Regarding the measure against vulnerability measure of RSA Key generation

USRM3-1255-00 2022-03 en

Contents

Preface

Preface

You must update the firmware and perform additional procedures described in this document, in order to upgrade an RSA key that is created with a vulnerable encryption library.

First, check the model and version of your machine.
If you find the model and version of your machine on this page, update the firmware, then perform the additional procedures described in this document. **Checking whether You Must Perform the Additional Procedures(P. 4)**
For information on updating the firmware, see the website where you obtained this document.

Checking the Version of Your Machine

Follow the procedure below to check the version of your machine.

1 Start the Remote UI.

2 Click [Status Monitor/Cancel] on the portal page.

3 Click [Device Information] ▶ check [Main Controller] in [Version Information].

Models and Versions Requiring the Additional Procedures

Models	Versions
- iR C3222L	Ver 01.16 to Ver 02.05
- LBP631Cw - LBP632Cdw / LBP633Cdw	Ver 01.22
- MF651Cw / MF652Cw - MF653Cdw / MF654Cdw / MF655Cdw / MF656Cdw / MF657Cdw	Ver 01.22
- LBP233dw / LBP236dw / LBP237dw - LBP1238 II - 1238P II / 1238Pr II	Ver 01.22 to Ver 01.26
- 1238 II - MF1238 II - MF451dw / MF452dw / MF453dw / MF455dw	Ver 01.22 to Ver 01.26

NOTE

- The screenshots used in this document may differ from the ones you actually see, depending on the model of your machine. For details on the screenshots, see the manual for your machine on the online manual website.
  https://oip.manual.canon/

Checking whether You Must Perform the Additional Procedures

Checking whether You Must Perform the Additional Procedures

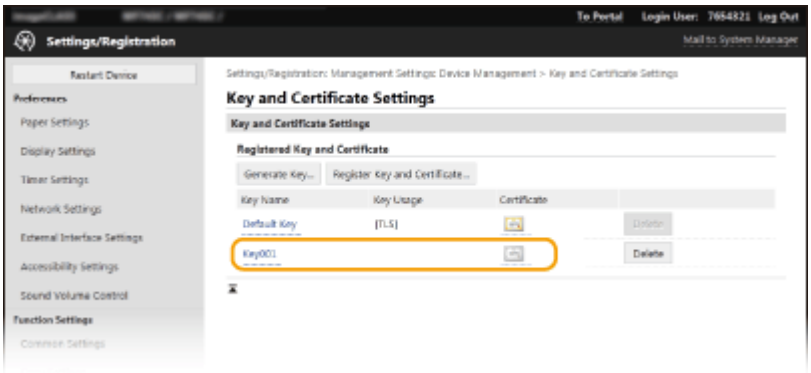
Check for an RSA key and perform the procedures required, according to the settings of your machine.
Checking for an RSA key is not required if "Default Key" appears for a key registered in your machine.

NOTE

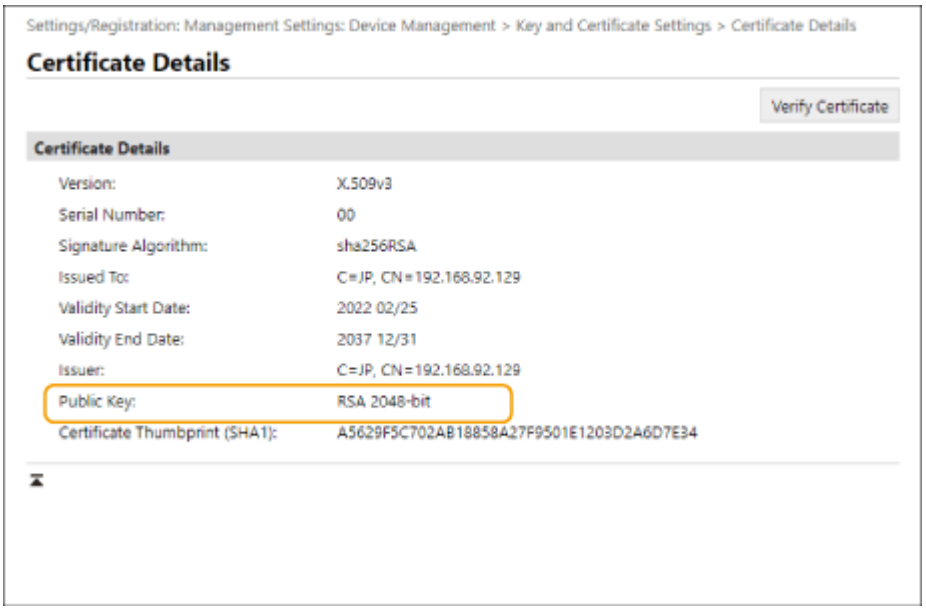
- The screenshots used in this document are only an example. They may differ from the ones you actually see, depending on the model of your machine.

1 Start the Remote UI ▶ click [Settings/Registration] ▶ [Device Management] ▶ [Key and Certificate Settings].

2 Click a key other than [Default Key].



3 Check [Public Key].



For a Certificate Other than RSA

You do not need to perform the additional procedures.

For an RSA Certificate

Click [Key and Certificate Settings] on the top of the screen ▶ check the key usage.

- Perform the additional procedures according to what appears here. **RSA Key Usage and Additional Procedure(P. 7)**
- If the key is an RSA key that has been generated externally and registered to the machine, you do not need to perform the additional procedures.
- If you must perform the additional procedures, you may need certificate information for disabling the certificate. Make a note of the required information before deleting the key/certificate. Ask the certificate authority that has issued the certificate about the required information.

