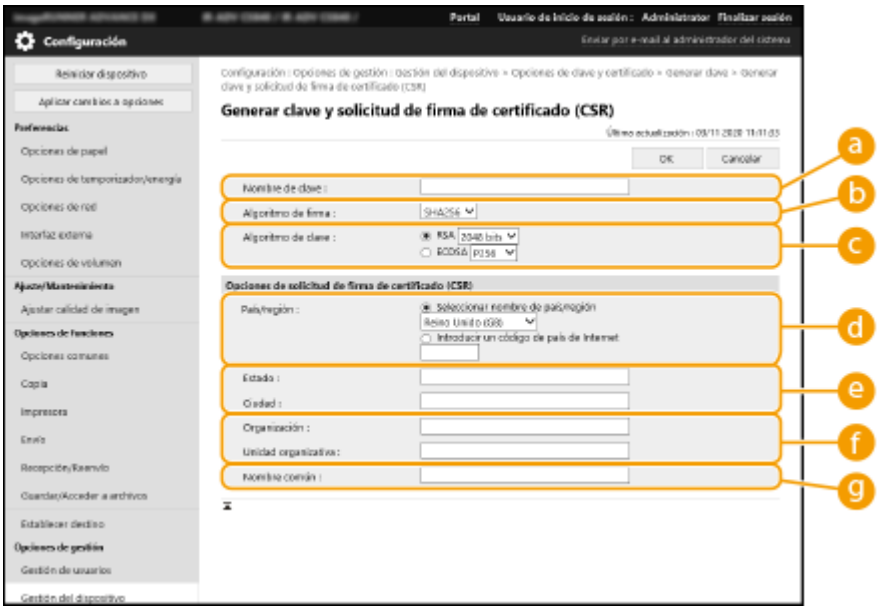
2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Haga clic en [Generar clave].**

5 **Haga clic en [Clave y solicitud de firma de certificado (CSR)].**

6 **Configure la clave y los ajustes del certificado.**



ⓐ [Nombre de clave]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

ⓑ [Algoritmo de firma]

Seleccione el algoritmo hash para utilizar para la firma.

ⓒ [Algoritmo de clave]

Seleccione el algoritmo de clave y especifique la longitud de la clave si se selecciona [RSA], o bien especifique el tipo de clave si se selecciona [ECDSA].

[País/región]

Seleccione el código de país de la lista o introdúzcalo directamente.

[Estado]/[Ciudad]

Introduzca la ubicación.

[Organización]/[Unidad organizativa]

Escriba el nombre de la organización.

[Nombre común]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

7 Haga clic en [Bien].

➡ Aparecen los datos de CSR.

- Si desea guardar los datos de CSR en un archivo, haga clic en [Guardar en archivo] y especifique la ubicación de almacenamiento.

NOTA:

- La clave que ha generado la CSR aparece en la pantalla de lista de claves y certificados, pero no puede usarla por sí sola. Para utilizar esta clave, tiene que registrar el certificado que se emite luego a partir de la CSR.

8 Solicite a la autoridad de certificación que emita un certificado en base a los datos de la CSR.

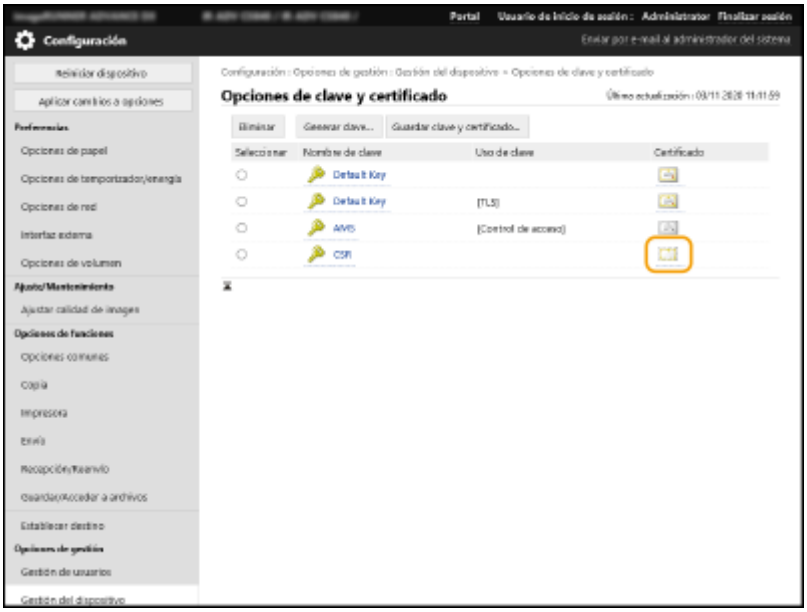
■2. Registro del certificado emitido en la clave

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 En la lista [Certificado], haga clic en para el certificado que desee registrar.



5 **Haga clic en [Guardar certificado...].**

6 **Registre el certificado.**

- Haga clic en [Examinar...] ▶ Especifique el archivo (certificado) para registrar ▶ Haga clic en [Guardar].

Para un certificado SCEP

Solicite manualmente al servidor SCEP que emita un certificado.
Solo puede configurar este ajuste desde la IU remota.

NOTA

- No podrá enviar una solicitud manual de emisión de un certificado si se selecciona [Habilitar el temporizador para la solicitud automática de emisión de certificado]. Desmarque esta opción si está seleccionada.

Inicie la IU remota ▶ Haga clic en [Configuración] ▶ [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)] ▶ [Opciones para la solicitud automática de emisión de certificado] ▶ Desmarque [Habilitar el temporizador para la solicitud automática de emisión de certificado] ▶ Haga clic en [Actualizar].

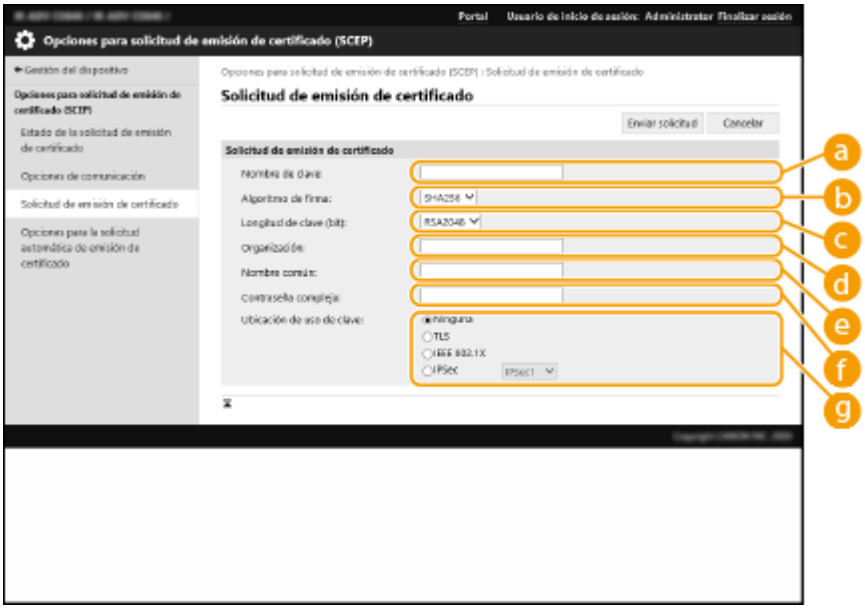
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)].**

4 **Haga clic en [Solicitud de emisión de certificado].**

5 Configure los ajustes necesarios para solicitar un certificado.



a [Nombre de clave:]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b [Algoritmo de firma:]

Seleccione el algoritmo hash para utilizar para la firma.

c [Longitud de clave (bit):]

Seleccione la longitud de la clave.

d [Organización:]

Escriba el nombre de la organización.

e [Nombre común:]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

f [Contraseña compleja:]

Cuando se configure una contraseña en la parte del servidor SCEP, introduzca la contraseña de comprobación incluida en los datos de solicitud (PKCS#9) para solicitar un certificado para emitirse.

g [Ubicación de uso de clave:]

Seleccione [IEEE 802.1X].

NOTA:

- Al seleccionar una opción que no sea [Ninguna], active cada función con antelación. Si se obtiene correctamente un certificado con todas las funciones desactivadas, el certificado se asigna a la ubicación de uso de la clave, pero las funciones no se activan de forma automática.

6 Haga clic en [Enviar solicitud].

7 **Haga clic en [Reiniciar].**

Paso 3: Restablecimiento de la clave y el certificado (para IEEE 802.1X)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.
Este procedimiento no es necesario para un certificado SCEP.

Para un certificado autofirmado/CSR

Uso del panel de control(P. 39)
Al utilizar la IU remota(P. 40)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de IEEE 802.1X>.**

3 **Pulse <Sí> para <Usar IEEE 802.1X> ▶ Configure las opciones necesarias ▶ Pulse <Siguiente>.**
Pantalla de ejemplo:

a <Nombre de inicio sesión>

Introduzca el nombre (Identidad EAP) del usuario de inicio de sesión para recibir la autenticación IEEE 802.1X.

b <Verificar certificado servidor autenticac.>

Defina el ajuste en <Sí> cuando verifique los certificados del servidor enviados desde un servidor de autenticación.

c <Verificar nombre servidor autenticación>

Para verificar un nombre común en el certificado del servidor, seleccione <Sí>. A continuación, introduzca el nombre del servidor de autenticación en el que el usuario de inicio de sesión se encuentra registrado en<Nombre servid. autenticación>.

4 **Pulse <Sí> para <Usar TLS> ▶ Pulse <Clave y certificado>.**

5 **Seleccione la clave y el certificado a utilizar en la lista ▶ Pulse <Convertir en prefijada> ▶ <Sí>.**

6 **Pulse <Aceptar>.**

7 **Pulse (Configuración) ▶ (Configuración) ▶ <Aplicar camb. a opc.> ▶ <Sí>.**

➠ El equipo se reinicia y las opciones se aplican.

