Erforderliche Maßnahmen im Hinblick auf Sicherheitsrisiken bei Generierung von RSA-Schlüsseln

USRM3-1249-02 2022-07 de

Inhalt

Vorwort

Vorwort

Sie müssen die Firmware aktualisieren und weitere in diesem Dokument beschriebene Verfahren durchführen, um einen RSA-Schlüssel zu aktualisieren, der mit einer anfälligen Verschlüsselungsbibliothek erstellt wurde.

Überprüfen Sie zunächst das Modell und die Version Ihres Geräts.
Wenn Sie das Modell und die Version Ihres Geräts auf dieser Seite finden, aktualisieren Sie die Firmware, und führen Sie dann die weiteren in diesem Dokument beschriebenen Verfahren aus. **Prüfen, ob Sie weitere Verfahren durchführen müssen(P. 5)**
Informationen zum Aktualisieren der Firmware finden Sie auf der Website, von der Sie dieses Dokument bezogen haben.

Überprüfen der Version Ihres Geräts

Befolgen Sie den nachstehenden Ablauf, um die Version Ihres Geräts zu überprüfen.

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Status Monitor/Abbruch].

3 Klicken Sie auf [Geräte-Informationen] ▶ überprüfen Sie [Controller] unter [Informationen über die Version].

Modelle und Versionen, die weitere Verfahren erfordern

Modelle	Versionen
- 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 bis 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 bis Ver. 37.30
- iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B	Ver. 17.44 bis Ver. 27.30

Modelle	Versionen
- iR-ADV C3730 / C3720 - iR-ADV C7780 / C7770 / C7765	
- iR-ADV C357 - iR-ADV C477	Ver. 19.34 bis Ver. 27.30
- iR-ADV C5760 / C5750 / C5740 / C5735	Ver. 19.40 bis Ver. 27.30
- iR-ADV 6765 / 6780	Ver. 17.44 bis Ver. 27.33
- iR-ADV C5870 / C5860 / C5850 / C5840	Ver. 03.11 bis Ver. 17.32
- iR-ADV 6860 / 6870	Ver. 05.25 bis Ver. 17.32
- iR-ADV C3830 / C3826 / C3835	Ver. 06.28 bis Ver. 17.32
- iR-ADV C568	Ver. 04.13 bis Ver. 17.08
- iR C3226 / C3222	Ver. 01.12 bis Ver. 02.13
- MF830Cx / MF832Cx / MF832Cdw - iR C1533 / C1538	Ver. 200.0.301 bis Ver. 309.0.405
- LBP720Cx / LBP722Cx / LBP722Ci / LBP722Cdw - C1533P / C1538P	Ver. 114.0.301 bis Ver. 309.0.405
- iR2425	Ver. 02.06 bis Ver. 05.00
- iR2635 / iR2645 / iR2630 / iR2625	Ver. 130.0.117 bis Ver. 600.0.601

HINWEIS

- Die in diesem Dokument verwendeten Bildschirmabbildungen können je nach Modell Ihres Geräts von denen abweichen, die Sie tatsächlich sehen. Näheres zu den Bildschirmabbildungen finden Sie im Handbuch für Ihr Gerät auf der Website mit den Online-Handbüchern.

  https://oip.manual.canon/

Prüfen, ob Sie weitere Verfahren durchführen müssen

Prüfen, ob Sie weitere Verfahren durchführen müssen

Führen Sie folgende drei Vorgänge aus, um zu prüfen, welche zusätzliche Verfahren Sie durchführen müssen.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. In diesem Fall führen Sie die Vorgänge über die Remote UI aus.

Überprüfen des RSA-Schlüssels(P. 5)
Überprüfen der Bluetooth-Einstellungen(P. 8)
Überprüfen der Einstellungen des Zugangsverwaltungssystems(P. 9)
Die Prüfung auf einen RSA-Schlüssel ist nicht erforderlich, wenn "Standardschlüssel" oder "AMS" für einen in Ihrem Gerät registrierten Schlüssel angezeigt wird. Überprüfen Sie die Bluetooth-Einstellungen und die Einstellungen für das Zugangsverwaltungssystem, und führen Sie bei Bedarf die zusätzlichen Verfahren durch.

HINWEIS

- Die in diesem Dokument verwendeten Bildschirmabbildungen sind lediglich Beispiele. Je nach Modell Ihres Geräts können sie von den tatsächlich gezeigten abweichen.

Überprüfen des RSA-Schlüssels

Überprüfen Sie, ob ein RSA-Schlüssel vorhanden ist. Wenn es einen RSA-Schlüssel gibt, der mit dem Gerät generiert wurde, prüfen Sie die Verwendung des Schlüssels.

Verwenden des Bedienfelds(P. 5)
Verwenden von Remote UI(P. 7)

■ Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Liste Schlüssel und Zertifikat>.

3 Drücken Sie <Schlüsselu. Zertifikatsliste für d.Gerät>.

- <Schlüsselu. Zertifikatsliste für d.Gerät> wird nur angezeigt, wenn die Benutzersignaturfunktion auf dem Gerät aktiviert ist. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

4 Wählen Sie einen anderen Schlüssel als <Default Key> und <AMS> aus, bei dem als <Status> die Option <Verwendet> angezeigt wird ▶ drücken Sie <Zertifikat details>.
Beispielbildschirm:

5 Prüfen Sie <Öffentlicher Schlüssel>.

Beispielbildschirm:

Für ein anderes Zertifikat als RSA

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen. Drücken Sie <OK>, um den Bildschirm zu schließen.

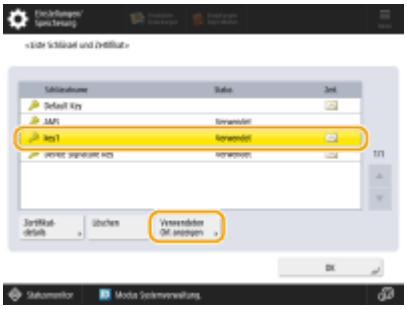
Für ein RSA-Zertifikat

Fahren Sie mit Schritt 6 fort.

- Sie brauchen die zusätzlichen Verfahren für die folgenden Schlüssel nicht durchzuführen. Drücken Sie <OK>, um den Bildschirm zu schließen.
  - Ein RSA-Schlüssel, der extern generiert und auf dem Gerät registriert wurde
- Wenn Sie die zusätzlichen Verfahren durchführen müssen, benötigen Sie möglicherweise Zertifikatsinformationen zum Deaktivieren des Zertifikats. Notieren Sie sich die erforderlichen Informationen vor dem Löschen des Schlüssels/Zertifikats. Erkundigen Sie sich bei der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, nach den erforderlichen Informationen.

6 Drücken Sie <Verwendeten Ort anzeigen> ▶ überprüfen Sie die Verwendung des Schlüssels.

Beispielbildschirm:



Führen Sie die zusätzlichen Verfahren gemäß den folgenden Angaben durch. **Verwenden von RSA-Schlüsseln und zusätzliche Verfahren(P. 12)**

■Verwenden von Remote UI

1 Starten Sie Remote UI ▶ klicken Sie auf [Einstellungen/Speicherung] ▶ [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

2 Klicken Sie auf einen anderen Schlüssel als [Default Key] und [AMS].

3 Überprüfen Sie [Öffentlicher Schlüssel].

Für ein anderes Zertifikat als RSA

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen.

Für ein RSA-Zertifikat

Klicken Sie oben auf dem Bildschirm auf [Einstellungen Schlüssel und Zertifikat] ▶ überprüfen Sie die Verwendung des Schlüssels.

- Führen Sie die zusätzlichen Verfahren gemäß den folgenden Angaben durch. **Verwenden von RSA-Schlüsseln und zusätzliche Verfahren(P. 12)**
- Sie brauchen die zusätzlichen Verfahren für die folgenden Schlüssel nicht durchzuführen.
  - Ein RSA-Schlüssel, der extern generiert und auf dem Gerät registriert wurde

- Wenn Sie die zusätzlichen Verfahren durchführen müssen, benötigen Sie möglicherweise Zertifikatsinformationen zum Deaktivieren des Zertifikats. Notieren Sie sich die erforderlichen Informationen vor dem Löschen des Schlüssels/Zertifikats. Erkundigen Sie sich bei der Zertifizierungsstelle, die das Zertifikat ausgestellt hat, nach den erforderlichen Informationen.

Überprüfen der Bluetooth-Einstellungen

Überprüfen Sie, ob Bluetooth auf <Ein> gesetzt ist. Wenn es auf <Ein> gesetzt ist, müssen Sie die zusätzlichen Verfahren durchführen.

Verwenden des Bedienfelds(P. 8)
Verwenden von Remote UI(P. 8)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen Bluetooth>.

3 Prüfen Sie <Bluetooth verwenden>.

- Wenn <Bluetooth verwenden> auf <Ein> gesetzt ist, führen Sie die folgenden Schritte aus. **Zusätzliche Verfahren für Bluetooth-Einstellungen(P. 89)**
- Wenn <Bluetooth verwenden> auf <Aus> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Netzwerk] ▶ [Einstellungen Bluetooth].

4 Überprüfen Sie [Bluetooth verwenden].

- Wenn [Bluetooth verwenden] ausgewählt ist, führen Sie die folgenden Schritte aus. **Zusätzliche Verfahren für Bluetooth-Einstellungen(P. 89)**
- Wenn [Bluetooth verwenden] abgewählt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

Überprüfen der Einstellungen des Zugangsverwaltungssystems

Überprüfen Sie, ob das Zugangsverwaltungssystem auf <Ein> gesetzt ist. Wenn es auf <Ein> gesetzt ist, müssen Sie die zusätzlichen Verfahren durchführen.

Je nach Gerät wird diese Einstellung möglicherweise nicht angezeigt. In diesem Fall brauchen Sie die zusätzlichen Verfahren nicht durchzuführen.

Verwenden des Bedienfelds(P. 9)
Verwenden von Remote UI(P. 9)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Verwaltung> ▶ <Lizenz/Andere> ▶ <ACCESS MANAGEMENT SYSTEM verwenden>.