RSA Key Usage and Additional Procedure

RSA Key Usage and Additional Procedure

Refer to "Additional Procedures" and perform them according to the key usage.

RSA Key Usage	Conditions	Additional Procedures
[TLS]	You must perform the additional procedures in any conditions.	**Procedure for TLS(P. 8)**
[IEEE 802.1X]	You must perform the additional procedures if the IEEE 802.1X authentication method is set to TLS.	**Procedure for IEEE 802.1X(P. 17)**
[IPSec]	You must perform the additional procedures if the IKE authentication method is set to the digital signature method.	**Procedure for IPSec(P. 28)**
[Device Signature]	You must perform the additional procedures in the following cases: • When a digital signature is added to sent files using a key for device signatures	**Procedure for Device Signatures(P. 38)**

NOTE

- The screenshots used in this document are only an example. They may differ from the ones you actually see, depending on the model of your machine.

Procedure for TLS

Step 1: Regenerating the Key and Certificate (for TLS)

You can generate two types of certificates for a key generated with the machine: a self-signed certificate and CSR certificate. The procedure differs according to the type of certificate.

For a Self-Signed Certificate(P. 9)
For a CSR Certificate(P. 10)

For a Self-Signed Certificate

1 Start the Remote UI.

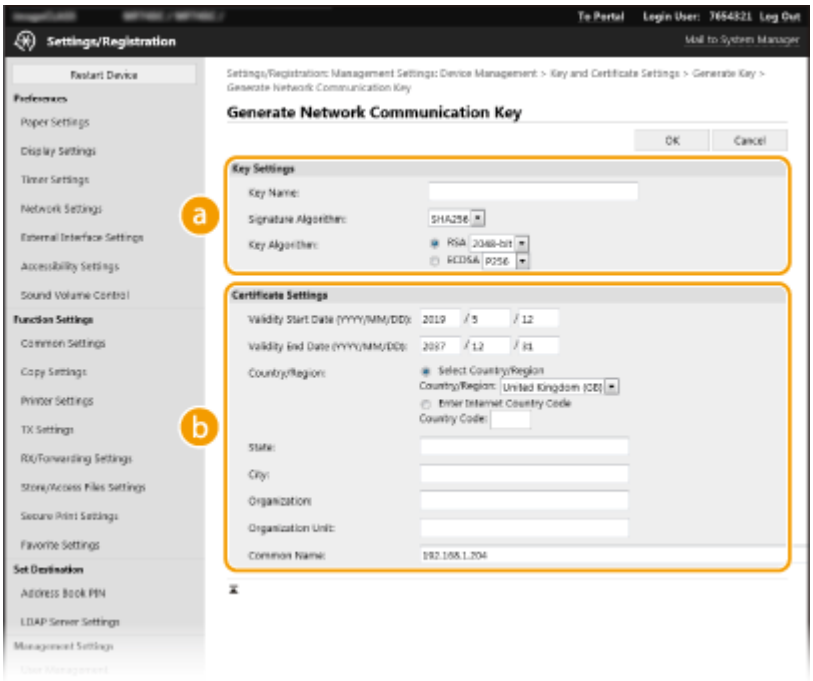
2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Generate Key].

5 Select [Network Communication] ▶ click [OK].

6 Configure the key and certificate settings.



a [Key Settings]

[Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

[Certificate Settings]

[Validity Start Date (YYYY/MM/DD)]
Enter the start date of the validity period for the certificate.

[Validity End Date (YYYY/MM/DD)]
Enter the end date of the validity period for the certificate. You cannot set a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]
Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key.

■1. Generating a Key and CSR

1 Start the Remote UI.

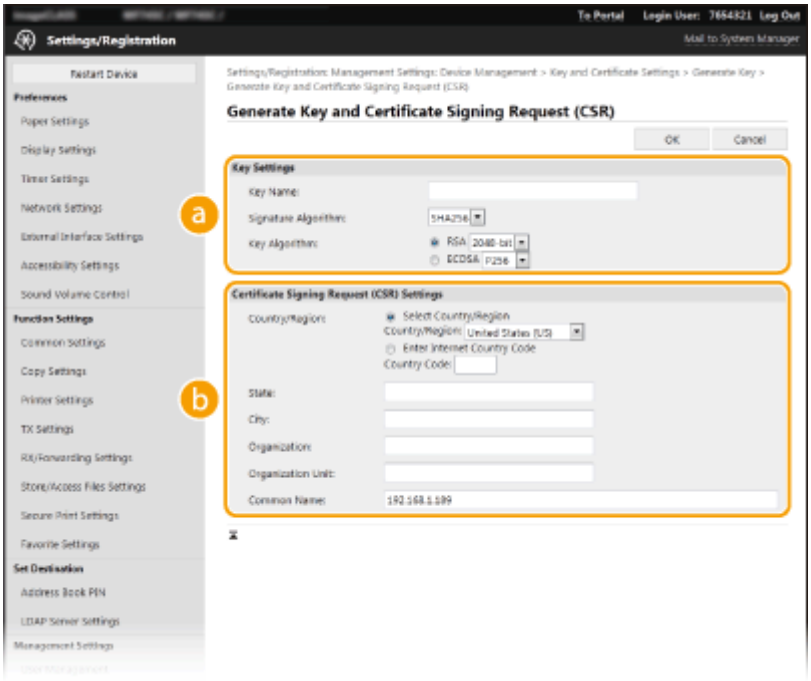
2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Generate Key].