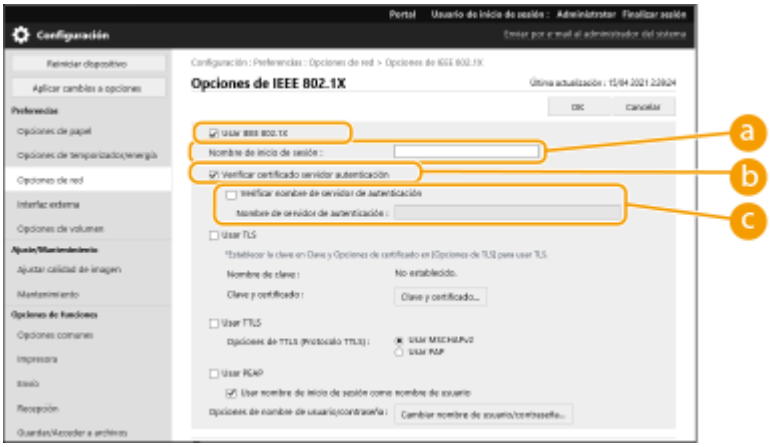
■ Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Opciones de red] ▶ [Opciones de IEEE 802.1X].**

4 **Seleccione [Usar IEEE 802.1X] ▶ Configure las opciones necesarias.**



a [Nombre de inicio de sesión]

Introduzca el nombre (Identidad EAP) del usuario de inicio de sesión para recibir la autenticación IEEE 802.1X.

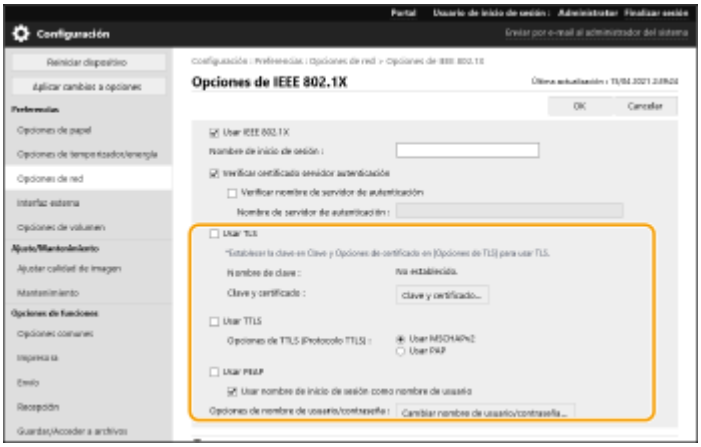
b [Verificar certificado servidor autenticación]

Seleccione esta casilla de verificación cuando verifique los certificados del servidor enviados desde un servidor de autenticación.

c [Verificar nombre de servidor de autenticación]

Para verificar el nombre común en el certificado del servidor, seleccione esta casilla de verificación. A continuación, introduzca el nombre del servidor de autenticación en el que el usuario de inicio de sesión se encuentra registrado en [Nombre de servidor de autenticación].

5 Seleccione [Usar TLS] ▶ Haga clic en [Clave y certificado].



6 Haga clic en [Usar] para utilizar la clave en la lista.

7 Haga clic en [Bien].

8 Haga clic en [Aplicar cambios a opciones] para reiniciar el equipo.

➠ El equipo se reinicia y las opciones se aplican.

Paso 4: Eliminación de una clave/certificado generado en el pasado (para IEEE 802.1X)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

NOTA

- Es posible que tenga que transmitir información a la autoridad de certificación cuando desactive el certificado. Consulte **Comprobación de si debe realizar procedimientos adicionales(P. 5)** , y anote la información necesaria antes de borrar la clave/certificado.

Uso del panel de control(P. 42)
Al utilizar la IU remota(P. 43)

■ Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Lista de claves y certificados> ▶ <Lista claves y certificados para disposit.>.**

- <Lista claves y certificados para disposit.> no aparecerá a menos que la función de firma del usuario esté habilitada en el equipo. Si es el caso, proceda al siguiente paso.

3 **Seleccione la clave y el certificado ▶ Pulse <Eliminar> ▶ <Sí>.**

Pantalla de ejemplo:

NOTA:

- Si aparece , la clave está corrupta o no es válida.
- Si no aparece , el certificado de la clave no existe.
- Si selecciona una clave y certificado y pulsa <Detalles de certificado>, aparecerá información detallada sobre el certificado. También puede pulsar <Verif. certif.> en esta pantalla para comprobar si el certificado es válido.

■Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Seleccione la clave y el certificado ▶ Haga clic en [Eliminar] ▶ [Aceptar].**

NOTA

- Si aparece , la clave está corrupta o no es válida.
- Si aparece , el certificado de la clave no existe.
- Haga clic en un nombre de clave para ver la información detallada del certificado. También puede hacer clic en [Verificar certificado] en esta pantalla para comprobar si el certificado es válido.

Paso 5: Desactivación del certificado (para IEEE 802.1X)

Desactive los certificados generados en el pasado. El procedimiento difiere según el tipo de certificado.

■ Para un certificado autofirmado

Si tiene algún certificado con clave que requiera procedimientos adicionales registrado en el servidor de autenticación IEEE 802.1X como certificado de confianza, elimínelo.

■ Para un certificado CSR/SCEP

Solicite a la autoridad de certificación que ha emitido el certificado que lo revoque. Consulte el [Emisor] en el certificado para que la autoridad de certificación lo solicite.

NOTA

- Si está comprobando la revocación de un certificado mediante una CRL en un servidor de autenticación IEEE 802.1X , registre la CRL actualizada en el ordenador o navegador web después de que el certificado sea revocado.
- Si utiliza un método distinto a la CRL (por ejemplo, OCSP) para comprobar la revocación de certificados, realice el procedimiento correspondiente a ese método.

Paso 6: Activación del certificado nuevo (para IEEE 802.1X)

Active el certificado.

■ Para un certificado autofirmado

Registre el nuevo certificado como certificado de confianza en el servidor de autenticación IEEE 802.1X.

■ Para un certificado CSR/SCEP

No es necesario realizar procedimientos adicionales.

Procedimiento para IPSec

Paso 1: Comprobación del método de autenticación (para IPSec)

Debe realizar los procedimientos siguientes si el método de autenticación para la opción IKE en IPSec está establecido como <Método de firma digital>.
Siga el procedimiento siguiente para comprobar el método de autenticación.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Uso del panel de control(P. 47)
Al utilizar la IU remota(P. 48)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de IPSec>.**

3 **Seleccione la política registrada ▶ Pulse <Editar> ▶ <Opciones de IKE>.**

Pantalla de ejemplo:

4 **Pulse <Siguiente> ▶ Compruebe <Método de autenticación>.**

Pantalla de ejemplo:

- Si <Método de autenticación> está establecido como <Método de firma digital> y aparece un nombre clave para <Clave y certificado>, realice los procedimientos siguientes.
- Si <Método de autenticación> se ha establecido como <Método clave precompart.>, no es necesario que realice los procedimientos siguientes.

■Al utilizar la IU remota

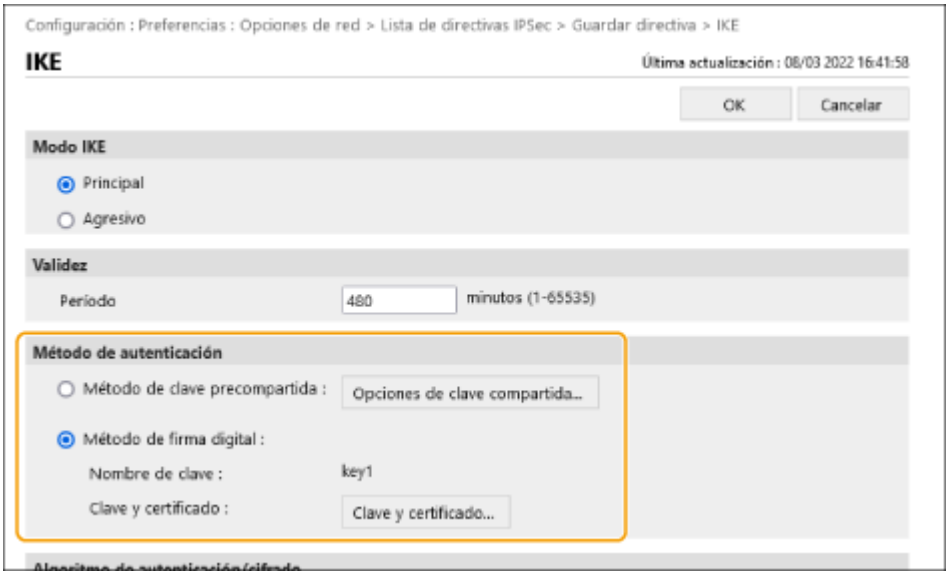
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Opciones de red] ▶ [Lista de directivas IPSec].**

4 **Haga clic en la política en la lista ▶ Haga clic en [Opciones de IKE].**

5 **Compruebe [Método de autenticación].**



- Si [Método de autenticación] está establecido como [Método de firma digital] y aparece un nombre clave, realice los procedimientos siguientes.
- Si <Método de autenticación> se ha establecido como <Método de clave precompartida>, no es necesario que realice los procedimientos siguientes.