3 Prüfen Sie <ACCESS MANAGEMENT SYSTEM verwenden>.

- Wenn <ACCESS MANAGEMENT SYSTEM verwenden> auf <Ein> gesetzt ist, führen Sie die folgenden Schritte aus. **Zusätzliche Verfahren für die Einstellungen des Zugangsverwaltungssystems(P. 94)**
- Wenn <ACCESS MANAGEMENT SYSTEM verwenden> auf <Aus> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Lizenz/Andere] ▶ [Einstellungen ACCESS MANAGEMENT SYSTEM].

4 Überprüfen Sie [ACCESS MANAGEMENT SYSTEM verwenden].

- Wenn [ACCESS MANAGEMENT SYSTEM verwenden] ausgewählt ist, führen Sie die folgenden Schritte aus. **Zusätzliche Verfahren für die Einstellungen des Zugangsverwaltungssystems(P. 94)**
- Wenn [ACCESS MANAGEMENT SYSTEM verwenden] abgewählt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

Verwenden von RSA-Schlüsseln und zusätzliche Verfahren

Verwenden von RSA-Schlüsseln und zusätzliche Verfahren

Lesen Sie den Abschnitt "Zusätzliche Verfahren" und führen Sie diese entsprechend der Verwendung des Schlüssels aus.

Verwenden von RSA-Schlüsseln	Bedingungen	Zusätzliche Verfahren
TLS	Sie müssen die zusätzlichen Verfahren unter allen Bedingungen durchführen.	**Verfahren für TLS(P. 13)**
IEEE 802.1X	Sie müssen die zusätzlichen Verfahren durchführen, wenn die IEEE 802.1X-Authentifizierungsmethode auf EAP-TLS eingestellt ist.	**Verfahren für IEEE 802.1X(P. 28)**
IPSec	Sie müssen die zusätzlichen Verfahren durchführen, wenn die IKE-Authentifizierungsmethode auf die digitale Signaturmethode eingestellt ist.	**Verfahren für IPSec(P. 46)**
SIP	Sie müssen die zusätzlichen Verfahren durchführen, wenn TLS verwendet wird.	**Verfahren für SIP(P. 64)**
Gerätesignatur	Sie müssen die zusätzlichen Verfahren in den folgenden Fällen durchführen: • Wenn den gesendeten Dateien eine digitale Signatur mit einem Schlüssel für Gerätesignaturen hinzugefügt wird • Wenn die Verschlüsselung in den S/MIME-Verschlüsselungseinstellungen aktiviert ist	**Verfahren für Gerätesignaturen(P. 81)**

HINWEIS

- Die in diesem Dokument verwendeten Bildschirmabbildungen sind lediglich Beispiele. Je nach Modell Ihres Geräts können sie von den tatsächlich gezeigten abweichen.

Verfahren für TLS

Schritt 1: Neugenerieren des Schlüssels und des Zertifikats (für TLS)

Sie können drei Typen von Zertifikaten für einen mit dem Gerät generierten Schlüssel erzeugen: ein selbstsigniertes Zertifikat, ein CSR-Zertifikat und ein SCEP-Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. In diesem Fall führen Sie die Vorgänge über die Remote UI aus.

Für ein selbstsigniertes Zertifikat(P. 14)
Für ein CSR-Zertifikat(P. 17)
Für ein SCEP-Zertifikat(P. 19)

Für ein selbstsigniertes Zertifikat

Verwenden des Bedienfelds(P. 14)
Verwenden von Remote UI(P. 15)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Schlüssel generieren> ▶ <Netzwerk Kommunikationsschl. generieren>.**

3 **Konfigurieren Sie die erforderlichen Einstellungen, und fahren Sie mit dem nächsten Bildschirm fort.**
Beispielbildschirm:

a <Schlüsselname>

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b <Algorithmus Signatur>

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt. Wenn Sie <RSA> für c wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für d setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

c <Schlüsselalgorithmus>

Wählen Sie den Schlüsselalgorithmus. Wenn Sie <RSA> wählen, erscheint <Schlüssellänge (Bit)> als Einstelloption für d. Wenn Sie <ECDSA> wählen, wird stattdessen <Schlüsseltyp> angezeigt.

d <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für c wählen, oder legen Sie den Schlüsseltyp fest, wenn Sie <ECDSA> wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

4 Konfigurieren Sie die erforderlichen Elemente für das Zertifikat ▸ drücken Sie <Schlüssel gener.>.

Beispielbildschirm:

a <Startdatum Gültigkeit>/<Enddatum Gültigkeit>

Geben Sie das Startdatum und das Enddatum des Gültigkeitszeitraums für das Zertifikat ein.

b <Land/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

Wählen Sie die Landeskennzahl aus der Liste, und geben Sie den Standort und den Namen des Unternehmens an.

c <Allgemeiner Name>

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

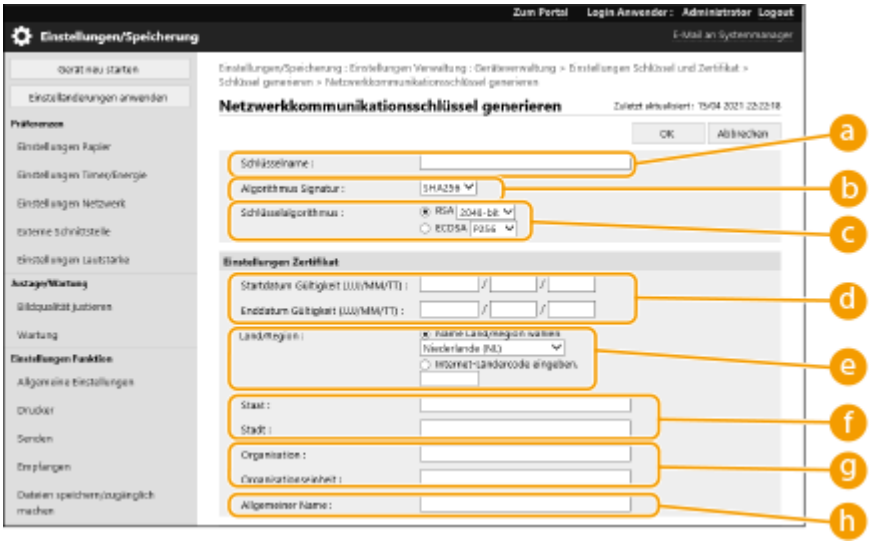
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▸ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Netzwerkkommunikation].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a [Schlüsselname]

Geben Sie einen Namen für den Schlüssel in alphanumerischen Zeichen ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt.

c [Schlüsselalgorithmus]

Wählen Sie [RSA] oder [ECDSA] als Algorithmus zur Generierung des Schlüssels. Geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

HINWEIS:

- Wenn Sie [SHA384] oder [SHA512] für [Algorithmus Signatur] wählen, können Sie die Schlüssellänge nicht auf [512-bit] einstellen, wenn Sie [RSA] für [Schlüsselalgorithmus] wählen.

d [Startdatum Gültigkeit (JJJJ/MM/TT)]/[Enddatum Gültigkeit (JJJJ/MM/TT)]

Geben Sie das Startdatum und Enddatum des Gültigkeitszeitraums für das Zertifikat ein. [Enddatum Gültigkeit (JJJJ/MM/TT)] kann nicht auf ein Datum vor dem Datum in [Startdatum Gültigkeit (JJJJ/MM/TT)] festgelegt werden.

e [Land/Region]

Klicken Sie auf [Name Land/Region wählen], und wählen Sie das Land/die Region aus der Dropdown-Liste. Alternativ können Sie auch auf [Internet-Ländercode eingeben.] klicken und einen Ländercode eingeben, wie beispielsweise "US" für die Vereinigten Staaten.

f [Staat]/[Stadt]

Geben Sie den Standort in alphanumerischen Zeichen ein, sofern erforderlich.

g [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation in alphanumerischen Zeichen ein, sofern erforderlich.

h [Allgemeiner Name]

Geben Sie gegebenenfalls den allgemeinen Namen (Common Name) des Zertifikats ein, und verwenden Sie dabei alphanumerische Zeichen. Der "Common Name" wird häufig mit "CN" abgekürzt.

7 Klicken Sie auf [OK].

- Die Erzeugung eines Schlüssels und eines Zertifikats kann einige Zeit dauern.
- Generierte Schlüssel und Zertifikate werden automatisch auf dem Gerät registriert.

Für ein CSR-Zertifikat

Generieren Sie einen Schlüssel und eine Zertifizierungsanforderung (CSR) auf dem Gerät. Verwenden Sie die auf dem Bildschirm angezeigten oder in eine Datei ausgegebenen CSR-Daten, um die Zertifizierungsstelle zur Ausstellung eines Zertifikats aufzufordern. Registrieren Sie dann das ausgestellte Zertifikat für den Schlüssel.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

■1. Generieren eines Schlüssels und einer CSR

1 Starten Sie die Remote UI.

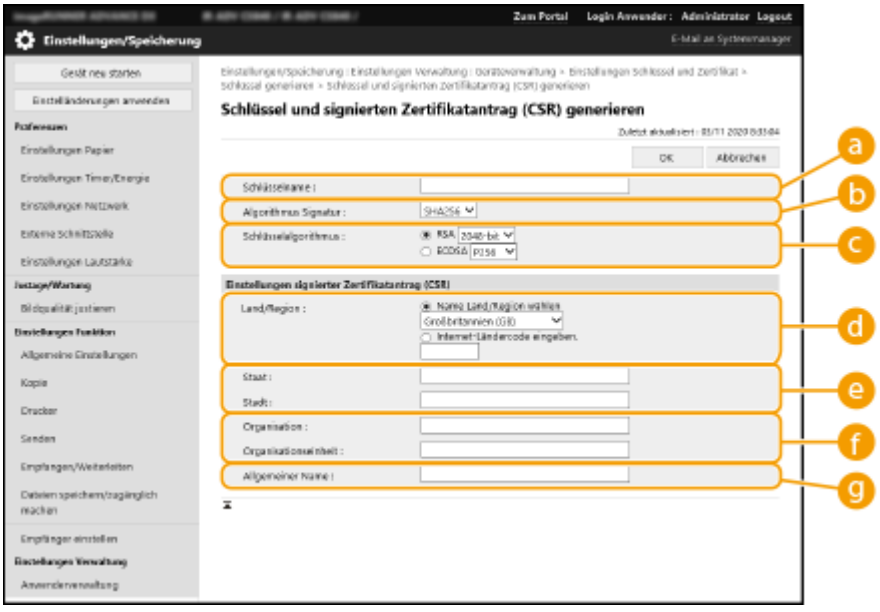
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Schlüssel und signierter Zertifikatantrag (CSR)].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a **[Schlüsselname]**

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

c [Schlüsselalgorithmus]

Wählen Sie den Schlüsselalgorithmus aus, und geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen.

d [Land/Region]

Wählen Sie den Ländercode aus der Liste, oder geben Sie ihn direkt ein.

e [Staat]/[Stadt]

Geben Sie den Standort ein.

f [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation ein.

g [Allgemeiner Name]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

7 Klicken Sie auf [OK].

➠ Die CSR-Daten werden angezeigt.