5 Select [Key and Certificate Signing Request (CSR)] ▶ click [OK].

6 Configure the key and CSR settings.



a [Key Settings]

[Key Name]
Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

b [Certificate Signing Request (CSR) Settings]

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and CSR may take some time.

8 Click [Store in File].

- When the dialog box for saving the file appears, select the destination to save the file ▶ click [Save].

  ➠ The CSR file is saved to the computer.

9 Attach the saved file and make a request to the certificate authority.

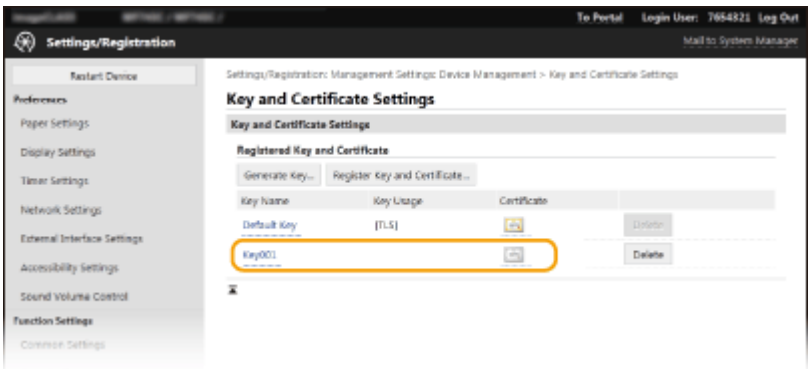
■2. Registering the Issued Certificate to the Key

1 Start the Remote UI and log in as an administrator.

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Key Name] or [Certificate] for the certificate to register.



5 Click [Register Certificate].

6 Click [Browse] ▶ specify the certificate file that you requested ▶ click [Register].

Step 2: Resetting the Key and Certificate (for TLS)

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Network] ▶ [TLS Settings].**

4 **Click [Key and Certificate].**

5 **Click [Register Default Key] on the right of the key and certificate to use.**

- If you want to use the preinstalled key and certificate, select [Default Key].

6 **Click [OK].**

7 **Restart the machine.**

➠ The machine restarts, and the settings are applied.

Step 3: Deleting a Key/Certificate Generated in the Past (for TLS)

NOTE

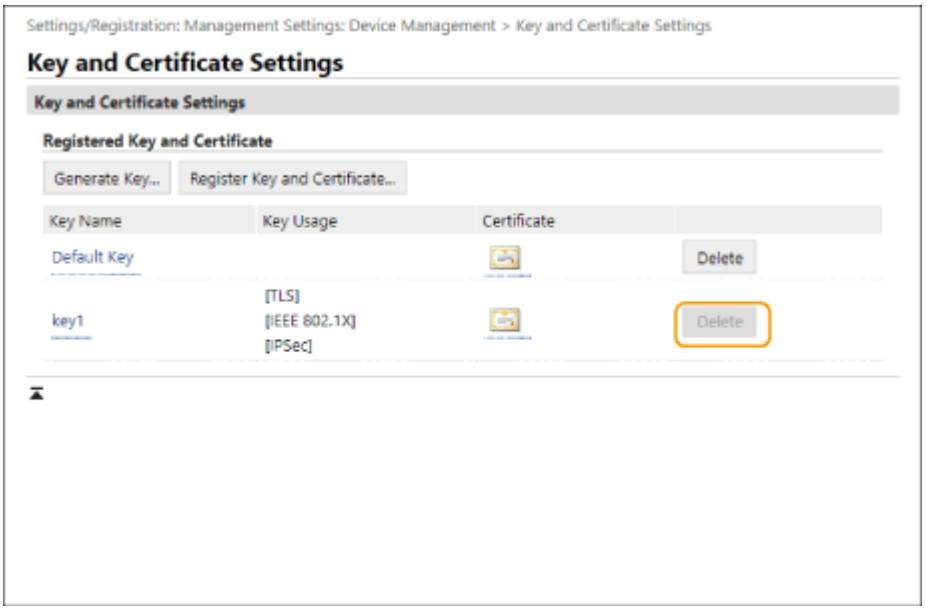
- You may need to convey information to the certificate authority when disabling the certificate. See **Checking whether You Must Perform the Additional Procedures(P. 4)** , and make a note of the required information before deleting the key/certificate.

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Select the key and certificate ▶ click [Delete] ▶ [OK].**



NOTE

- A key and certificate that is being used has its usage displayed, such as [TLS] or [IEEE 802.1X], and cannot be deleted. Delete it after disabling the corresponding function or changing to another key and certificate.

Step 4: Disabling the Certificate (for TLS)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

■ For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered in a computer or Web browser as a trusted certificate, delete the registered certificate.

■ For a CSR Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in a computer or Web browser that communicates with the machine, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 5: Enabling the New Certificate (for TLS)

Enable the certificate that is newly generated on the machine.

■ For a Self-Signed Certificate

Register the new certificate to the computer or Web browser as a trusted certificate.

■ For a CSR Certificate

You do not need to perform the additional procedures.