Paso 2: Regeneración de la clave y el certificado (para IPSec)

Puede generar tres tipos de certificados para una clave generada con el equipo: un certificado autofirmado, un certificado CSR y un certificado SCEP. El procedimiento difiere según el tipo de certificado.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Para un certificado autofirmado(P. 49)
Para un certificado CSR(P. 52)
Para un certificado SCEP(P. 54)

Para un certificado autofirmado

Uso del panel de control(P. 49)
Al utilizar la IU remota(P. 50)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Generar clave> ▶ <Generar clave de comunicaciones por red>.**

3 **Configure los ajustes necesarios y pase a la pantalla siguiente.**

Pantalla de ejemplo:

a <Nombre de clave>

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b <Algoritmo de firma>

Seleccione el algoritmo hash a utilizar para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512. Si se selecciona <RSA> para c, y se establece <Longitud de clave (bits)> para <1024> o más para d, se pueden seleccionar los algoritmos hash SHA384 y SHA512.

c <Algoritmo de clave>

Seleccione el algoritmo de clave. Si se selecciona <RSA>, aparecerá <Longitud de clave (bits)> como elemento de configuración para d. Si se selecciona <ECDSA>, aparecerá en su lugar <Tipo de clave>.

d <Longitud de clave (bits)>/<Tipo de clave>

Especifique la longitud de la clave si se selecciona <RSA> para c, o especifique el tipo de clave si se selecciona <ECDSA>. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

4 Configure los elementos necesarios para el certificado ▶ Pulse <Generar clave>.

Pantalla de ejemplo:

a <Válido desde>/<Fecha de caducidad>

Introduzca la fecha de inicio y los datos de finalización del periodo de validez del certificado.

b <País/región>/<Estado>/<Ciudad>/<Organización>/<Unidad organiz.>

Seleccione el código de país de la lista e introduzca la ubicación y el nombre de la organización.

c <Nombre común>

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

■ Al utilizar la IU remota

1 Inicie la IU remota.

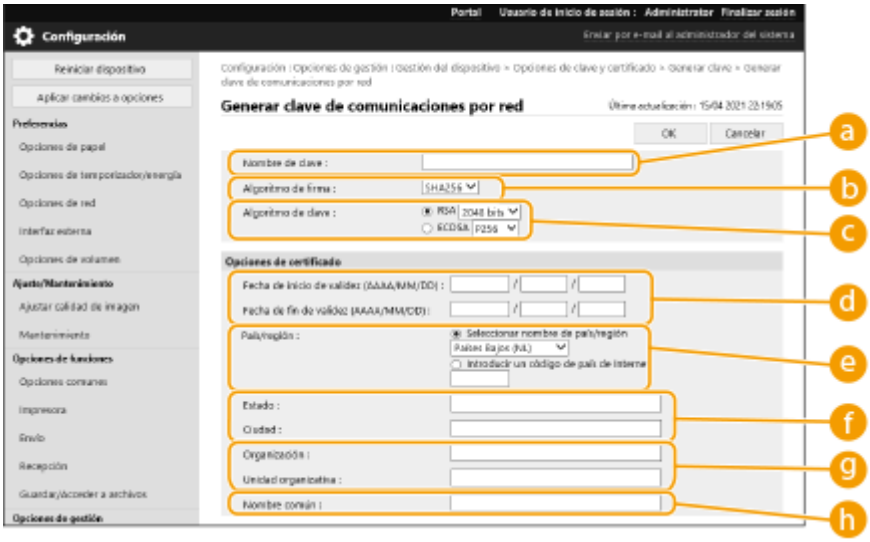
2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 Haga clic en [Generar clave].

5 Haga clic en [Comunicación de red].

6 Configure la clave y los ajustes del certificado.



a [Nombre de clave]

Introduzca un nombre de clave utilizando caracteres alfanuméricos. Utilice un nombre que sea fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash que se utilizará para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512.

c [Algoritmo de clave]

Seleccione [RSA] o [ECDSA] como el algoritmo de generación de clave. Especifique la longitud de la clave si se selecciona [RSA] o indique el tipo de clave si se selecciona [ECDSA]. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

NOTA:

- Si se selecciona [SHA384] o [SHA512] para [Algoritmo de firma], no se podrá establecer la longitud de la clave en [512 bits] al seleccionar [RSA] para [Algoritmo de clave].

d [Fecha de inicio de validez (AAAA/MM/DD)]/[Fecha de fin de validez (AAAA/MM/DD)]

Introduzca la fecha de inicio y los datos de finalización del período de validez del certificado. La [Fecha de fin de validez (AAAA/MM/DD)] no puede ajustarse a una fecha anterior a la fecha en [Fecha de inicio de validez (AAAA/MM/DD)].

e [País/región]

Haga clic en [Seleccionar nombre de país/región] y seleccione el país/región en la lista desplegable. También puede hacer clic en [Introducir un código de país de Internet] e introducir el código el país, como por ejemplo "US" para Estados Unidos.

f [Estado]/[Ciudad]

Introduzca la ubicación utilizando los caracteres alfanuméricos que sean necesarios.

g [Organización]/[Unidad organizativa]

Introduzca el nombre de la organización utilizando los caracteres alfanuméricos que sean necesarios.

h [Nombre común]

Introduzca el nombre común del certificado utilizando los caracteres alfanuméricos que sean necesarios. "Nombre común" suele abreviarse como "CN".

7 Haga clic en [Bien].

- Generar una clave y un certificado puede llevar cierto tiempo.
- Las claves y certificados generados se registran automáticamente en el equipo.

Para un certificado CSR

Genere una clave y una CSR en el equipo. Utilice los datos de CSR que aparecen en la pantalla o que se envían a un archivo para solicitar a la autoridad de certificación que emita un certificado. A continuación, registre el certificado emitido para la clave.
Este ajuste solo se puede configurar desde la IU remota.

■1. Generación de una clave y una CSR

1 **Inicie la IU remota.**

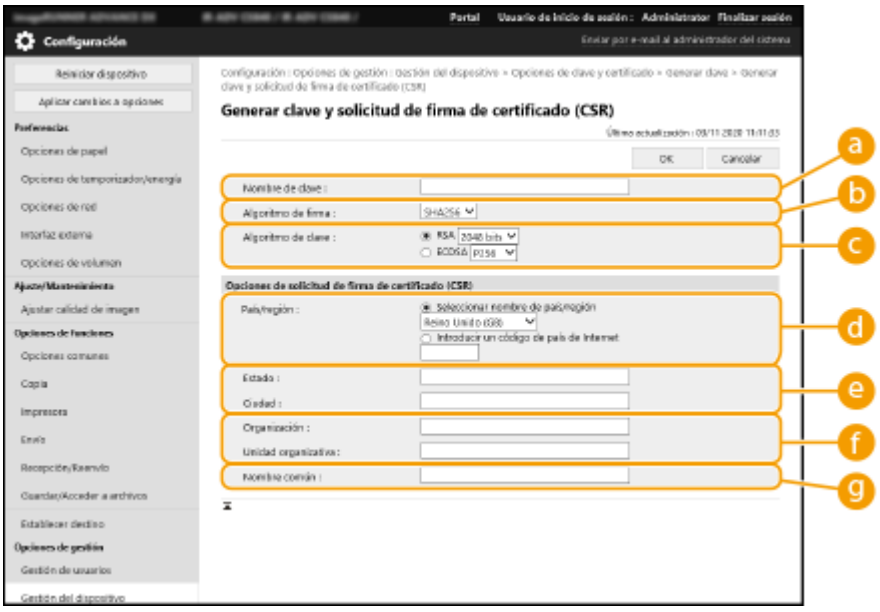
2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Haga clic en [Generar clave].**

5 **Haga clic en [Clave y solicitud de firma de certificado (CSR)].**

6 **Configure la clave y los ajustes del certificado.**



ⓐ [Nombre de clave]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

ⓑ [Algoritmo de firma]

Seleccione el algoritmo hash para utilizar para la firma.

ⓒ [Algoritmo de clave]

Seleccione el algoritmo de clave y especifique la longitud de la clave si se selecciona [RSA], o bien especifique el tipo de clave si se selecciona [ECDSA].

[País/región]

Seleccione el código de país de la lista o introdúzcalo directamente.

[Estado]/[Ciudad]

Introduzca la ubicación.

[Organización]/[Unidad organizativa]

Escriba el nombre de la organización.

[Nombre común]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

7 Haga clic en [Bien].

➡ Aparecen los datos de CSR.

- Si desea guardar los datos de CSR en un archivo, haga clic en [Guardar en archivo] y especifique la ubicación de almacenamiento.

NOTA:

- La clave que ha generado la CSR aparece en la pantalla de lista de claves y certificados, pero no puede usarla por sí sola. Para utilizar esta clave, tiene que registrar el certificado que se emite luego a partir de la CSR.

8 Solicite a la autoridad de certificación que emita un certificado en base a los datos de la CSR.

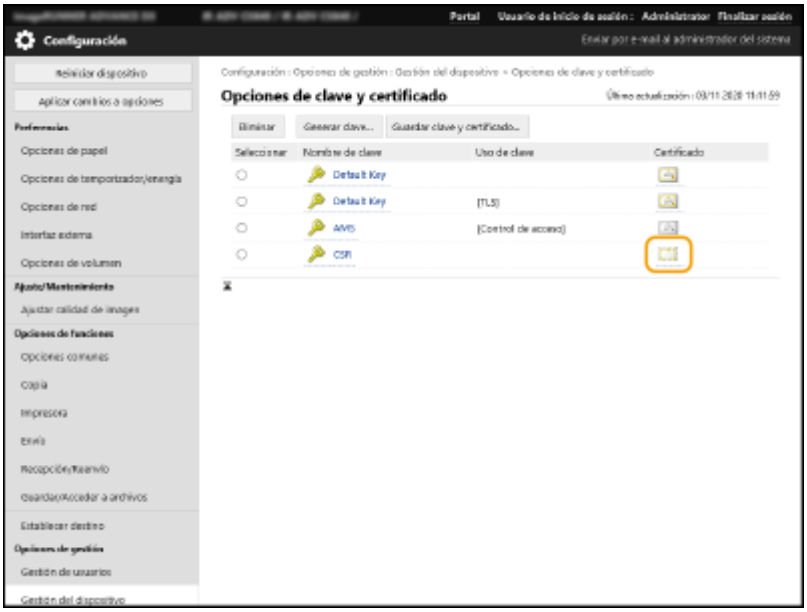
■2. Registro del certificado emitido en la clave

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 En la lista [Certificado], haga clic en para el certificado que desee registrar.