- Wenn Sie die CSR-Daten in einer Datei speichern möchten, klicken Sie auf [In Datei speichern], und legen Sie den Speicherort fest.

HINWEIS:

- Der Schlüssel, der die CSR generiert hat, wird auf dem Schlüssel- und- Zertifikatlistenbildschirm angezeigt, jedoch können Sie den Schlüssel selbst nicht verwenden. Um diesen Schlüssel zu verwenden, müssen Sie das Zertifikat registrieren, das später auf der Grundlage der CSR ausgestellt wird.

8 Fordern Sie die Zertifizierungsstelle auf, ein Zertifikat auf der Grundlage der CSR-Daten auszustellen.

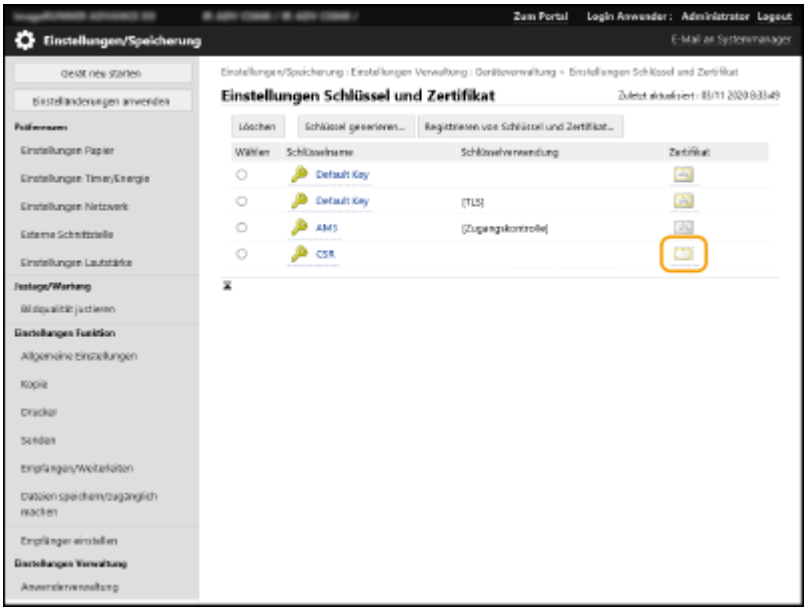
■2. Registrieren des ausgestellten Zertifikats für den Schlüssel

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie in der Liste [Zertifikat] auf für das Zertifikat, das Sie registrieren möchten.



5 Klicken Sie auf [Zertifikat speichern...].

6 Registrieren Sie das Zertifikat.

- Klicken Sie auf [Durchsuchen...] ▶ geben Sie die zu registrierende Datei (Zertifikat) an ▶ klicken Sie auf [Speichern].

Für ein SCEP-Zertifikat

Fordern Sie den SCEP-Server manuell zur Ausstellung eines Zertifikats auf.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

HINWEIS

- Sie können keine manuelle Anforderung zur Ausstellung eines Zertifikats senden, wenn [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ausgewählt ist. Deaktivieren Sie diese Option, wenn sie ausgewählt ist.

Starten Sie die Remote UI ▶ klicken Sie auf [Einstellungen/Speicherung] ▶ [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)] ▶ [Einstellungen für automatische Anforderung der Zertifikatsausstellung] ▶ deaktivieren Sie [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ▶ klicken Sie auf [Update].

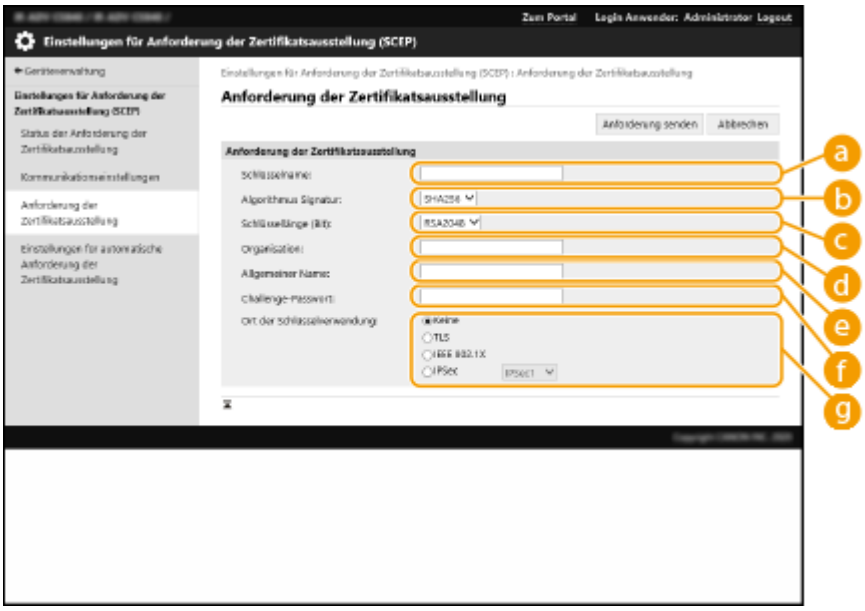
1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)].**

4 **Klicken Sie auf [Anforderung der Zertifikatsausstellung].**

5 **Konfigurieren Sie die erforderlichen Einstellungen für die Anforderung eines Zertifikats.**



a [Schlüsselname:]

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur:]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

c [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

d [Organisation:]

Geben Sie den Namen der Organisation ein.

e [Allgemeiner Name:]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

f [Challenge-Passwort:]

Ist auf der Seite des SCEP-Servers ein Passwort vorgeschrieben, geben Sie das abzufragende Passwort, das in den Anforderungsdaten (PKCS#9) enthalten ist, ein, um die Ausstellung eines Zertifikats anzufordern.

g [Ort der Schlüsselverwendung:]

Wählen Sie [TLS].

HINWEIS:

- Wenn Sie etwas anderes als [Keine] auswählen, aktivieren Sie jede Funktion im Voraus. Wenn ein Zertifikat bei jeweils deaktivierter Funktion erfolgreich bezogen wird, wird das Zertifikat dem Standort der Schlüsselnutzung zugewiesen, jedoch wird nicht jede Funktion automatisch aktiviert.

6 **Klicken Sie auf [Anforderung senden].**

7 **Klicken Sie auf [Neustart].**

Schritt 2: Zurücksetzen des Schlüssels und des Zertifikats (für TLS)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.
Dieses Verfahren ist für ein SCEP-Zertifikat nicht erforderlich.

Für ein selbstsigniertes Zertifikat/CSR-Zertifikat

Verwenden des Bedienfelds(P. 22)
Verwenden von Remote UI(P. 23)

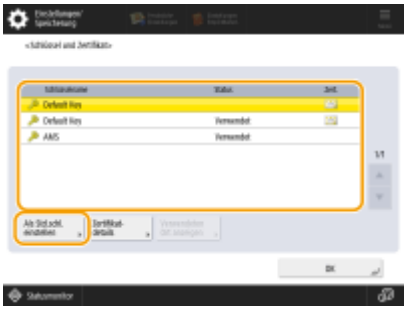
■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen TLS>.**

3 **Drücken Sie <Schlüssel und Zertifikat>.**

4 **Wählen Sie den Schlüssel und das Zertifikat für die TLS-verschlüsselte Kommunikation aus ▶ drücken Sie <Als Std.schl. einstellen> ▶ <Ja>.**
Beispielbildschirm:



- Wenn Sie den vorinstallierten Schlüssel und das Zertifikat verwenden möchten, wählen Sie <Default Key> aus.

HINWEIS:

- Die TLS-verschlüsselte Kommunikation kann den für die Gerätesignaturen verwendeten <Device Signature Key> oder das für die Zugriffsbeschränkung verwendete <AMS> nicht benutzen.

5 **Drücken Sie <OK>.**

6 Drücken Sie (Einstell./Speicherung) ▶ <Einstelländerungen anwenden> ▶ <Ja>.

➠ Das Gerät startet neu und übernimmt die Einstellungen.

■ Verwenden von Remote UI

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstell./Speicherung].

3 Klicken Sie auf [Netzwerk] ▶ [Einstellungen TLS].

4 Klicken Sie auf [Schlüssel und Zertifikat].

5 Klicken Sie auf [Verwenden] für den Schlüssel und das Zertifikat, die für die TLS-verschlüsselte Kommunikation verwendet werden sollen.

- Wenn Sie den vorinstallierten Schlüssel und das Zertifikat verwenden möchten, wählen Sie [Default Key].

6 Klicken Sie auf [Einstelländer. anw.], um das Gerät neu zu starten.

➠ Das Gerät startet neu und übernimmt die Einstellungen.