Procedure for IEEE 802.1X

Step 1: Checking the Authentication Method (for IEEE 802.1X)

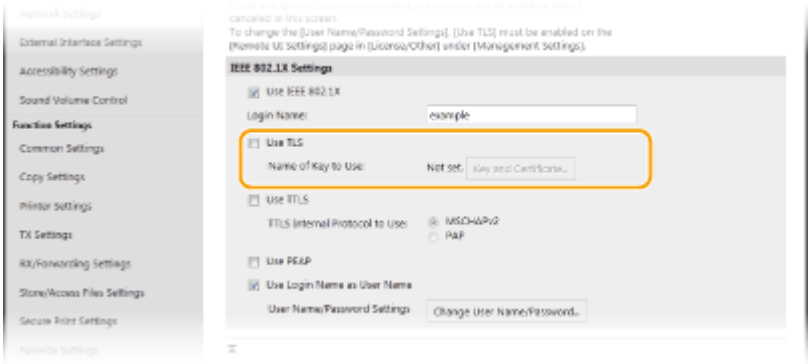
You must perform the subsequent procedures if the IEEE 802.1X authentication method is set to TLS.
Follow the procedure below to check the authentication method.

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Network] ▶ [IEEE 802.1X Settings] ▶ [Edit].**

4 **Check [Use TLS].**



- If [Use TLS] is selected and a key name appears, perform the subsequent procedures.
- If [Use TLS] is deselected, you do not need to perform the subsequent procedures.

Step 2: Regenerating the Key and Certificate (for IEEE 802.1X)

You can generate two types of certificates for a key generated with the machine: a self-signed certificate and CSR certificate. The procedure differs according to the type of certificate.

For a Self-Signed Certificate(P. 19)
For a CSR Certificate(P. 20)

For a Self-Signed Certificate

1 **Start the Remote UI.**

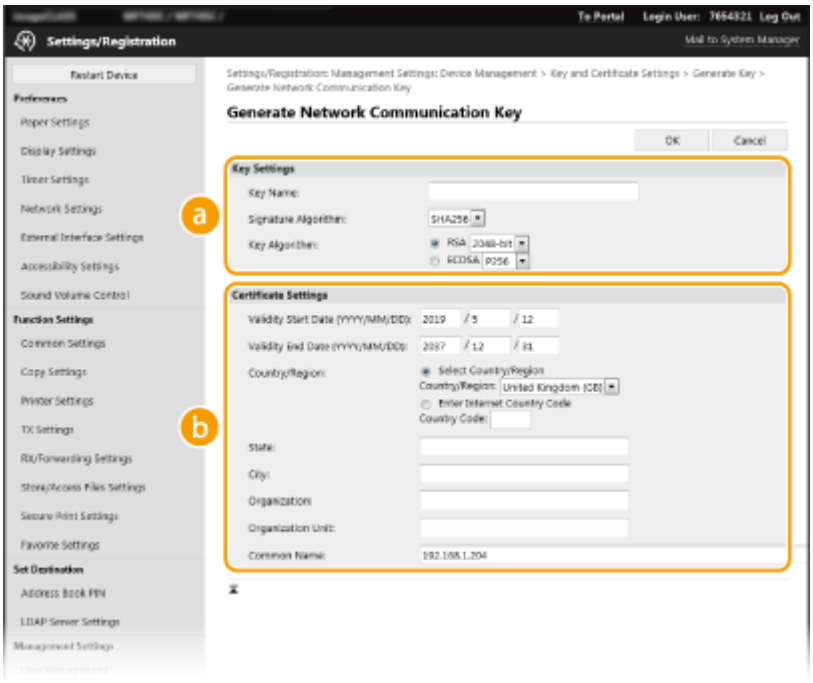
2 **Click [Settings/Registration] on the portal page.**

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Click [Generate Key].**

5 **Select [Network Communication] ▶ click [OK].**

6 **Configure the key and certificate settings.**



[Key Settings]

[Key Name]
Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

[Certificate Settings]

[Validity Start Date (YYYY/MM/DD)]
Enter the start date of the validity period for the certificate.

[Validity End Date (YYYY/MM/DD)]
Enter the end date of the validity period for the certificate. You cannot set a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]
Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key.

■1. Generating a Key and CSR

1 Start the Remote UI.

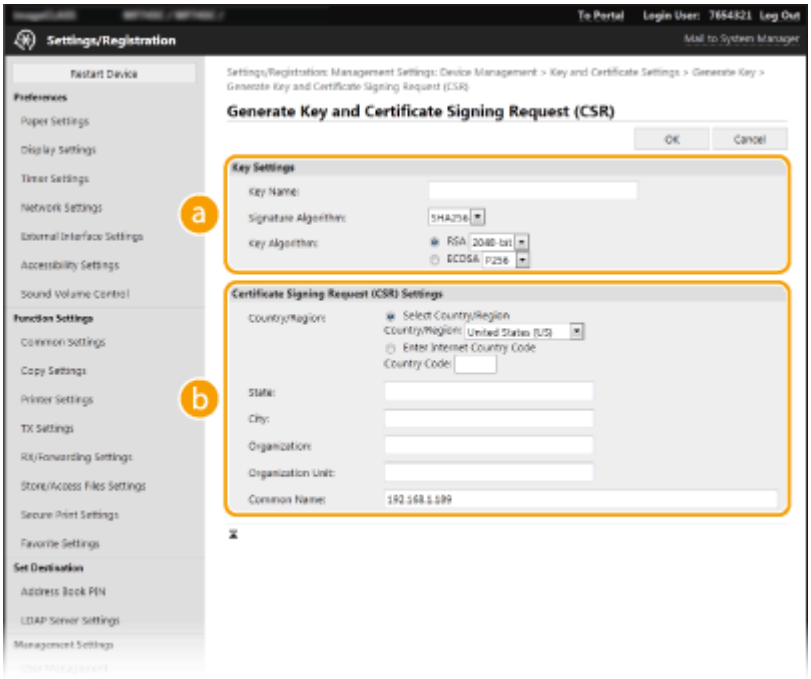
2 Click [Settings/Registration] on the portal page.