5 **Haga clic en [Guardar certificado...].**

6 **Registre el certificado.**

- Haga clic en [Examinar...] ▶ Especifique el archivo (certificado) para registrar ▶ Haga clic en [Guardar].

Para un certificado SCEP

Solicite manualmente al servidor SCEP que emita un certificado.
Solo puede configurar este ajuste desde la IU remota.

NOTA

- No podrá enviar una solicitud manual de emisión de un certificado si se selecciona [Habilitar el temporizador para la solicitud automática de emisión de certificado]. Desmarque esta opción si está seleccionada.

Inicie la IU remota ▶ Haga clic en [Configuración] ▶ [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)] ▶ [Opciones para la solicitud automática de emisión de certificado] ▶ Desmarque [Habilitar el temporizador para la solicitud automática de emisión de certificado] ▶ Haga clic en [Actualizar].

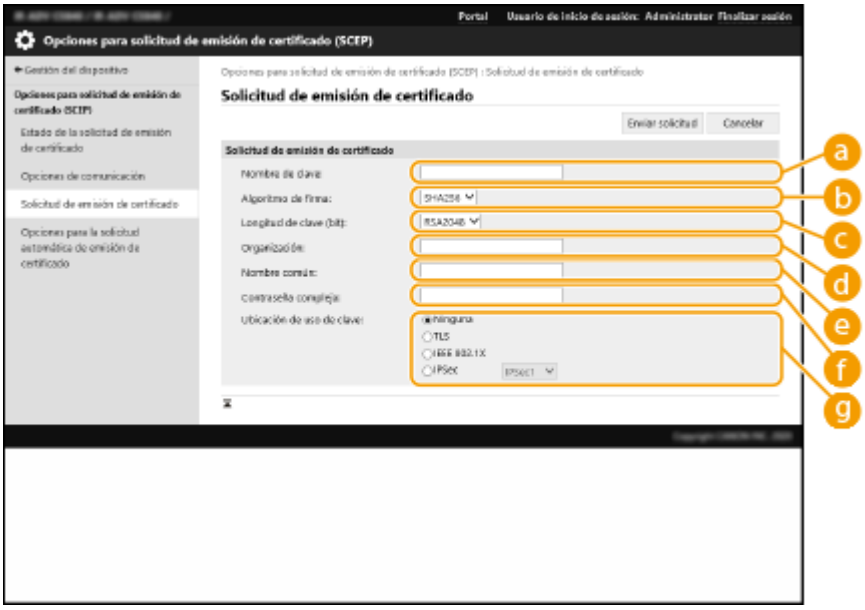
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones para solicitud de emisión de certificado (SCEP)].**

4 **Haga clic en [Solicitud de emisión de certificado].**

5 Configure los ajustes necesarios para solicitar un certificado.



a [Nombre de clave:]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b [Algoritmo de firma:]

Seleccione el algoritmo hash para utilizar para la firma.

c [Longitud de clave (bit):]

Seleccione la longitud de la clave.

d [Organización:]

Escriba el nombre de la organización.

e [Nombre común:]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

f [Contraseña compleja:]

Cuando se configure una contraseña en la parte del servidor SCEP, introduzca la contraseña de comprobación incluida en los datos de solicitud (PKCS#9) para solicitar un certificado para emitirse.

g [Ubicación de uso de clave:]

Seleccione [IPSec].

NOTA:

- Al seleccionar una opción que no sea [Ninguna], active cada función con antelación. Si se obtiene correctamente un certificado con todas las funciones desactivadas, el certificado se asigna a la ubicación de uso de la clave, pero las funciones no se activan de forma automática.

6 Haga clic en [Enviar solicitud].

7 **Haga clic en [Reiniciar].**

Paso 3: Restablecimiento de la clave y el certificado (para IPSec)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.
Este procedimiento no es necesario para un certificado SCEP.

Para un certificado autofirmado/CSR

Uso del panel de control(P. 57)
Al utilizar la IU remota(P. 58)

■Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de IPSec>.**

3 **Seleccione la política para restablecer la clave y el certificado para ▶ Pulse <Editar> ▶ <Opciones de IKE>.**
Pantalla de ejemplo:

4 **Pulse <Siguiente> ▶ Seleccione <Método de firma digital> en <Método de autenticación> ▶ Pulse <Clave y certificado>.**
Pantalla de ejemplo:

5 **Seleccione la clave y el certificado a utilizar en la lista ▶ Pulse <Convertir en prefijada> ▶ <Sí>.**

6 **Pulse <Aceptar>.**

7 **Pulse (Configuración) ▶ (Configuración) ▶ <Aplicar camb. a opc.> ▶ <Sí>.**

➠ El equipo se reinicia y las opciones se aplican.

■ Al utilizar la IU remota

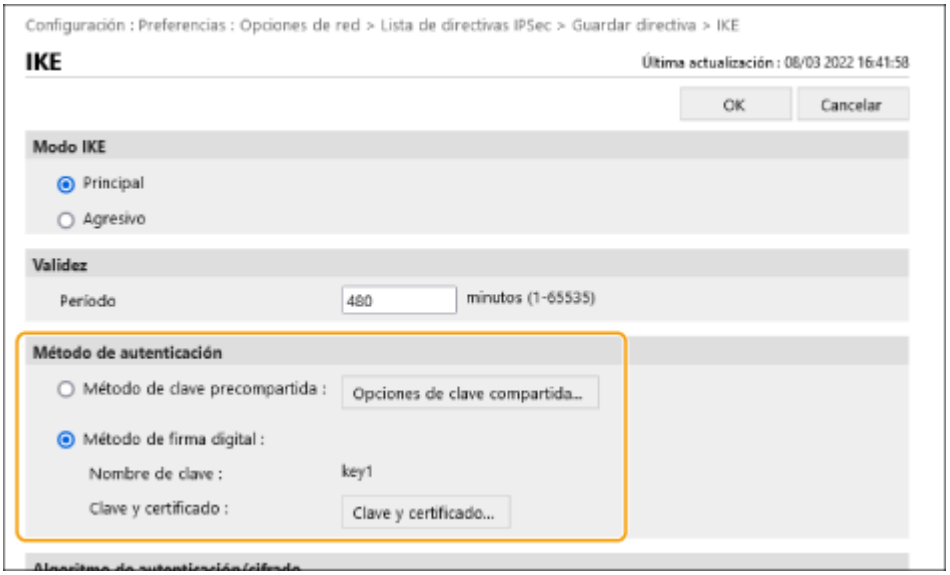
1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Opciones de red] ▶ [Lista de directivas IPSec].**

4 **Haga clic en la política para restablecer la clave y el certificado en la lista ▶ Haga clic en [Opciones de IKE].**

5 **Seleccione [Método de firma digital] en [Método de autenticación] ▶ Haga clic en [Clave y certificado].**



6 **Haga clic en [Usar] para utilizar la clave en la lista.**

7 **Haga clic en [Bien].**

8 **Haga clic en [Aplicar cambios a opciones] para reiniciar el equipo.**

➠ El equipo se reinicia y las opciones se aplican.

Paso 4: Eliminación de una clave/certificado generado en el pasado (para IPSec)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

NOTA

- Es posible que tenga que transmitir información a la autoridad de certificación cuando desactive el certificado. Consulte **Comprobación de si debe realizar procedimientos adicionales(P. 5)** , y anote la información necesaria antes de borrar la clave/certificado.

Uso del panel de control(P. 60)
Al utilizar la IU remota(P. 61)

■ Uso del panel de control

1 Pulse (Configuración).

2 Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Lista de claves y certificados> ▶ <Lista claves y certificados para disposit.>.

- <Lista claves y certificados para disposit.> no aparecerá a menos que la función de firma del usuario esté habilitada en el equipo. Si es el caso, proceda al siguiente paso.

3 Seleccione la clave y el certificado ▶ Pulse <Eliminar> ▶ <Sí>.

Pantalla de ejemplo:

NOTA:

- Si aparece , la clave está corrupta o no es válida.
- Si no aparece , el certificado de la clave no existe.
- Si selecciona una clave y certificado y pulsa <Detalles de certificado>, aparecerá información detallada sobre el certificado. También puede pulsar <Verif. certif.> en esta pantalla para comprobar si el certificado es válido.

■Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Seleccione la clave y el certificado ▶ Haga clic en [Eliminar] ▶ [Aceptar].**

NOTA

- Si aparece , la clave está corrupta o no es válida.
- Si aparece , el certificado de la clave no existe.
- Haga clic en un nombre de clave para ver la información detallada del certificado. También puede hacer clic en [Verificar certificado] en esta pantalla para comprobar si el certificado es válido.

Paso 5: Desactivación del certificado (para IPSec)

Desactive los certificados generados en el pasado. El procedimiento difiere según el tipo de certificado.

■ Para un certificado autofirmado

Si tiene algún certificado con clave que requiera procedimientos adicionales registrado como certificado de confianza en el dispositivo que se comunica con IPSec, elimínelo.Tras eliminar el certificado registrado, registre el certificado de la clave regenerada.

■ Para un certificado CSR/SCEP

Solicite a la autoridad de certificación que ha emitido el certificado que lo revoque. Consulte el [Emisor] en el certificado para que la autoridad de certificación lo solicite.

NOTA

- Si está comprobando la revocación de un certificado mediante una CRL en el dispositivo que se comunica con IPSec, registre la CRL actualizada en el ordenador o navegador web después de que el certificado sea revocado.
- Si utiliza un método distinto a la CRL (por ejemplo, OCSP) para comprobar la revocación de certificados, realice el procedimiento correspondiente a ese método.

Paso 6: Activación del certificado nuevo (para IPSec)

Active el certificado.