Schritt 3: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für TLS)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

HINWEIS

- Möglicherweise müssen Sie der Zertifizierungsstelle beim Deaktivieren des Zertifikats einige Informationen übermitteln. Schauen Sie unter **Prüfen, ob Sie weitere Verfahren durchführen müssen(P. 5)** nach, und notieren Sie sich die erforderlichen Informationen, bevor Sie den Schlüssel/das Zertifikat löschen.

Verwenden des Bedienfelds(P. 24)
Verwenden von Remote UI(P. 25)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Liste Schlüssel und Zertifikat> ▶ <Schlüsselu. Zertifikatsliste für d.Gerät>.

- <Schlüsselu. Zertifikatsliste für d.Gerät> wird nur angezeigt, wenn die Benutzersignaturfunktion auf dem Gerät aktiviert ist. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

3 Wählen Sie den Schlüssel und das Zertifikat ▶ drücken Sie <Löschen> ▶ <Ja>.

Beispielbildschirm:

HINWEIS:

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn nicht erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Wenn Sie einen Schlüssel und ein Zertifikat auswählen und dann <Zertifikat details> drücken, erscheinen detaillierte Informationen über das Zertifikat. Sie können auch <Zert. verifiz.> auf diesem Bildschirm drücken, um zu prüfen, ob das Zertifikat gültig ist.

■Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstell./Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].**

4 **Wählen Sie den Schlüssel und das Zertifikat ▶ klicken Sie auf [Löschen] ▶ [OK].**

HINWEIS

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Klicken Sie auf einen Schlüsselnamen, um detaillierte Informationen zu dem Zertifikat anzuzeigen. Sie können auch auf [Zertifikat verifizieren] auf diesem Bildschirm klicken, um zu überprüfen, ob das Zertifikat gültig ist.

Schritt 4: Deaktivieren des Zertifikats (für TLS)

Deaktivieren Sie ein in der Vergangenheit erstelltes Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.

■ Für ein selbstsigniertes Zertifikat

Wenn ein Zertifikat mit enthaltenem Schlüssel, das zusätzliche Verfahren erfordert, in einem Computer oder Webbrowser als vertrauenswürdiges Zertifikat registriert ist, löschen Sie das registrierte Zertifikat.

■ Für ein CSR/SCEP-Zertifikat

Fordern Sie die Zertifizierungsstelle auf, die das Zertifikat ausgestellt hat, das Zertifikat zu widerrufen. Die zuständige Zertifizierungsstelle finden Sie unter [Aussteller] im Zertifikat.

HINWEIS

- Wenn Sie den Widerruf eines Zertifikats mithilfe einer CRL auf einem Computer oder Webbrowser, der mit dem Gerät kommuniziert, überprüfen, registrieren Sie die aktualisierte CRL auf dem Computer oder Webbrowser, nachdem das Zertifikat widerrufen wurde.
- Wenn Sie eine andere Methode als eine CRL (beispielsweise OCSP) zur Überprüfung des Zertifikatswiderrufs verwenden, führen Sie das Verfahren für diese Methode durch.

Schritt 5: Aktivieren des neuen Zertifikats (für TLS)

Aktivieren Sie das Zertifikat, das auf dem Gerät neu generiert wurde.

■ Für ein selbstsigniertes Zertifikat

Registrieren Sie das neue Zertifikat auf dem Computer oder im Webbrowser als vertrauenswürdiges Zertifikat.

■ Für ein CSR/SCEP-Zertifikat

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen.

Verfahren für IEEE 802.1X

Schritt 1: Überprüfen der Authentifizierungsmethode (für IEEE 802.1X)

Sie müssen die folgenden Verfahren durchführen, wenn die IEEE 802.1X-Authentifizierungsmethode auf EAP-TLS eingestellt ist.
Befolgen Sie das nachstehende Verfahren, um die Authentifizierungsmethode zu überprüfen.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

Verwenden des Bedienfelds(P. 29)
Verwenden von Remote UI(P. 29)

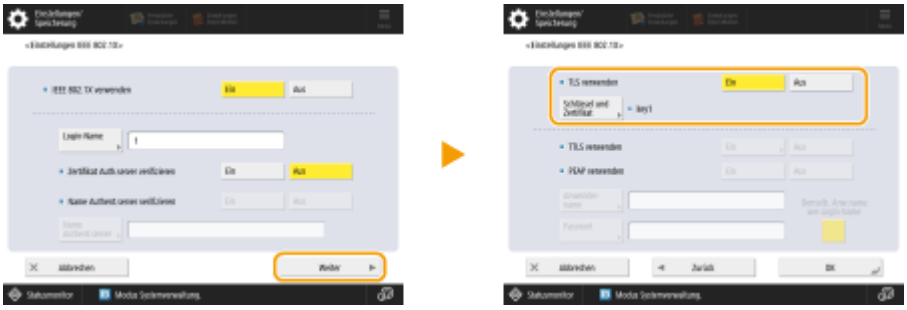
■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen IEEE 802.1X>.

3 Drücken Sie <Weiter> ▶ überprüfen Sie <TLS verwenden>.

Beispielbildschirm:



- Wenn <TLS verwenden> auf <Ein> gesetzt ist und ein Schlüsselname für <Schlüssel und Zertifikat> erscheint, führen Sie die folgenden Schritte aus.
- Wenn <TLS verwenden> auf <Aus> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

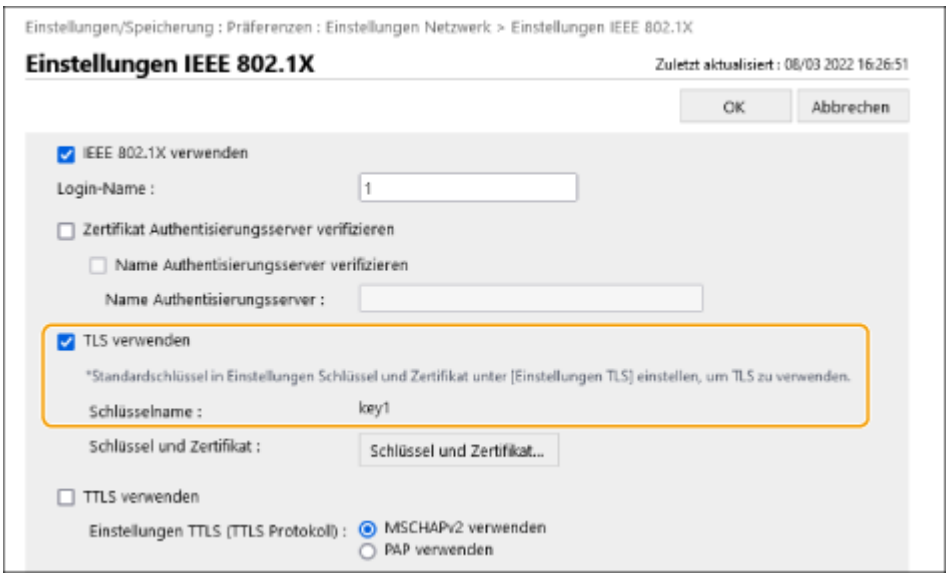
■Verwenden von Remote UI

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Netzwerk] ▶ [Einstellungen IEEE 802.1X].

4 Überprüfen Sie [TLS verwenden].



- Wenn [TLS verwenden] ausgewählt ist und ein Schlüsselname erscheint, führen Sie die folgenden Schritte aus.
- Wenn [TLS verwenden] abgewählt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IEEE 802.1X)

Sie können drei Typen von Zertifikaten für einen mit dem Gerät generierten Schlüssel erzeugen: ein selbstsigniertes Zertifikat, ein CSR-Zertifikat und ein SCEP-Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. In diesem Fall führen Sie die Vorgänge über die Remote UI aus.

Für ein selbstsigniertes Zertifikat(P. 31)
Für ein CSR-Zertifikat(P. 34)
Für ein SCEP-Zertifikat(P. 36)

Für ein selbstsigniertes Zertifikat

Verwenden des Bedienfelds(P. 31)
Verwenden von Remote UI(P. 32)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Schlüssel generieren> ▶ <Netzwerk Kommunikationsschl. generieren>.

3 Konfigurieren Sie die erforderlichen Einstellungen, und fahren Sie mit dem nächsten Bildschirm fort.
Beispielbildschirm:

a <Schlüsselname>

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b <Algorithmus Signatur>

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt. Wenn Sie <RSA> für c wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für d setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

c <Schlüsselalgorithmus>

Wählen Sie den Schlüsselalgorithmus. Wenn Sie <RSA> wählen, erscheint <Schlüssellänge (Bit)> als Einstelloption für d. Wenn Sie <ECDSA> wählen, wird stattdessen <Schlüsseltyp> angezeigt.

d <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für c wählen, oder legen Sie den Schlüsseltyp fest, wenn Sie <ECDSA> wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

4 Konfigurieren Sie die erforderlichen Elemente für das Zertifikat ▶ drücken Sie <Schlüssel gener.>.

Beispielbildschirm:

a <Startdatum Gültigkeit>/<Enddatum Gültigkeit>

Geben Sie das Startdatum und das Enddatum des Gültigkeitszeitraums für das Zertifikat ein.

b <Land/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

Wählen Sie die Landeskennzahl aus der Liste, und geben Sie den Standort und den Namen des Unternehmens an.