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Click [Generate Key].**

5 **Select [Key and Certificate Signing Request (CSR)] ▶ click [OK].**

6 **Configure the key and CSR settings.**



a [Key Settings]

[Key Name]
Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

b [Certificate Signing Request (CSR) Settings]

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]
Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and CSR may take some time.

8 Click [Store in File].

- When the dialog box for saving the file appears, select the destination to save the file ▶ click [Save].

  ➠ The CSR file is saved to the computer.

9 Attach the saved file and make a request to the certificate authority.

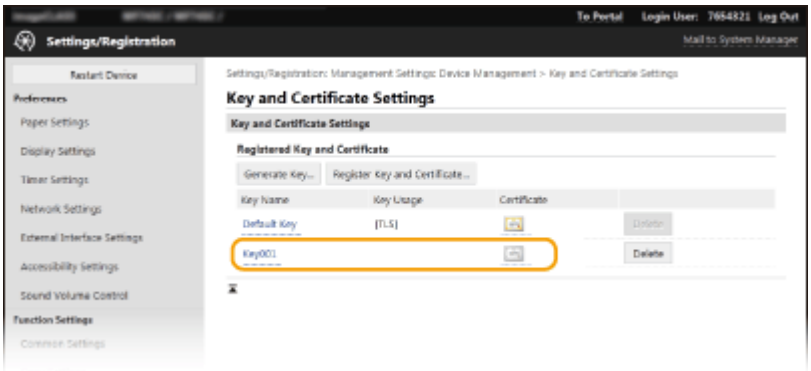
■2. Registering the Issued Certificate to the Key

1 Start the Remote UI and log in as an administrator.

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Key Name] or [Certificate] for the certificate to register.



5 Click [Register Certificate].

6 Click [Browse] ▶ specify the certificate file that you requested ▶ click [Register].

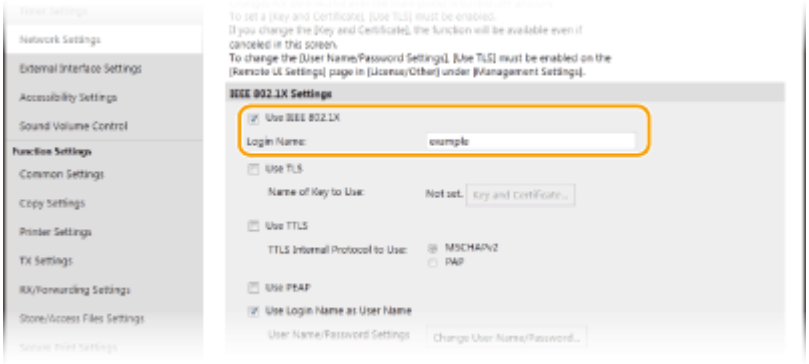
Step 3: Resetting the Key and Certificate (for IEEE 802.1X)

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Network] ▶ [IEEE 802.1X Settings] ▶ [Edit].**

4 **Select [Use IEEE 802.1X] ▶ enter the login name in [Login Name].**



[Use IEEE 802.1X]

Select this to use IEEE 802.1X authentication.

[Login Name]

Enter the name for identifying the user (EAP identity) using alphanumeric characters.

5 **Select [Use TLS] ▶ click [Key and Certificate].**

6 **Click [Register Default Key] on the right of the key and certificate to use.**

7 **Click [OK].**

8 Restart the machine.

➠ The machine restarts, and the settings are applied.

Step 4: Deleting a Key/Certificate Generated in the Past (for IEEE 802.1X)

NOTE

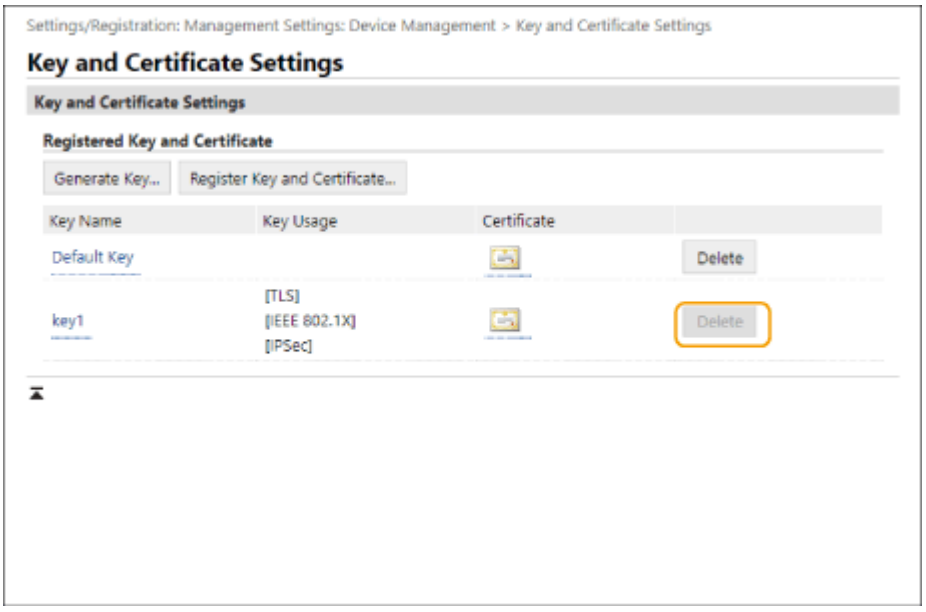
- You may need to convey information to the certificate authority when disabling the certificate. See **Checking whether You Must Perform the Additional Procedures(P. 4)** , and make a note of the required information before deleting the key/certificate.