■ Para un certificado autofirmado

Registre el nuevo certificado como certificado de confianza en el dispositivo que se comunica con IPSec.

■ Para un certificado CSR/SCEP

No es necesario realizar procedimientos adicionales.

Procedimiento para SIP

Paso 1: Comprobación de los ajustes (para SIP)

Deberá realizar los procedimientos adicionales cuando se cumplan las dos condiciones siguientes:

- <Usar TLS> está activado <Opciones de intranet> en <Opciones de SIP>
- Se muestra el nombre de la clave para <Clave y certificado> en <Opciones de TLS> en <Opciones de SIP>

Siga el procedimiento que se indica a continuación para comprobar los ajustes.

Uso del panel de control(P. 65)
Al utilizar la IU remota(P. 66)

Uso del panel de control

■ Comprobación de <Usar TLS>

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de SIP> ▶ <Opciones de intranet>.**

3 **Compruebe <Usar TLS>.**

Pantalla de ejemplo:

- Si <Usar TLS> está configurado como <Sí>, pase a comprobar <Clave y certificado>.
- Si <Usar TLS> se ha establecido como <No>, no es necesario que realice los procedimientos siguientes.

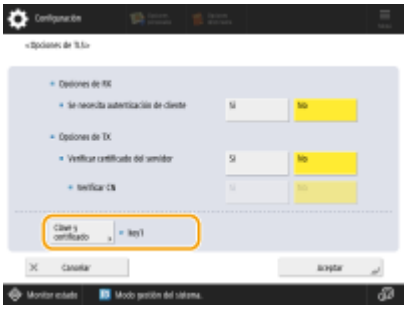
■ Comprobación de <Clave y certificado>

1 **Pulse (Configuración).**

2 **Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de SIP> ▶ <Opciones de TLS>.**

3 Compruebe si aparece el nombre de clave para <Clave y certificado>.

Pantalla de ejemplo:



- Si aparece un nombre de clave para <Clave y certificado>, realice los procedimientos siguientes.
- Si el nombre de clave no aparece para <Clave y certificado>, no es necesario que realice los procedimientos siguientes.

Al utilizar la IU remota

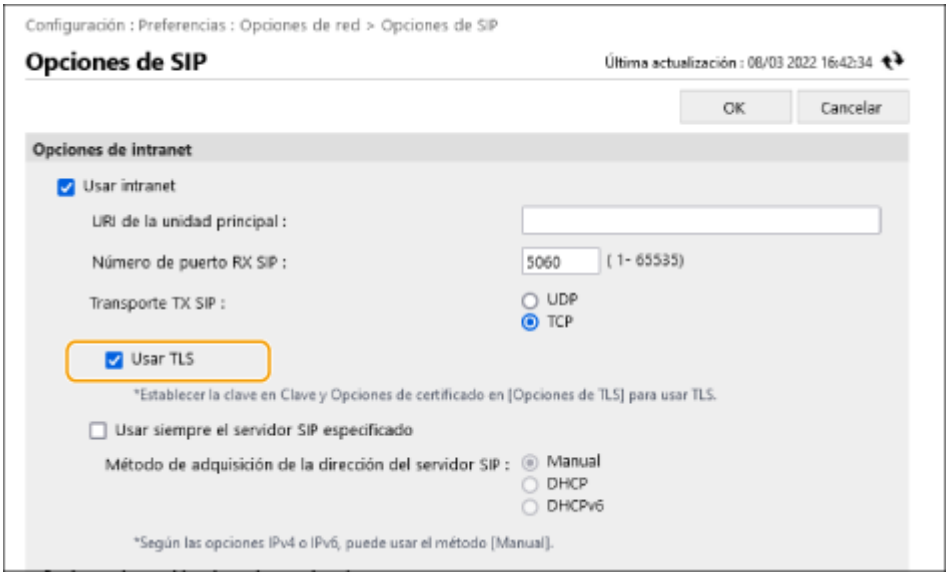
■Comprobación de [Usar TLS] y [Clave y certificado]

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

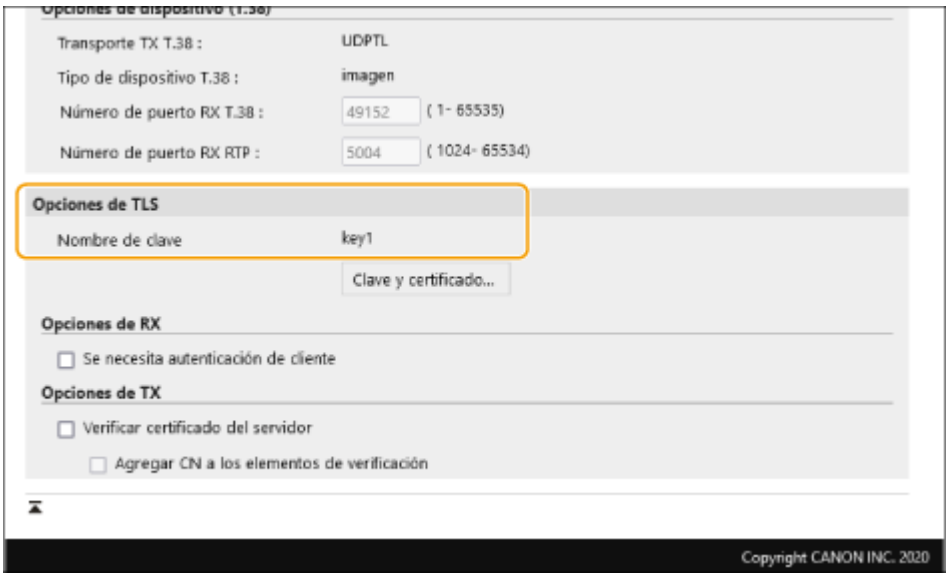
3 Haga clic en [Opciones de red] ▶ [Opciones de SIP].

4 Compruebe [Usar TLS] en [Opciones de intranet].



- Si se ha seleccionado [Usar TLS], continúe para comprobar [Clave y certificado].
- Si se ha desmarcado [Usar TLS], no es necesario que realice los procedimientos siguientes.

5 Compruebe [Nombre de clave] en [Opciones de TLS].



- Si aparece un nombre de clave, realice los procedimientos siguientes.
- Si el nombre de clave no aparece, no es necesario que realice los procedimientos siguientes.

Paso 2: Regeneración de la clave y el certificado (para SIP)

Puede generar dos tipos de certificados para una clave generada con el equipo: un certificado autofirmado y un certificado CSR. El procedimiento difiere según el tipo de certificado.
Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

Para un certificado autofirmado(P. 68)
Para un certificado CSR(P. 71)

Para un certificado autofirmado

Uso del panel de control(P. 68)
Al utilizar la IU remota(P. 69)

■ Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Generar clave> ▶ <Generar clave de comunicaciones por red>.**

3 **Configure los ajustes necesarios y pase a la pantalla siguiente.**

Pantalla de ejemplo:

a <Nombre de clave>

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b <Algoritmo de firma>

Seleccione el algoritmo hash a utilizar para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512. Si se selecciona <RSA> para c, y se establece <Longitud de clave (bits)> para <1024> o más para d, se pueden seleccionar los algoritmos hash SHA384 y SHA512.

c <Algoritmo de clave>

Seleccione el algoritmo de clave. Si se selecciona <RSA>, aparecerá <Longitud de clave (bits)> como elemento de configuración para d. Si se selecciona <ECDSA>, aparecerá en su lugar <Tipo de clave>.

d <Longitud de clave (bits)>/<Tipo de clave>

Especifique la longitud de la clave si se selecciona <RSA> para c, o especifique el tipo de clave si se selecciona <ECDSA>. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

4 Configure los elementos necesarios para el certificado ▶ Pulse <Generar clave>.

Pantalla de ejemplo:

a <Válido desde>/<Fecha de caducidad>

Introduzca la fecha de inicio y los datos de finalización del periodo de validez del certificado.

b <País/región>/<Estado>/<Ciudad>/<Organización>/<Unidad organiz.>

Seleccione el código de país de la lista e introduzca la ubicación y el nombre de la organización.

c <Nombre común>

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

■ Al utilizar la IU remota

1 Inicie la IU remota.

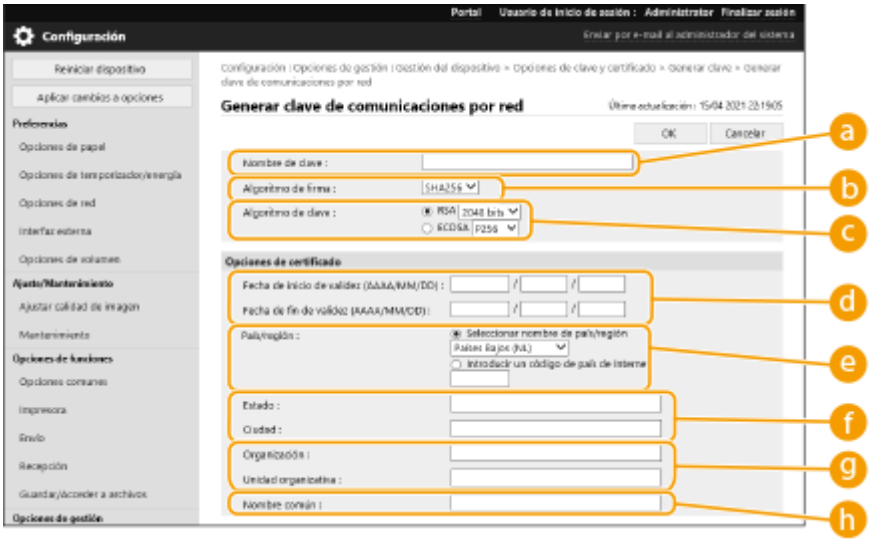
2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 Haga clic en [Generar clave].