c <Allgemeiner Name>

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

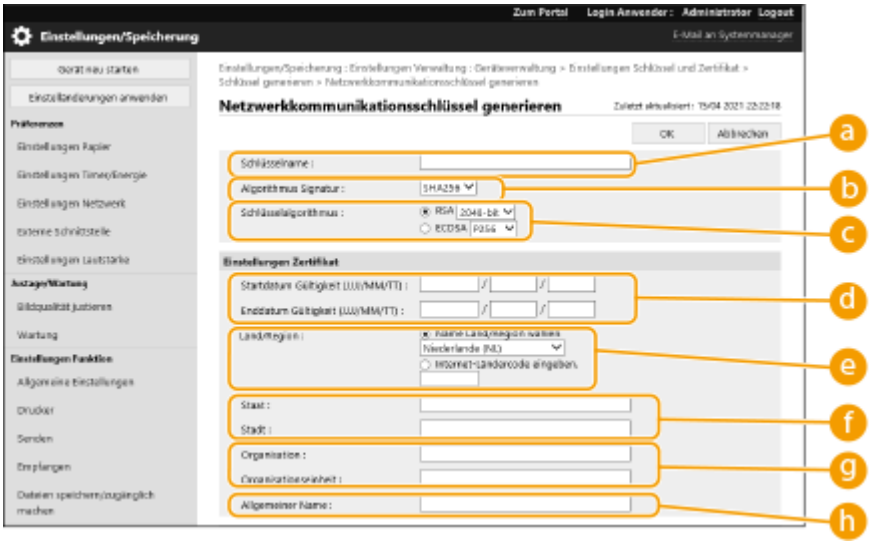
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Netzwerkkommunikation].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a [Schlüsselname]

Geben Sie einen Namen für den Schlüssel in alphanumerischen Zeichen ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt.

c [Schlüsselalgorithmus]

Wählen Sie [RSA] oder [ECDSA] als Algorithmus zur Generierung des Schlüssels. Geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

HINWEIS:

- Wenn Sie [SHA384] oder [SHA512] für [Algorithmus Signatur] wählen, können Sie die Schlüssellänge nicht auf [512-bit] einstellen, wenn Sie [RSA] für [Schlüsselalgorithmus] wählen.

d [Startdatum Gültigkeit (JJJJ/MM/TT)]/[Enddatum Gültigkeit (JJJJ/MM/TT)]

Geben Sie das Startdatum und Enddatum des Gültigkeitszeitraums für das Zertifikat ein. [Enddatum Gültigkeit (JJJJ/MM/TT)] kann nicht auf ein Datum vor dem Datum in [Startdatum Gültigkeit (JJJJ/MM/TT)] festgelegt werden.

e [Land/Region]

Klicken Sie auf [Name Land/Region wählen], und wählen Sie das Land/die Region aus der Dropdown-Liste. Alternativ können Sie auch auf [Internet-Ländercode eingeben.] klicken und einen Ländercode eingeben, wie beispielsweise "US" für die Vereinigten Staaten.

f [Staat]/[Stadt]

Geben Sie den Standort in alphanumerischen Zeichen ein, sofern erforderlich.

g [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation in alphanumerischen Zeichen ein, sofern erforderlich.

h [Allgemeiner Name]

Geben Sie gegebenenfalls den allgemeinen Namen (Common Name) des Zertifikats ein, und verwenden Sie dabei alphanumerische Zeichen. Der "Common Name" wird häufig mit "CN" abgekürzt.

7 Klicken Sie auf [OK].

- Die Erzeugung eines Schlüssels und eines Zertifikats kann einige Zeit dauern.
- Generierte Schlüssel und Zertifikate werden automatisch auf dem Gerät registriert.

Für ein CSR-Zertifikat

Generieren Sie einen Schlüssel und eine Zertifizierungsanforderung (CSR) auf dem Gerät. Verwenden Sie die auf dem Bildschirm angezeigten oder in eine Datei ausgegebenen CSR-Daten, um die Zertifizierungsstelle zur Ausstellung eines Zertifikats aufzufordern. Registrieren Sie dann das ausgestellte Zertifikat für den Schlüssel.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

■1. Generieren eines Schlüssels und einer CSR

1 Starten Sie die Remote UI.

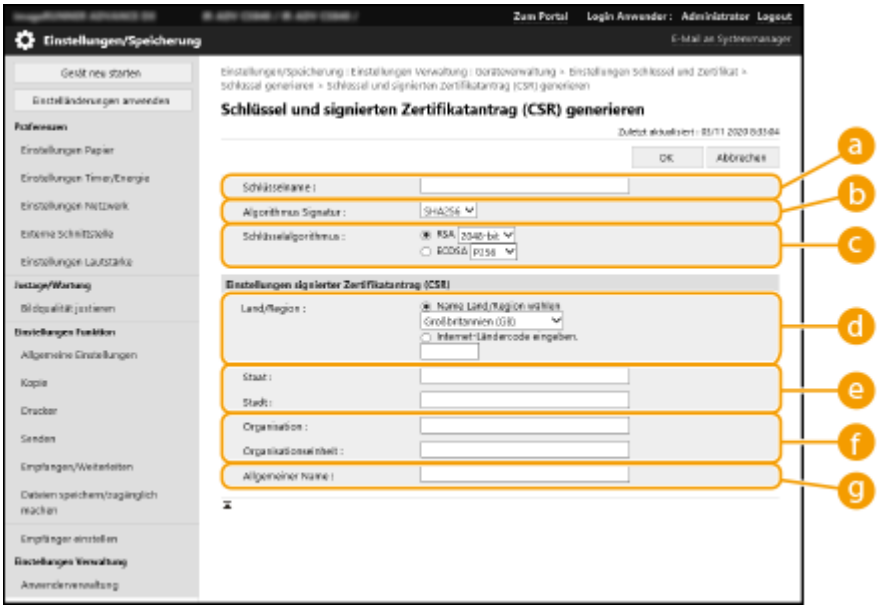
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Schlüssel und signierter Zertifikatantrag (CSR)].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a [Schlüsselname]

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

[Algorithmus Signatur]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

[Schlüsselalgorithmus]

Wählen Sie den Schlüsselalgorithmus aus, und geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen.

[Land/Region]

Wählen Sie den Ländercode aus der Liste, oder geben Sie ihn direkt ein.

[Staat]/[Stadt]

Geben Sie den Standort ein.

[Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation ein.

[Allgemeiner Name]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

7 Klicken Sie auf [OK].

➠ Die CSR-Daten werden angezeigt.

- Wenn Sie die CSR-Daten in einer Datei speichern möchten, klicken Sie auf [In Datei speichern], und legen Sie den Speicherort fest.

HINWEIS:

- Der Schlüssel, der die CSR generiert hat, wird auf dem Schlüssel- und- Zertifikatlistenbildschirm angezeigt, jedoch können Sie den Schlüssel selbst nicht verwenden. Um diesen Schlüssel zu verwenden, müssen Sie das Zertifikat registrieren, das später auf der Grundlage der CSR ausgestellt wird.

8 Fordern Sie die Zertifizierungsstelle auf, ein Zertifikat auf der Grundlage der CSR-Daten auszustellen.

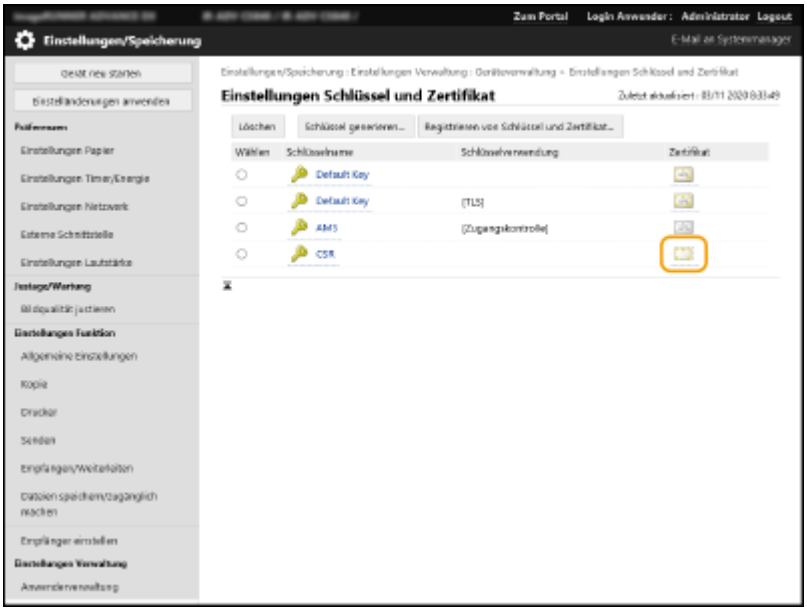
■2. Registrieren des ausgestellten Zertifikats für den Schlüssel

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie in der Liste [Zertifikat] auf für das Zertifikat, das Sie registrieren möchten.



5 Klicken Sie auf [Zertifikat speichern...].

6 Registrieren Sie das Zertifikat.

- Klicken Sie auf [Durchsuchen...] ▶ geben Sie die zu registrierende Datei (Zertifikat) an ▶ klicken Sie auf [Speichern].

Für ein SCEP-Zertifikat

Fordern Sie den SCEP-Server manuell zur Ausstellung eines Zertifikats auf.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

HINWEIS

- Sie können keine manuelle Anforderung zur Ausstellung eines Zertifikats senden, wenn [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ausgewählt ist. Deaktivieren Sie diese Option, wenn sie ausgewählt ist.

Starten Sie die Remote UI ▶ klicken Sie auf [Einstellungen/Speicherung] ▶ [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)] ▶ [Einstellungen für automatische Anforderung der Zertifikatsausstellung] ▶ deaktivieren Sie [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ▶ klicken Sie auf [Update].