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Select the key and certificate ▶ click [Delete] ▶ [OK].**



NOTE

- A key and certificate that is being used has its usage displayed, such as [TLS] or [IEEE 802.1X], and cannot be deleted. Delete it after disabling the corresponding function or changing to another key and certificate.

Step 5: Disabling the Certificate (for IEEE 802.1X)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

■ For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered to the IEEE 802.1X authentication server as a trusted certificate, delete the registered certificate.

■ For a CSR Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in an IEEE 802.1X authentication server, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 6: Enabling the New Certificate (for IEEE 802.1X)

Enable the certificate.

■ For a Self-Signed Certificate

Register the new certificate to the IEEE 802.1X authentication server as a trusted certificate.

■ For a CSR Certificate

You do not need to perform the additional procedures.

Procedure for IPSec

Step 1: Checking the Authentication Method (for IPSec)

You must perform the subsequent procedures if the authentication method for IKE setting in IPSec is set to [Digital Signature Method].
Follow the procedure below to check the authentication method.

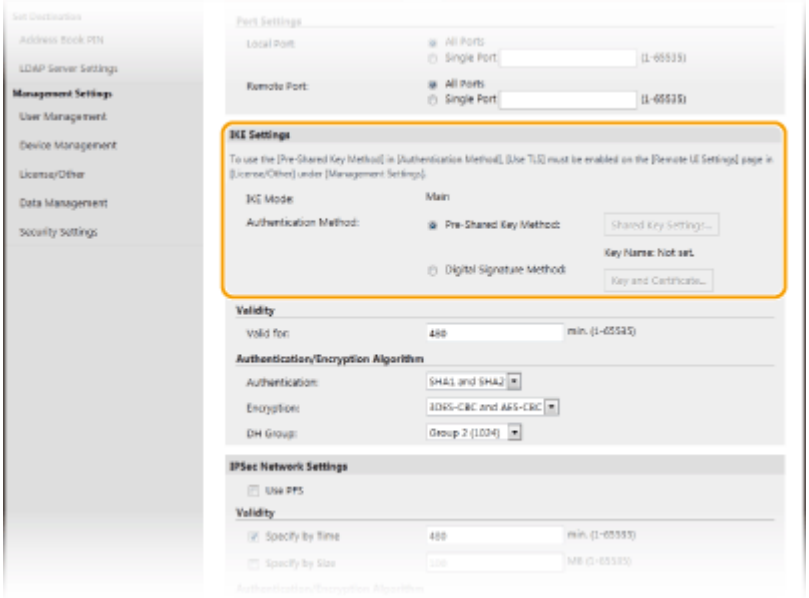
1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Network] ▶ [IPSec Settings].**

4 **Click the policy in [Registered IPSec Policies].**

5 **Check [Authentication Method] in [IKE Settings].**



- If [Authentication Method] is set to [Digital Signature Method] and a key name appears, perform the subsequent procedures.
- If [Authentication Method] is set to [Pre-Shared Key Method], you do not need to perform the subsequent procedures.

Step 2: Regenerating the Key and Certificate (for IPSec)

You can generate two types of certificates for a key generated with the machine: a self-signed certificate and CSR certificate. The procedure differs according to the type of certificate.

For a Self-Signed Certificate(P. 30)
For a CSR Certificate(P. 31)

For a Self-Signed Certificate

1 Start the Remote UI.

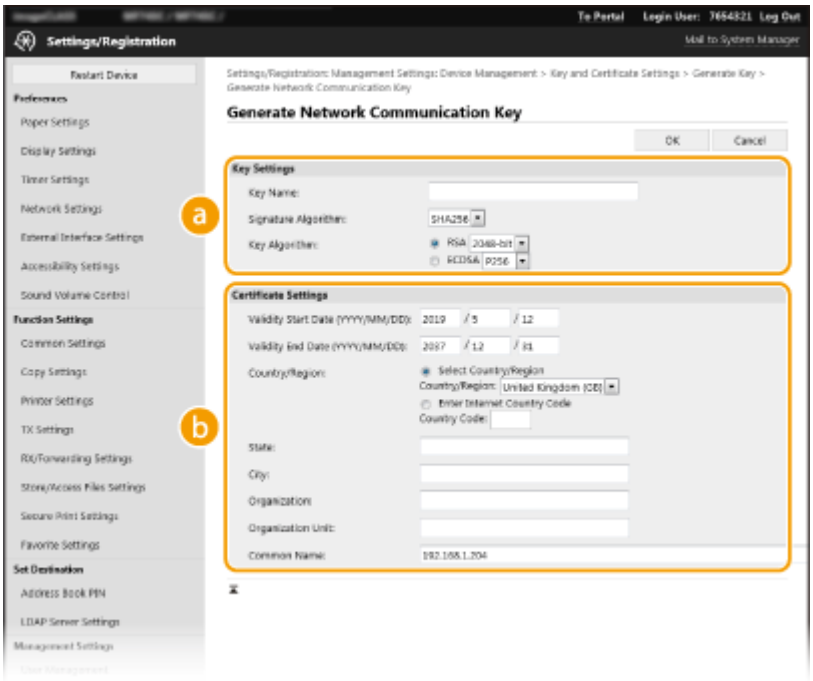
2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Generate Key].