5 Haga clic en [Comunicación de red].

6 Configure la clave y los ajustes del certificado.



a [Nombre de clave]

Introduzca un nombre de clave utilizando caracteres alfanuméricos. Utilice un nombre que sea fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash que se utilizará para la firma. Los algoritmos hash disponibles varían en función de la longitud de la clave. Una clave de 1024 bits de longitud o más puede admitir algoritmos hash SHA384 y SHA512.

c [Algoritmo de clave]

Seleccione [RSA] o [ECDSA] como el algoritmo de generación de clave. Especifique la longitud de la clave si se selecciona [RSA] o indique el tipo de clave si se selecciona [ECDSA]. En ambos casos, un valor superior proporciona una mayor seguridad, pero reduce la velocidad de procesamiento de la comunicación.

NOTA:

- Si se selecciona [SHA384] o [SHA512] para [Algoritmo de firma], no se podrá establecer la longitud de la clave en [512 bits] al seleccionar [RSA] para [Algoritmo de clave].

d [Fecha de inicio de validez (AAAA/MM/DD)]/[Fecha de fin de validez (AAAA/MM/DD)]

Introduzca la fecha de inicio y los datos de finalización del período de validez del certificado. La [Fecha de fin de validez (AAAA/MM/DD)] no puede ajustarse a una fecha anterior a la fecha en [Fecha de inicio de validez (AAAA/MM/DD)].

e [País/región]

Haga clic en [Seleccionar nombre de país/región] y seleccione el país/región en la lista desplegable. También puede hacer clic en [Introducir un código de país de Internet] e introducir el código el país, como por ejemplo "US" para Estados Unidos.

f [Estado]/[Ciudad]

Introduzca la ubicación utilizando los caracteres alfanuméricos que sean necesarios.

g [Organización]/[Unidad organizativa]

Introduzca el nombre de la organización utilizando los caracteres alfanuméricos que sean necesarios.

h [Nombre común]

Introduzca el nombre común del certificado utilizando los caracteres alfanuméricos que sean necesarios. "Nombre común" suele abreviarse como "CN".

7 Haga clic en [Bien].

- Generar una clave y un certificado puede llevar cierto tiempo.
- Las claves y certificados generados se registran automáticamente en el equipo.

Para un certificado CSR

Genere una clave y una CSR en el equipo. Utilice los datos de CSR que aparecen en la pantalla o que se envían a un archivo para solicitar a la autoridad de certificación que emita un certificado. A continuación, registre el certificado emitido para la clave.
Este ajuste solo se puede configurar desde la IU remota.

■1. Generación de una clave y una CSR

1 **Inicie la IU remota.**

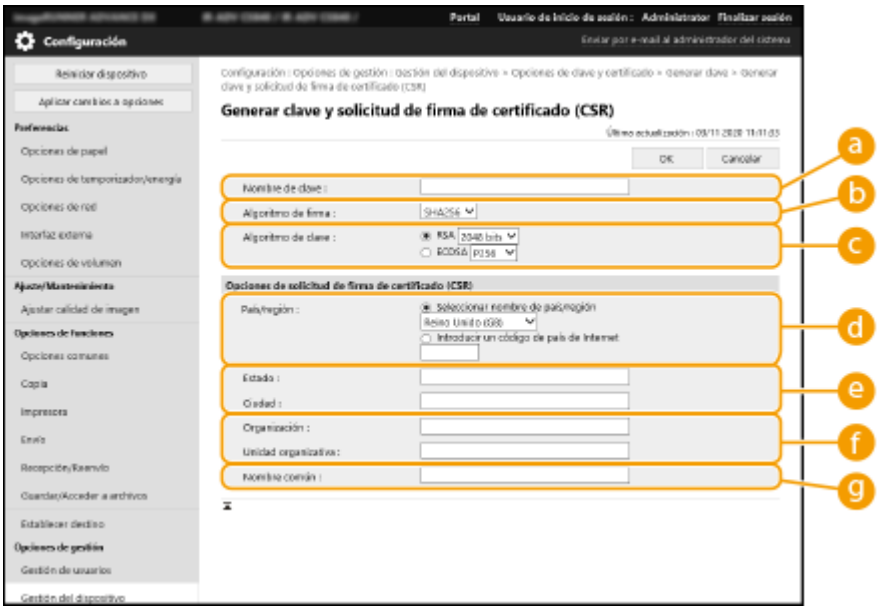
2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Haga clic en [Generar clave].**

5 **Haga clic en [Clave y solicitud de firma de certificado (CSR)].**

6 **Configure la clave y los ajustes del certificado.**



a [Nombre de clave]

Introduzca un nombre de clave. Utilice un nombre fácil de buscar en una lista.

b [Algoritmo de firma]

Seleccione el algoritmo hash para utilizar para la firma.

c [Algoritmo de clave]

Seleccione el algoritmo de clave y especifique la longitud de la clave si se selecciona [RSA], o bien especifique el tipo de clave si se selecciona [ECDSA].

[País/región]

Seleccione el código de país de la lista o introdúzcalo directamente.

[Estado]/[Ciudad]

Introduzca la ubicación.

[Organización]/[Unidad organizativa]

Escriba el nombre de la organización.

[Nombre común]

Introduzca la dirección IP o FQDN.

- Al realizar una impresión IPPS en un entorno Windows, asegúrese de introducir la dirección IP del equipo.
- Es necesario un servidor DNS para introducir el FQDN en el equipo. Introduzca la dirección IP del equipo si no se utiliza un servidor DNS.

7 Haga clic en [Bien].

➡ Aparecen los datos de CSR.

- Si desea guardar los datos de CSR en un archivo, haga clic en [Guardar en archivo] y especifique la ubicación de almacenamiento.

NOTA:

- La clave que ha generado la CSR aparece en la pantalla de lista de claves y certificados, pero no puede usarla por sí sola. Para utilizar esta clave, tiene que registrar el certificado que se emite luego a partir de la CSR.

8 Solicite a la autoridad de certificación que emita un certificado en base a los datos de la CSR.

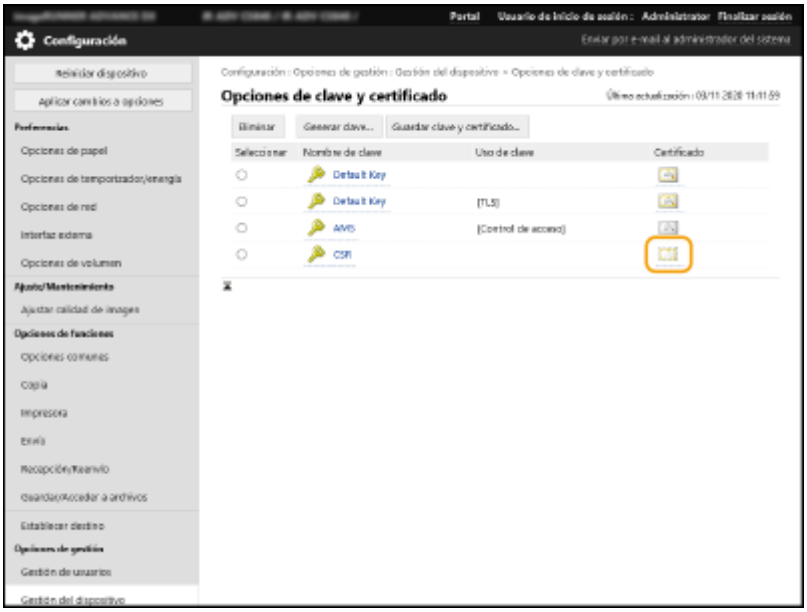
■2. Registro del certificado emitido en la clave

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].

4 En la lista [Certificado], haga clic en para el certificado que desee registrar.



5 Haga clic en [Guardar certificado...].

6 Registre el certificado.

- Haga clic en [Examinar...] ▶ Especifique el archivo (certificado) para registrar ▶ Haga clic en [Guardar].

Paso 3: Restablecimiento de la clave y el certificado (para SIP)

Establezca la clave y el certificado generados como la clave y el certificado a utilizar en la comunicación cifrada TLS de SIP.

Uso del panel de control(P. 74)
Al utilizar la IU remota(P. 75)

■ Uso del panel de control

1 Pulse (Configuración).

2 Pulse <Preferencias> ▶ <Red> ▶ <Opciones de TCP/IP> ▶ <Opciones de SIP> ▶ <Opciones de TLS>.

3 Configure las diferentes opciones de <Opciones de RX> y <Opciones de TX> ▶ Pulse <Clave y certificado>.

Pantalla de ejemplo:

<Opciones de RX>	
<Se necesita autenticación de cliente>	Seleccione <Sí> o <No>. Si selecciona <Sí>, el equipo solicitará la autenticación del cliente cuando el equipo reciba un fax IP.
<Opciones de TX>	
<Verificar certificado del servidor>	Seleccione <Sí> o <No>. Si selecciona <Sí>, el equipo comprobará si el certificado del servidor TLS es válido cuando el equipo reciba un fax IP.
<Verificar CN>	Seleccione <Sí> o <No>. Si selecciona <Sí>, el equipo comprobará el CN (nombre común) cuando el equipo reciba un fax IP.

4 Seleccione la clave y el certificado a usar para la comunicación cifrada TLS de SIP ▶ Pulse <Convertir en prefijada> ▶ <Aceptar>.

Pantalla de ejemplo:

NOTA

- No puede seleccionar la clave y el certificado si el estado es "Uso".
- Puede pulsar <Detalles de certificado> para comprobar la información detallada del certificado.
- Puede pulsar <Mostrar ubicación de uso> para comprobar el uso de la clave/certificado.

5 **Pulse <Aceptar>.**

6 **Pulse (Configuración) ▶ (Configuración) ▶ <Aplicar cambios a opciones> ▶ <Sí>.**

➠ El equipo se reinicia y las opciones se aplican.