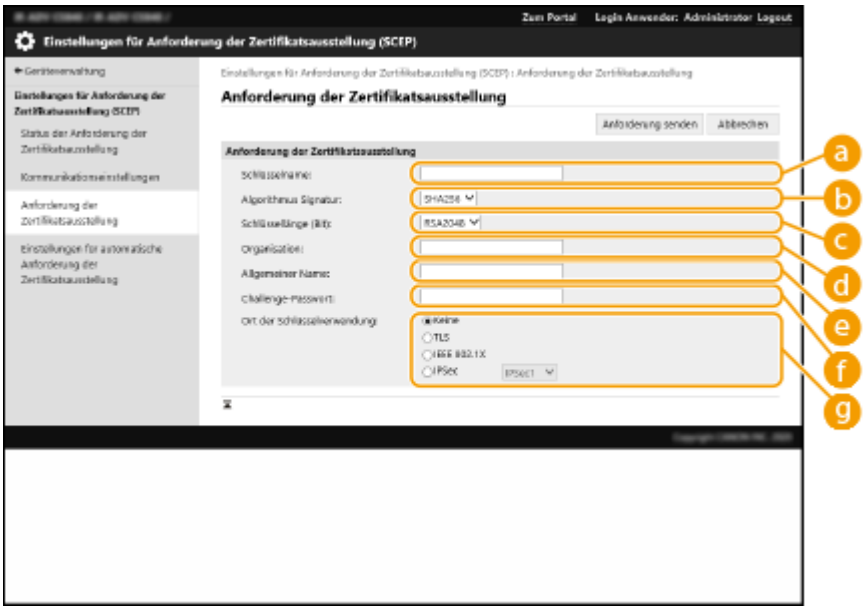
1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)].**

4 **Klicken Sie auf [Anforderung der Zertifikatsausstellung].**

5 **Konfigurieren Sie die erforderlichen Einstellungen für die Anforderung eines Zertifikats.**



a [Schlüsselname:]

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur:]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

c [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

d [Organisation:]

Geben Sie den Namen der Organisation ein.

e [Allgemeiner Name:]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

f [Challenge-Passwort:]

Ist auf der Seite des SCEP-Servers ein Passwort vorgeschrieben, geben Sie das abzufragende Passwort, das in den Anforderungsdaten (PKCS#9) enthalten ist, ein, um die Ausstellung eines Zertifikats anzufordern.

g [Ort der Schlüsselverwendung:]

Wählen Sie [IEEE 802.1X].

HINWEIS:

- Wenn Sie etwas anderes als [Keine] auswählen, aktivieren Sie jede Funktion im Voraus. Wenn ein Zertifikat bei jeweils deaktivierter Funktion erfolgreich bezogen wird, wird das Zertifikat dem Standort der Schlüsselnutzung zugewiesen, jedoch wird nicht jede Funktion automatisch aktiviert.

6 **Klicken Sie auf [Anforderung senden].**

7 **Klicken Sie auf [Neustart].**

Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IEEE 802.1X)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.
Dieses Verfahren ist für ein SCEP-Zertifikat nicht erforderlich.

Für ein selbstsigniertes Zertifikat/CSR-Zertifikat

Verwenden des Bedienfelds(P. 39)
Verwenden von Remote UI(P. 40)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen IEEE 802.1X>.**

3 **Drücken Sie <Ein> für <IEEE 802.1X verwenden> ▶ konfigurieren Sie die erforderlichen Einstellungen ▶ drücken Sie <Weiter>.**
Beispielbildschirm:

a <Login-Name>

Geben Sie den Namen (EAP-Identität) des Anmeldebenutzers ein, um die IEEE 802.1X-Authentifizierung zu erhalten.

b <Zertifikat Auth.server verifizieren>

Setzen Sie diese Einstellung auf <Ein>, wenn von einem Authentifizierungsserver gesendete Serverzertifikate verifiziert werden sollen.

c <Name Authent.server verifizieren>

Um einen allgemeinen Namen im Serverzertifikat zu verifizieren, wählen Sie <Ein>. Geben Sie dann den Namen des Authentifizierungsservers, bei dem der Anmeldebenutzer registriert ist, unter <Name Authent.server> ein.

4 **Drücken Sie <Ein> für <TLS verwenden> ▶ drücken Sie <Schlüssel und Zertifikat>.**

5 **Wählen Sie den zu verwendenden Schlüssel und das Zertifikat in der Liste aus ▶ drücken Sie <Als Std.schl. einstellen> ▶ <Ja>.**

6 **Drücken Sie <OK>.**

7 **Drücken Sie (Einstell./Speicherung) ▶ (Einstell./Speicherung) ▶ <Einstelländer. anw.> ▶ <Ja>.**

➠ Das Gerät startet neu und übernimmt die Einstellungen.

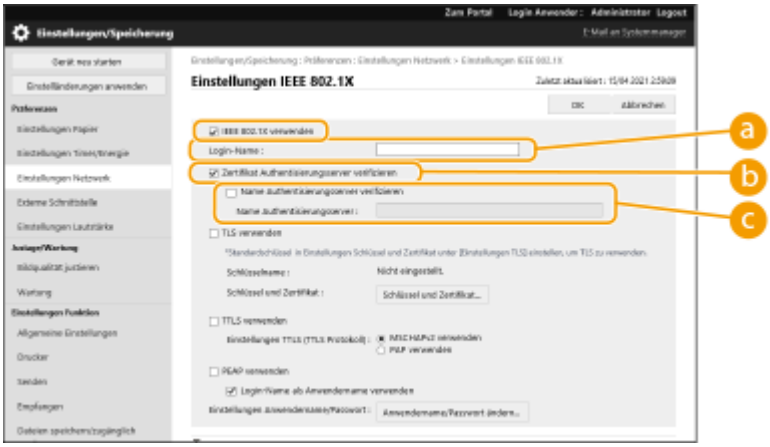
■ Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].**

3 **Klicken Sie auf [Einstellungen Netzwerk] ▶ [Einstellungen IEEE 802.1X].**

4 **Wählen Sie[IEEE 802.1X verwenden] ▶ konfigurieren Sie die erforderlichen Einstellungen.**



a [Login-Name]

Geben Sie den Namen (EAP-Identität) des Anmeldebenutzers ein, um die IEEE 802.1X-Authentifizierung zu erhalten.

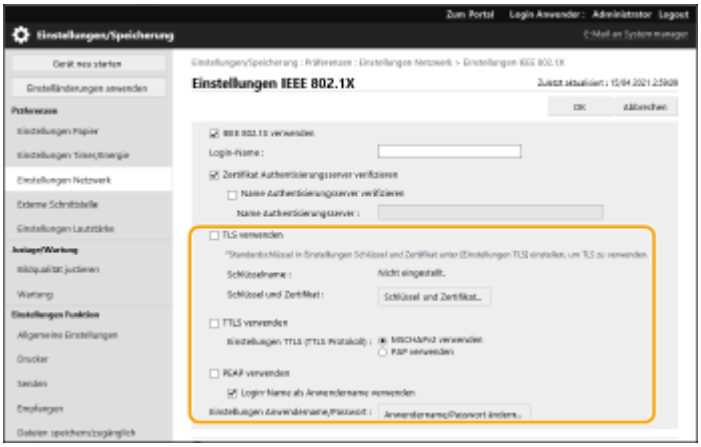
b [Zertifikat Authentisierungsserver verifizieren]

Aktivieren Sie dieses Kontrollkästchen, wenn von einem Authentifizierungsserver gesendete Serverzertifikate verifiziert werden sollen.

c [Name Authentisierungsserver verifizieren]

Um den allgemeinen Namen im Serverzertifikat zu verifizieren, aktivieren Sie dieses Kontrollkästchen. Geben Sie dann den Namen des Authentifizierungsservers, bei dem der Anmeldebenutzer registriert ist, unter [Name Authentisierungsserver] ein.

5 Wählen Sie [TLS verwenden] ▶ klicken Sie auf [Schlüssel und Zertifikat].



6 Klicken Sie auf [Verwenden] für den zu verwendenden Schlüssel in der Liste.

7 Klicken Sie auf [OK].

8 Klicken Sie auf [Einstelländerungen anwenden], um das Gerät neu zu starten.

➠ Das Gerät startet neu und übernimmt die Einstellungen.

Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IEEE 802.1X)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

HINWEIS

- Möglicherweise müssen Sie der Zertifizierungsstelle beim Deaktivieren des Zertifikats einige Informationen übermitteln. Schauen Sie unter **Prüfen, ob Sie weitere Verfahren durchführen müssen(P. 5)** nach, und notieren Sie sich die erforderlichen Informationen, bevor Sie den Schlüssel/das Zertifikat löschen.

Verwenden des Bedienfelds(P. 42)
Verwenden von Remote UI(P. 43)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Liste Schlüssel und Zertifikat> ▶ <Schlüsselu. Zertifikatsliste für d.Gerät>.**

- <Schlüsselu. Zertifikatsliste für d.Gerät> wird nur angezeigt, wenn die Benutzersignaturfunktion auf dem Gerät aktiviert ist. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

3 **Wählen Sie den Schlüssel und das Zertifikat ▶ drücken Sie <Löschen> ▶ <Ja>.**

Beispielbildschirm:

HINWEIS:

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn nicht erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Wenn Sie einen Schlüssel und ein Zertifikat auswählen und dann <Zertifikat details> drücken, erscheinen detaillierte Informationen über das Zertifikat. Sie können auch <Zert. verifiz.> auf diesem Bildschirm drücken, um zu prüfen, ob das Zertifikat gültig ist.

■Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstell./Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].**

4 **Wählen Sie den Schlüssel und das Zertifikat ▶ klicken Sie auf [Löschen] ▶ [OK].**

HINWEIS

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Klicken Sie auf einen Schlüsselnamen, um detaillierte Informationen zu dem Zertifikat anzuzeigen. Sie können auch auf [Zertifikat verifizieren] auf diesem Bildschirm klicken, um zu überprüfen, ob das Zertifikat gültig ist.

Schritt 5: Deaktivieren des Zertifikats (für IEEE 802.1X)

Deaktivieren Sie ein in der Vergangenheit erstelltes Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.

■ Für ein selbstsigniertes Zertifikat

Wenn ein Zertifikat mit enthaltenem Schlüssel, das zusätzliche Verfahren erfordert, auf einem IEEE 802.1X-Authentifizierungsserver als vertrauenswürdiges Zertifikat registriert ist, löschen Sie das registrierte Zertifikat.

■ Für ein CSR/SCEP-Zertifikat

Fordern Sie die Zertifizierungsstelle auf, die das Zertifikat ausgestellt hat, das Zertifikat zu widerrufen. Die zuständige Zertifizierungsstelle finden Sie unter [Aussteller] im Zertifikat.