5 Select [Network Communication] ▶ click [OK].

6 Configure the key and certificate settings.



a [Key Settings]

[Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

[Certificate Settings]

[Validity Start Date (YYYY/MM/DD)]
Enter the start date of the validity period for the certificate.

[Validity End Date (YYYY/MM/DD)]
Enter the end date of the validity period for the certificate. You cannot set a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]
Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key.

■1. Generating a Key and CSR

1 Start the Remote UI.

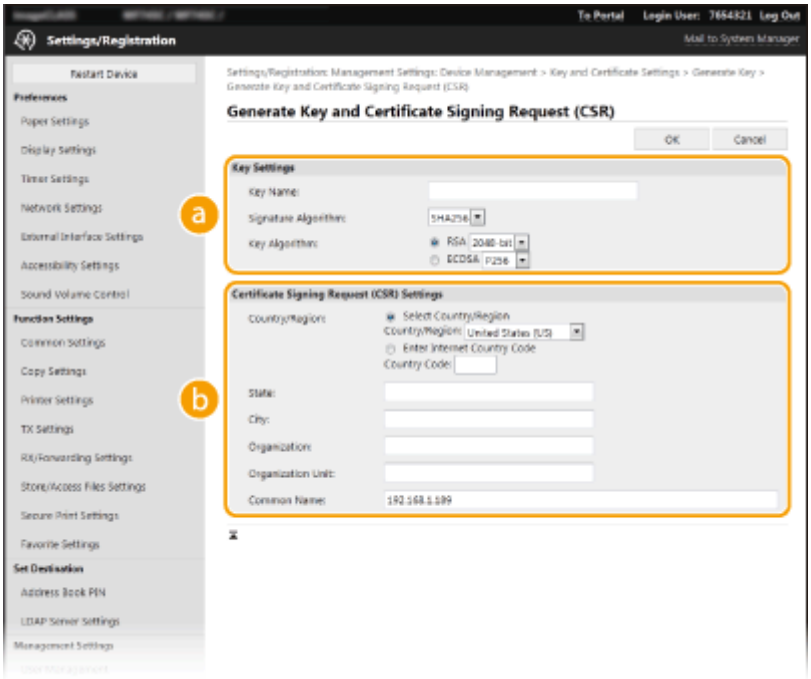
2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Generate Key].

5 Select [Key and Certificate Signing Request (CSR)] ▶ click [OK].

6 Configure the key and CSR settings.



a [Key Settings]

[Key Name]
Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

[Signature Algorithm]
Select the key algorithm from the drop-down list.

[Key Algorithm]
Select [RSA] or [ECDSA] as the key generation algorithm ▶ select the key length from the drop-down list. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

- If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

b [Certificate Signing Request (CSR) Settings]

[Country/Region]
Click [Select Country/Region] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[State]/[City]
Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]
Enter the organization name using alphanumeric characters as necessary.

[Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and CSR may take some time.

8 Click [Store in File].

- When the dialog box for saving the file appears, select the destination to save the file ▶ click [Save].

  ➠ The CSR file is saved to the computer.

9 Attach the saved file and make a request to the certificate authority.

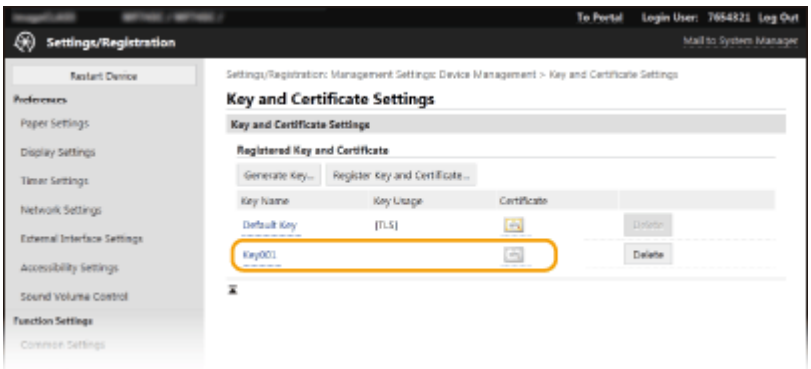
■2. Registering the Issued Certificate to the Key

1 Start the Remote UI and log in as an administrator.

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] ▶ [Key and Certificate Settings].