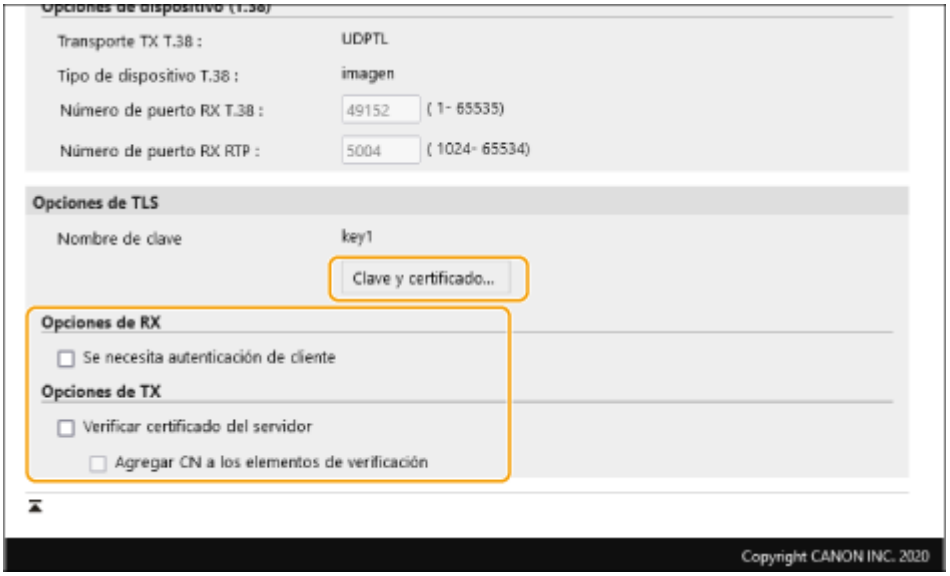
■ Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

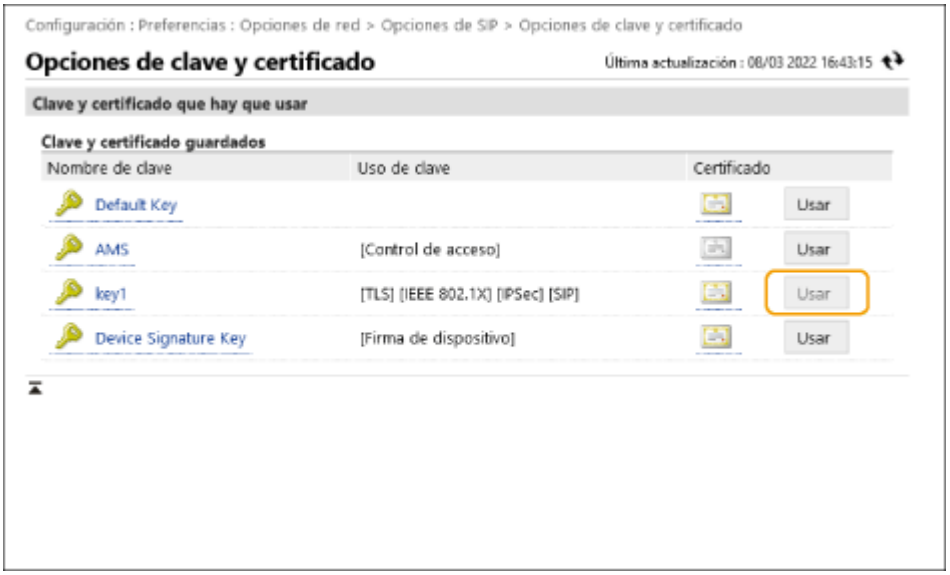
3 **Haga clic en [Opciones de red] ▶ [Opciones de SIP].**

4 **Configure las diferentes opciones de [Opciones de TLS] ▶ Haga clic en [Clave y certificado].**



[Opciones de RX]	
[Se necesita autenticación de cliente]	Si selecciona esta casilla, el equipo solicitará la autenticación del cliente cuando el equipo reciba un fax IP.
[Opciones de TX]	
[Verificar certificado del servidor]	Si selecciona esta casilla, el equipo comprobará si el certificado del servidor TLS es válido cuando el equipo reciba un fax IP.
[Agregar CN a los elementos de verificación]	Seleccione [Sí] o [No]. Si selecciona esta casilla, el equipo comprobará el CN (nombre común) cuando el equipo reciba un fax IP.

5 Haga clic en [Usar] para utilizar la clave en la lista.



6 Haga clic en [OK].

7 Haga clic en [Aplicar cambios a opciones] para reiniciar el equipo.

➠ El equipo se reinicia y las opciones se aplican.

Paso 4: Eliminación de una clave/certificado generado en el pasado (para SIP)

Es posible que no pueda realizar operaciones desde el panel de control en función del modelo del equipo. Si es el caso, realice las operaciones desde la IU remota.

NOTA

- Es posible que tenga que transmitir información a la autoridad de certificación cuando desactive el certificado. Consulte **Comprobación de si debe realizar procedimientos adicionales(P. 5)** , y anote la información necesaria antes de borrar la clave/certificado.

Uso del panel de control(P. 77)
Al utilizar la IU remota(P. 78)

■ Uso del panel de control

1 **Pulse (Configuración).**

2 **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Lista de claves y certificados> ▶ <Lista claves y certificados para disposit.>.**

- <Lista claves y certificados para disposit.> no aparecerá a menos que la función de firma del usuario esté habilitada en el equipo. Si es el caso, proceda al siguiente paso.

3 **Seleccione la clave y el certificado ▶ Pulse <Eliminar> ▶ <Sí>.**

Pantalla de ejemplo:

NOTA:

- Si aparece , la clave está corrupta o no es válida.
- Si no aparece , el certificado de la clave no existe.
- Si selecciona una clave y certificado y pulsa <Detalles de certificado>, aparecerá información detallada sobre el certificado. También puede pulsar <Verif. certif.> en esta pantalla para comprobar si el certificado es válido.

■Al utilizar la IU remota

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**

4 **Seleccione la clave y el certificado ▶ Haga clic en [Eliminar] ▶ [Aceptar].**

NOTA

- Si aparece , la clave está corrupta o no es válida.
- Si aparece , el certificado de la clave no existe.
- Haga clic en un nombre de clave para ver la información detallada del certificado. También puede hacer clic en [Verificar certificado] en esta pantalla para comprobar si el certificado es válido.

Paso 5: Desactivación del certificado (para SIP)

Desactive los certificados generados en el pasado. El procedimiento difiere según el tipo de certificado.

■ Para un certificado autofirmado

Si tiene algún certificado con clave que requiera procedimientos adicionales registrado como certificado de confianza en otro equipo de fax IP, elimínelo.Tras eliminar el certificado registrado, registre el certificado de la clave regenerada.

■ Para un certificado CSR

Solicite a la autoridad de certificación que ha emitido el certificado que lo revoque. Consulte el [Emisor] en el certificado para que la autoridad de certificación lo solicite.

NOTA

- Si está comprobando la revocación de un certificado mediante el otro equipo de fax IP, registre la CRL actualizada en el ordenador o navegador web después de que el certificado sea revocado.
- Si utiliza un método distinto a la CRL (por ejemplo, OCSP) para comprobar la revocación de certificados, realice el procedimiento correspondiente a ese método.

Paso 6: Activación del certificado nuevo (para SIP)

Active el certificado.

■ Para un certificado autofirmado

Registre el nuevo certificado como certificado de confianza en el otro equipo de fax IP.

■ Para un certificado CSR

No es necesario realizar procedimientos adicionales.

Procedimiento para las firmas de dispositivo

Paso 1: Comprobación de los ajustes S/MIME (para firmas de dispositivo)

Compruebe si debe realizar los procedimientos adicionales para S/MIME y las firmas de dispositivo.

Siga el procedimiento que se indica a continuación para comprobar S/MIME.

Uso del panel de control(P. 82)
Al utilizar la IU remota(P. 82)

■Uso del panel de control

1 Pulse (Configuración).

2 Pulse <Opciones de funciones> ▶ <Envío> ▶ <Opciones de e-mail/I-fax> ▶ <Opciones de S/MIME>.

3 Compruebe <Opciones de cifrado> y <Agregar firmas digitales>.

Pantalla de ejemplo:

- Si <Opciones de cifrado> se ha establecido como <No cifrar> y <Agregar firmas digitales> se ha establecido como <No>, realice los procedimientos siguientes solo para las firmas de dispositivo.
- Si se especifican otros ajustes, realice los procedimientos siguientes para S/MIME y las firmas de dispositivo.

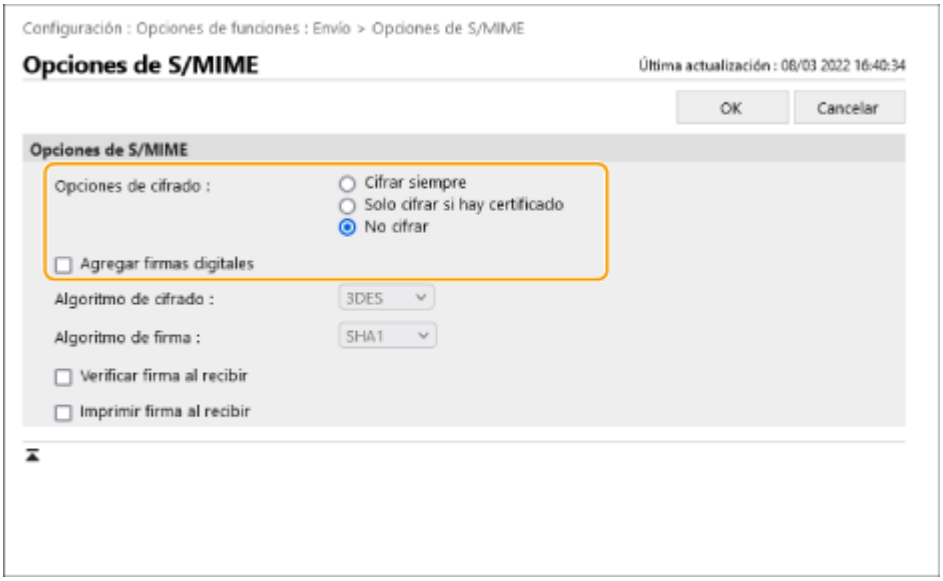
■Al utilizar la IU remota

1 Inicie la IU remota.

2 Haga clic en [Configuración] en la página del portal.

3 Haga clic en [Envío] ▶ [Opciones de S/MIME].

4 Compruebe [Opciones de cifrado] y [Agregar firmas digitales].



- Si se ha seleccionado [No cifrar] para [Opciones de cifrado] y [Agregar firmas digitales] no se ha seleccionado, realice los procedimientos siguientes solo para las firmas de dispositivo.
- Si se especifican otros ajustes, realice los procedimientos siguientes para S/MIME y las firmas de dispositivo.