HINWEIS

- Wenn Sie den Widerruf eines Zertifikats mithilfe einer CRL auf einem IEEE 802.1X-Authentifizierungsserver überprüfen, registrieren Sie die aktualisierte CRL auf dem Computer oder Webbrowser, nachdem das Zertifikat widerrufen wurde.
- Wenn Sie eine andere Methode als eine CRL (beispielsweise OCSP) zur Überprüfung des Zertifikatswiderrufs verwenden, führen Sie das Verfahren für diese Methode durch.

Schritt 6: Aktivieren des neuen Zertifikats (für IEEE 802.1X)

Aktivieren Sie das Zertifikat.

■ Für ein selbstsigniertes Zertifikat

Registrieren Sie das neue Zertifikat auf dem IEEE 802.1X-Authentifizierungsserver als vertrauenswürdiges Zertifikat.

■ Für ein CSR/SCEP-Zertifikat

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen.

Verfahren für IPSec

Schritt 1: Überprüfen der Authentifizierungsmethode (für IPSec)

Sie müssen die folgenden Verfahren durchführen, wenn die Authentifizierungsmethode für die IKE-Einstellung in IPsec auf <Digitale Sig. Methode> gesetzt ist.
Befolgen Sie das nachstehende Verfahren, um die Authentifizierungsmethode zu überprüfen.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

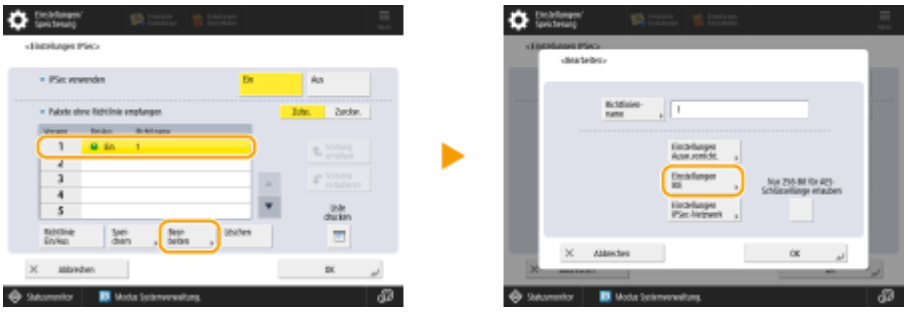
Verwenden des Bedienfelds(P. 47)
Verwenden von Remote UI(P. 48)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen IPSec>.**

3 **Wählen Sie die registrierte Richtlinie aus ▶ drücken Sie <Bearbeiten> ▶ <Einstellungen IKE>.**
Beispielbildschirm:



4 **Drücken Sie <Weiter> ▶ überprüfen Sie <Authentisierungsmethode>.**

Beispielbildschirm:

- Wenn <Authentisierungsmethode> auf <Digitale Sig. Methode> gesetzt ist und ein Schlüsselname für <Schlüssel und Zertifikat> erscheint, führen Sie die folgenden Schritte aus.

- Wenn <Authentisierungsmethode> auf <Meth. Pregem. Schls.> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

■Verwenden von Remote UI

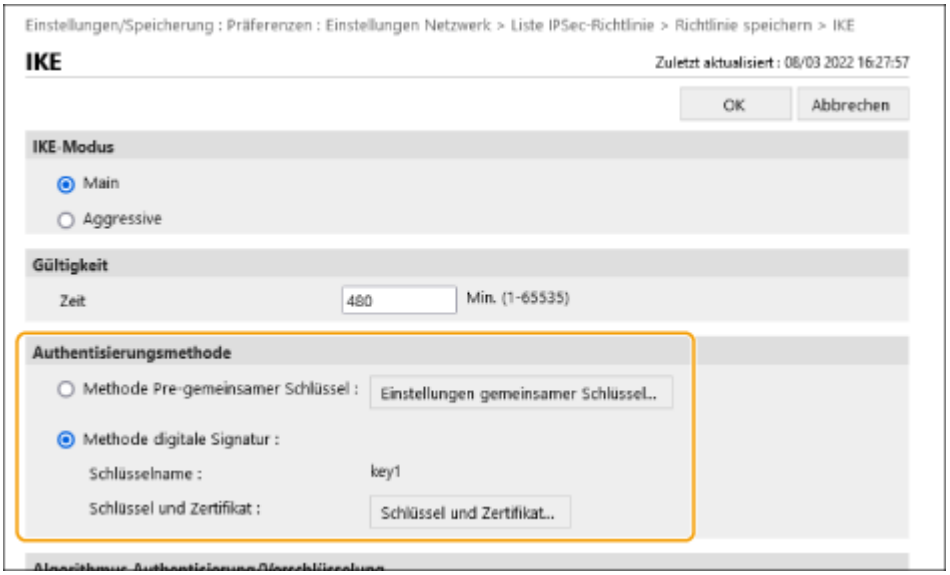
1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Einstellungen Netzwerk] ▶ [Liste IPSec-Richtlinie].

4 Klicken Sie auf die Richtlinie in der Liste ▶ klicken Sie auf [Einstellungen IKE].

5 Überprüfen Sie [Authentisierungsmethode].



- Wenn [Authentisierungsmethode] auf [Methode digitale Signatur] gesetzt ist und ein Schlüsselname erscheint, führen Sie die folgenden Schritte aus.
- Wenn <Authentisierungsmethode> auf <Methode Pre-gemeinsamer Schlüssel> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IPSec)

Sie können drei Typen von Zertifikaten für einen mit dem Gerät generierten Schlüssel erzeugen: ein selbstsigniertes Zertifikat, ein CSR-Zertifikat und ein SCEP-Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. In diesem Fall führen Sie die Vorgänge über die Remote UI aus.

Für ein selbstsigniertes Zertifikat(P. 49)
Für ein CSR-Zertifikat(P. 52)
Für ein SCEP-Zertifikat(P. 54)

Für ein selbstsigniertes Zertifikat

Verwenden des Bedienfelds(P. 49)
Verwenden von Remote UI(P. 50)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Schlüssel generieren> ▶ <Netzwerk Kommunikationsschl. generieren>.

3 Konfigurieren Sie die erforderlichen Einstellungen, und fahren Sie mit dem nächsten Bildschirm fort.
Beispielbildschirm:

a <Schlüsselname>

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b <Algorithmus Signatur>

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt. Wenn Sie <RSA> für c wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für d setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

c <Schlüsselalgorithmus>

Wählen Sie den Schlüsselalgorithmus. Wenn Sie <RSA> wählen, erscheint <Schlüssellänge (Bit)> als Einstelloption für d. Wenn Sie <ECDSA> wählen, wird stattdessen <Schlüsseltyp> angezeigt.

d <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für c wählen, oder legen Sie den Schlüsseltyp fest, wenn Sie <ECDSA> wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

4 Konfigurieren Sie die erforderlichen Elemente für das Zertifikat ▶ drücken Sie <Schlüssel gener.>.

Beispielbildschirm:

a <Startdatum Gültigkeit>/<Enddatum Gültigkeit>

Geben Sie das Startdatum und das Enddatum des Gültigkeitszeitraums für das Zertifikat ein.

b <Land/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

Wählen Sie die Landeskennzahl aus der Liste, und geben Sie den Standort und den Namen des Unternehmens an.

c <Allgemeiner Name>

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

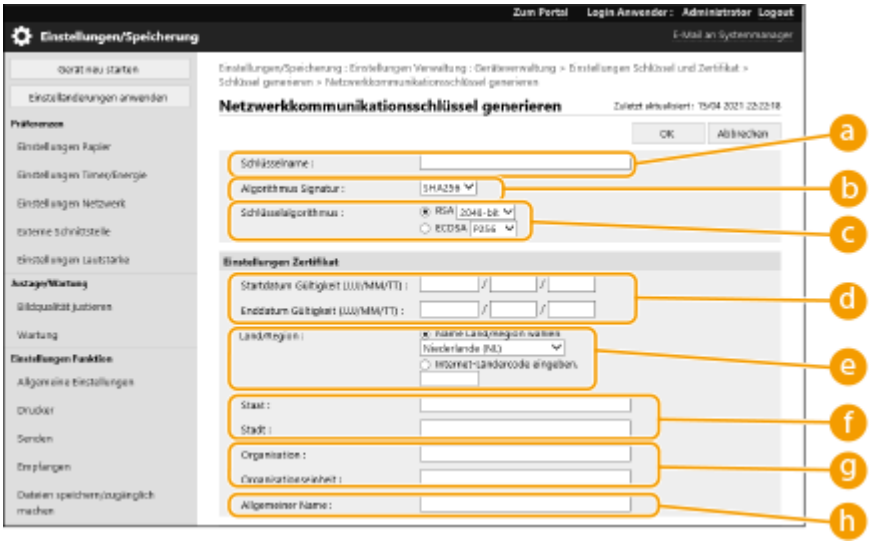
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Netzwerkkommunikation].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a [Schlüsselname]

Geben Sie einen Namen für den Schlüssel in alphanumerischen Zeichen ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt.

c [Schlüsselalgorithmus]

Wählen Sie [RSA] oder [ECDSA] als Algorithmus zur Generierung des Schlüssels. Geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

HINWEIS:

- Wenn Sie [SHA384] oder [SHA512] für [Algorithmus Signatur] wählen, können Sie die Schlüssellänge nicht auf [512-bit] einstellen, wenn Sie [RSA] für [Schlüsselalgorithmus] wählen.

d [Startdatum Gültigkeit (JJJJ/MM/TT)]/[Enddatum Gültigkeit (JJJJ/MM/TT)]

Geben Sie das Startdatum und Enddatum des Gültigkeitszeitraums für das Zertifikat ein. [Enddatum Gültigkeit (JJJJ/MM/TT)] kann nicht auf ein Datum vor dem Datum in [Startdatum Gültigkeit (JJJJ/MM/TT)] festgelegt werden.

e [Land/Region]

Klicken Sie auf [Name Land/Region wählen], und wählen Sie das Land/die Region aus der Dropdown-Liste. Alternativ können Sie auch auf [Internet-Ländercode eingeben.] klicken und einen Ländercode eingeben, wie beispielsweise "US" für die Vereinigten Staaten.

f [Staat]/[Stadt]

Geben Sie den Standort in alphanumerischen Zeichen ein, sofern erforderlich.

g [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation in alphanumerischen Zeichen ein, sofern erforderlich.

h [Allgemeiner Name]

Geben Sie gegebenenfalls den allgemeinen Namen (Common Name) des Zertifikats ein, und verwenden Sie dabei alphanumerische Zeichen. Der "Common Name" wird häufig mit "CN" abgekürzt.