4 Click [Key Name] or [Certificate] for the certificate to register.



5 Click [Register Certificate].

6 Click [Browse] ▶ specify the certificate file that you requested ▶ click [Register].

Step 3: Resetting the Key and Certificate (for IPSec)

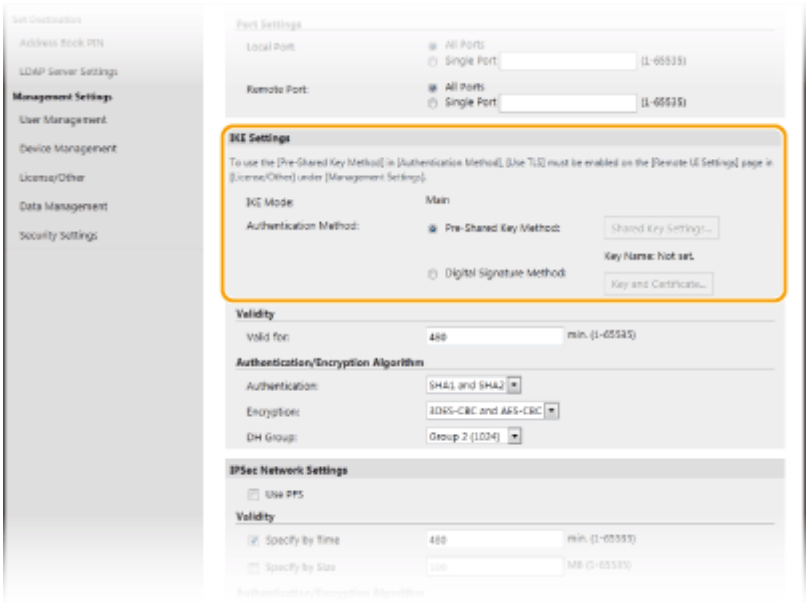
1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Network] ▶ [IPSec Settings].**

4 **Click the policy to reset the key and certificate for in [Registered IPSec Policies].**

5 **Configure [IKE Settings].**



6 **Select [Digital Signature Method] in [Authentication Method] ▶ click [Key and Certificate].**

7 **Click [Register Default Key] on the right of the key and certificate to use.**

8 **Click [OK].**

9 **Restart the machine.**

➠ The machine restarts, and the settings are applied.

Step 4: Deleting a Key/Certificate Generated in the Past (for IPSec)

NOTE

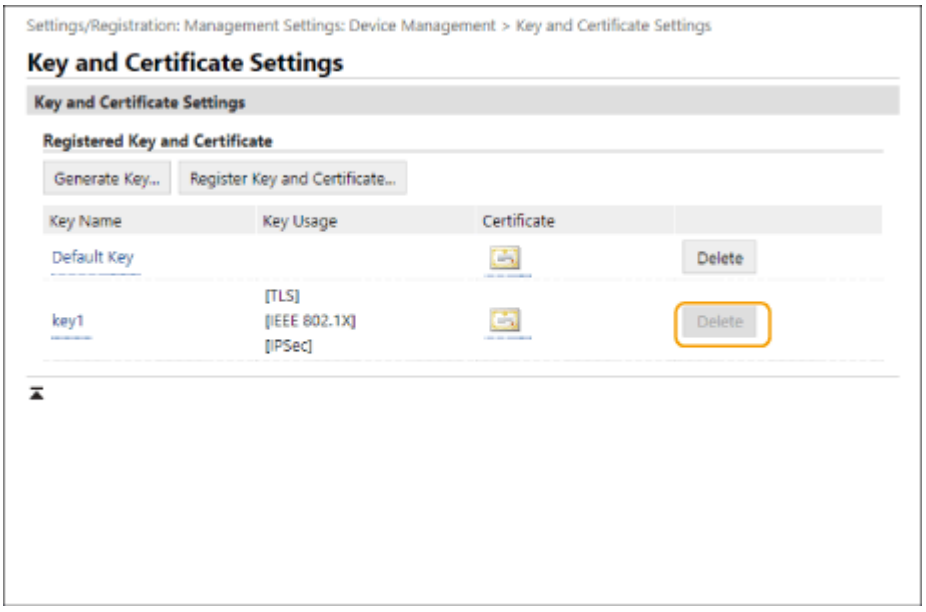
- You may need to convey information to the certificate authority when disabling the certificate. See **Checking whether You Must Perform the Additional Procedures(P. 4)** , and make a note of the required information before deleting the key/certificate.

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Select the key and certificate ▶ click [Delete] ▶ [OK].**



NOTE

- A key and certificate that is being used has its usage displayed, such as [TLS] or [IEEE 802.1X], and cannot be deleted. Delete it after disabling the corresponding function or changing to another key and certificate.

Step 5: Disabling the Certificate (for IPSec)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

■ For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered in the device that communicates with IPSec as a trusted certificate, delete the registered certificate. After deleting the registered certificate, register the certificate of the regenerated key.

■ For a CSR Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in the device that communicates with IPSec, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 6: Enabling the New Certificate (for IPSec)

Enable the certificate.

■ For a Self-Signed Certificate

Register the new certificate to the device that communicates with IPSec as a trusted certificate.

■ For a CSR Certificate

You do not need to perform the additional procedures.

Procedure for Device Signatures

Step 1: Regenerating the Key and Certificate (for Device Signatures)

1 **Start the Remote UI.**

2 **Click [Settings/Registration] on the portal page.**

3 **Click [Device Management] ▶ [Key and Certificate Settings].**

4 **Click [Update] on the right of the key and certificate for device signatures.**

5 **Click [OK].**

Step 2: Disabling the Certificate (for Device Signatures)

Disable a certificate generated in the past.

■If a Certificate for Device Signatures Is Registered to Acrobat

If a certificate for device signatures is registered in Acrobat, delete the registered certificate.

Step 3: Enabling the New Certificate (for Device Signatures)

Enable the certificate.

■ If a Certificate for Device Signatures Is Registered to Acrobat

If the certificate for device signatures is registered in Acrobat, register the certificate in a PDF file sent from the machine with a device signature attached to Acrobat.

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.