Paso 2: Regeneración de la clave y el certificado (para firmas de dispositivo)

Uso del panel de control(P. 84)
Al utilizar la IU remota(P. 84)

Uso del panel de control

1. **Pulse (Configuración).**
2. **Pulse <Opciones de gestión> ▶ <Gestión del dispositivo> ▶ <Opciones de certificado> ▶ <Generar clave>.**
3. **Pulse <Generar/Actualizar clave firma de dispositivo> ▶ <Sí> ▶ <Aceptar>.**

Al utilizar la IU remota

1. **Inicie la IU remota.**
2. **Haga clic en [Configuración] en la página del portal.**
3. **Haga clic en [Gestión del dispositivo] ▶ [Opciones de clave y certificado].**
4. **Haga clic en [Generar clave] ▶ [Firma de dispositivo].**
5. **Haga clic en [Generar/Actualizar] ▶ [Bien].**

Paso 3: Desactivación del certificado (para firmas de dispositivo)

Desactive un certificado generado en el pasado.

■ Si hay un certificado registrado para firmas de dispositivo en Acrobat

Si se ha registrado un certificado para firmas de dispositivo en Acrobat, elimínelo.

■ Si un certificado S/MIME exportado desde este equipo se ha importado a otro equipo

Si ha exportado el certificado de clave pública (certificado S/MIME) utilizado para cifrar el correo electrónico/I-faxes a través de S/MIME desde este equipo y ha importado el certificado a otro equipo, siga el procedimiento que se indica a continuación para eliminar el certificado del equipo del que se ha importado el certificado.

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de certificado S/MIME].**

4 **Seleccione el certificado correspondiente ▶ Haga clic en [Eliminar] ▶ [Bien].**

Paso 4: Activación del certificado nuevo (para firmas de dispositivo)

Active el certificado.

■ Si hay un certificado registrado para firmas de dispositivo en Acrobat

Si hay registrado un certificado para firmas de dispositivo en Acrobat, exporte el certificado regenerado para firmas de dispositivo y registre el nuevo certificado en Acrobat.

Exportación del certificado desde el equipo(P. 86)

■ Si un certificado S/MIME exportado desde este equipo se ha importado a otro equipo

Si ha exportado el certificado de clave pública (certificado S/MIME) utilizado para cifrar el correo electrónico/I-faxes a través de S/MIME desde este equipo y ha importado el certificado a otro equipo, exporte el certificado regenerado y regístrelo en el otro equipo.

Exportación del certificado desde el equipo(P. 86)
Registro del certificado en el otro equipo(P. 86)

■ Exportación del certificado desde el equipo

Realice el procedimiento siguiente para exportar el certificado.

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Exportar firma de dispositivo].**

4 **Haga clic en [Iniciar exportación] ▶ Guarde el archivo en la ubicación deseada.**

■ Registro del certificado en el otro equipo

Realice el procedimiento siguiente para registrar el certificado en el otro equipo.

1 **Inicie la IU remota.**

2 **Haga clic en [Configuración] en la página del portal.**

3 **Haga clic en [Gestión del dispositivo] ▶ [Opciones de certificado S/MIME].**

4 **Haga clic en [Guardar certificado S/MIME].**

5 **Registre el certificado de S/MIME.**

- Haga clic en [Examinar...] ▶ Especifique el archivo (certificado de S/MIME) para registrar ▶ Haga clic en [Guardar].

Procedimientos adicionales para la configuración de Bluetooth

Procedimientos adicionales para la configuración de Bluetooth

La clave para el Bluetooth se actualiza automáticamente después de actualizar el firmware del equipo. Si está utilizando la aplicación Canon PRINT Business para dispositivos móviles, deberá registrar el dispositivo de nuevo.

Procedimiento para Bluetooth(P. 90)

Procedimiento para Bluetooth

Paso 1: Eliminación del dispositivo registrado en Canon PRINT Business (para Bluetooth)

Si la opción de Bluetooth está establecida como <Sí>, siga el procedimiento siguiente.

Funcionamiento para iOS(P. 91)
Funcionamiento para Android(P. 91)

■ Funcionamiento para iOS

1 Toque [ ] en la parte superior izquierda de la pantalla de inicio de Canon PRINT Business.

Aparecerá la pantalla [Sel. Impr.].

2 Elimine un dispositivo de la lista tocando [ ] ▶ [Eliminar].

■ Funcionamiento para Android

1 Toque [ ] en la parte superior izquierda de la pantalla de inicio de Canon PRINT Business.

Aparecerá la pantalla [Sel. impr.].

2 Mantenga pulsado el nombre del dispositivo ▶ Toque [Eliminar] en el cuadro de diálogo mostrado.

Paso 2: Registro del dispositivo en Canon PRINT Business de nuevo (para Bluetooth)

Si la opción de Bluetooth está establecida como <Sí>, siga el procedimiento siguiente.

Funcionamiento para iOS(P. 92)
Funcionamiento para Android(P. 92)

Funcionamiento para iOS

1 Toque [ ] en la parte superior izquierda de la pantalla de inicio de Canon PRINT Business.

Aparecerá la pantalla [Sel. Impr.].

2 Toque [Impresoras próximas].

Aparecerán los dispositivos detectados.

Si no se detectan dispositivos

Acérquese a la máquina y toque [Buscar]. El Bluetooth puede detectar dispositivos a una distancia de hasta 2 metros o 80 pulgadas.

3 Seleccione el dispositivo ▶ Toque [Añadir].

Funcionamiento para Android

1 Toque [ ] en la parte superior izquierda de la pantalla de inicio de Canon PRINT Business.

Aparecerá la pantalla [Sel. impr.].

2 Toque [Impresoras próximas].

Aparecerán los dispositivos detectados.

Si no se detectan dispositivos

Acérquese a la máquina y toque [Buscar]. El Bluetooth puede detectar dispositivos a una distancia de hasta 2 metros.

3 Seleccione el dispositivo.

4 Compruebe la información del dispositivo en el cuadro de diálogo mostrado ▶ Toque [Añadir].

Si aparece la pantalla de configuración de la red wifi, siga las instrucciones de la pantalla.

Procedimientos adicionales para la configuración del sistema de gestión de acceso

Procedimientos adicionales para la configuración del sistema de gestión de acceso

La clave del sistema de gestión de acceso se actualiza automáticamente tras la actualización del firmware del equipo.

La información de restricción se recupera automáticamente de nuevo unos 30 minutos después de la actualización automática de la clave. La impresión podrá realizarse normalmente con la función del sistema de gestión de acceso.

Si desea imprimir con la función del sistema de gestión de acceso del controlador de la impresora inmediatamente después de la actualización del firmware, es necesario volver a recuperar manualmente la información de restricción del sistema de gestión de acceso.

Procedimiento para el sistema de gestión de acceso(P. 95)

Si intenta imprimir sin recuperar la información de restricción de nuevo, se producirá un error.

Procedimiento para el sistema de gestión de acceso

Si desea imprimir con la función del sistema de gestión de acceso del controlador de la impresora inmediatamente después de la actualización del firmware, deberá recuperar manualmente la información de restricción del sistema de gestión de acceso.

Para ello, siga el procedimiento a continuación.

El procedimiento que se indica a continuación no es necesario aproximadamente 30 minutos después de la actualización del firmware porque la información de restricción se habrá recuperado automáticamente en ese momento.

1 Inicie sesión en el ordenador.

2 Visualice las propiedades de la impresora que se va a utilizar con el controlador de impresora que tiene activada la función de sistema de gestión de acceso.

■En Windows Vista

- Haga clic en [Inicio] ▶ [Panel de control] ▶ [Hardware y sonido] ▶ Seleccione [Impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades].

■En Windows Server 2008

- Haga clic en [Inicio] ▶ [Panel de control] ▶ [Hardware y sonido] ▶ Seleccione [Impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades].

■En Windows Server 2008 R2

- Haga clic en [Inicio] ▶ [Panel de control] ▶ [Hardware] ▶ Seleccione [Dispositivos e impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades de impresora].

■En Windows 7

- Haga clic en [Inicio] ▶ [Panel de control] ▶ [Hardware y sonido] ▶ Seleccione [Dispositivos e impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades de impresora].

■En Windows 8.1/Windows Server 2012

- Vaya al escritorio y visualice los charms en la parte derecha de la pantalla.
- Haga clic en [Configuración] ▶ [Panel de control] ▶ Seleccione [Ver dispositivos e impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades de impresora].

■En Windows 10/Windows Server 2016

- Haga clic con el botón derecho del ratón en [Inicio] ▶ Seleccione [Panel de control] ▶ [Ver dispositivos e impresoras].
- Haga clic con el botón derecho del ratón en el icono de la impresora ▶ Seleccione [Propiedades de impresora].

3 **Haga clic en la ficha [AMS].**

4 **Haga clic en [Obtener la información de restricción].**

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.