7 Klicken Sie auf [OK].

- Die Erzeugung eines Schlüssels und eines Zertifikats kann einige Zeit dauern.
- Generierte Schlüssel und Zertifikate werden automatisch auf dem Gerät registriert.

Für ein CSR-Zertifikat

Generieren Sie einen Schlüssel und eine Zertifizierungsanforderung (CSR) auf dem Gerät. Verwenden Sie die auf dem Bildschirm angezeigten oder in eine Datei ausgegebenen CSR-Daten, um die Zertifizierungsstelle zur Ausstellung eines Zertifikats aufzufordern. Registrieren Sie dann das ausgestellte Zertifikat für den Schlüssel.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

■1. Generieren eines Schlüssels und einer CSR

1 Starten Sie die Remote UI.

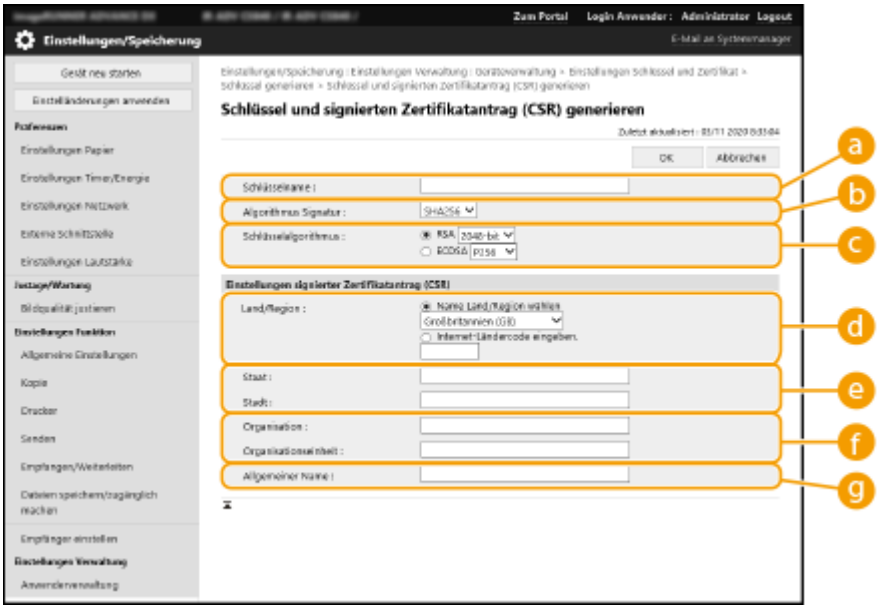
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Schlüssel und signierter Zertifikatantrag (CSR)].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a **[Schlüsselname]**

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

[Algorithmus Signatur]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

[Schlüsselalgorithmus]

Wählen Sie den Schlüsselalgorithmus aus, und geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen.

[Land/Region]

Wählen Sie den Ländercode aus der Liste, oder geben Sie ihn direkt ein.

[Staat]/[Stadt]

Geben Sie den Standort ein.

[Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation ein.

[Allgemeiner Name]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

7 Klicken Sie auf [OK].

➠ Die CSR-Daten werden angezeigt.

- Wenn Sie die CSR-Daten in einer Datei speichern möchten, klicken Sie auf [In Datei speichern], und legen Sie den Speicherort fest.

HINWEIS:

- Der Schlüssel, der die CSR generiert hat, wird auf dem Schlüssel- und- Zertifikatlistenbildschirm angezeigt, jedoch können Sie den Schlüssel selbst nicht verwenden. Um diesen Schlüssel zu verwenden, müssen Sie das Zertifikat registrieren, das später auf der Grundlage der CSR ausgestellt wird.

8 Fordern Sie die Zertifizierungsstelle auf, ein Zertifikat auf der Grundlage der CSR-Daten auszustellen.

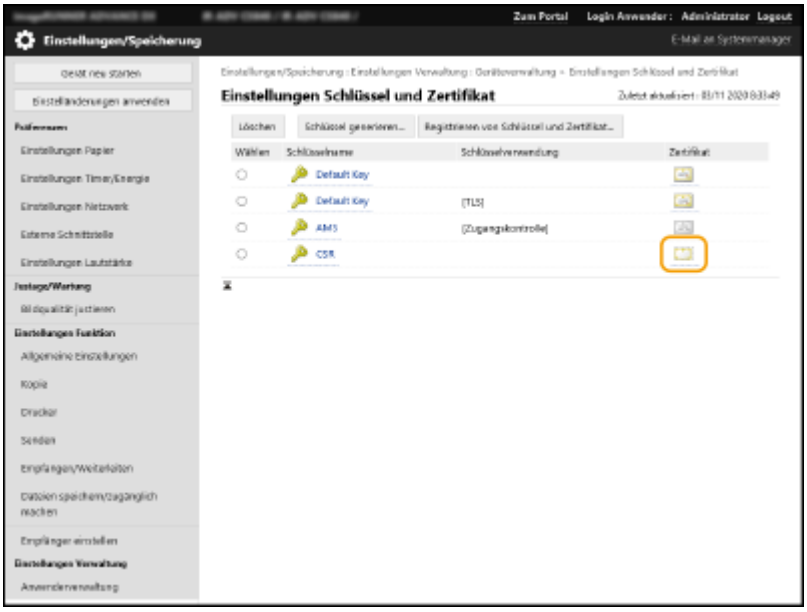
■2. Registrieren des ausgestellten Zertifikats für den Schlüssel

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie in der Liste [Zertifikat] auf für das Zertifikat, das Sie registrieren möchten.



5 Klicken Sie auf [Zertifikat speichern...].

6 Registrieren Sie das Zertifikat.

- Klicken Sie auf [Durchsuchen...] ▶ geben Sie die zu registrierende Datei (Zertifikat) an ▶ klicken Sie auf [Speichern].

Für ein SCEP-Zertifikat

Fordern Sie den SCEP-Server manuell zur Ausstellung eines Zertifikats auf.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

HINWEIS

- Sie können keine manuelle Anforderung zur Ausstellung eines Zertifikats senden, wenn [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ausgewählt ist. Deaktivieren Sie diese Option, wenn sie ausgewählt ist.

Starten Sie die Remote UI ▶ klicken Sie auf [Einstellungen/Speicherung] ▶ [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)] ▶ [Einstellungen für automatische Anforderung der Zertifikatsausstellung] ▶ deaktivieren Sie [Timer für automatische Anforderung der Zertifikatsausstellung aktivieren] ▶ klicken Sie auf [Update].

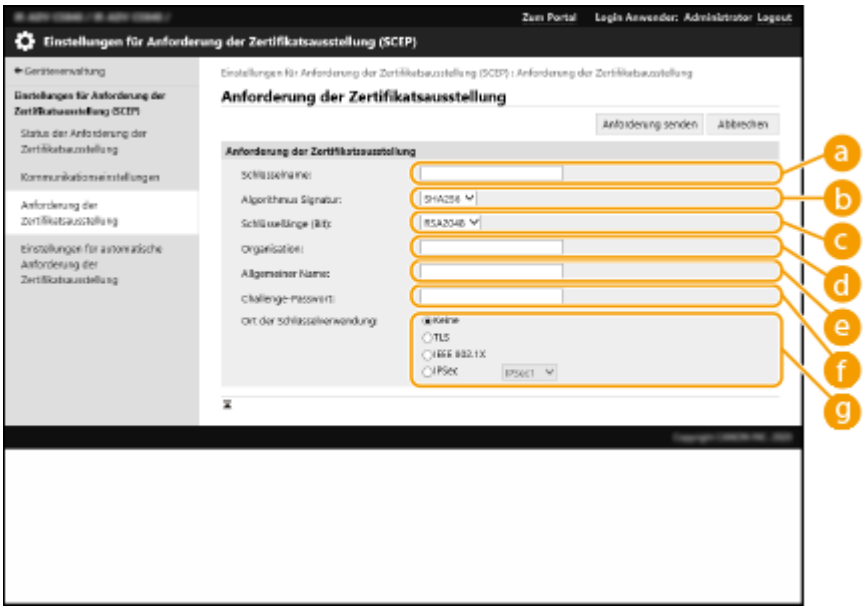
1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen für Anforderung Zertifikatsausstellung (SCEP)].**

4 **Klicken Sie auf [Anforderung der Zertifikatsausstellung].**

5 **Konfigurieren Sie die erforderlichen Einstellungen für die Anforderung eines Zertifikats.**



a [Schlüsselname:]

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur:]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

c [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

d [Organisation:]

Geben Sie den Namen der Organisation ein.

e [Allgemeiner Name:]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

f [Challenge-Passwort:]

Ist auf der Seite des SCEP-Servers ein Passwort vorgeschrieben, geben Sie das abzufragende Passwort, das in den Anforderungsdaten (PKCS#9) enthalten ist, ein, um die Ausstellung eines Zertifikats anzufordern.

g [Ort der Schlüsselverwendung:]

Wählen Sie [IPSec].

HINWEIS:

- Wenn Sie etwas anderes als [Keine] auswählen, aktivieren Sie jede Funktion im Voraus. Wenn ein Zertifikat bei jeweils deaktivierter Funktion erfolgreich bezogen wird, wird das Zertifikat dem Standort der Schlüsselnutzung zugewiesen, jedoch wird nicht jede Funktion automatisch aktiviert.

6 **Klicken Sie auf [Anforderung senden].**

7 **Klicken Sie auf [Neustart].**

Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IPSec)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.
Dieses Verfahren ist für ein SCEP-Zertifikat nicht erforderlich.

Für ein selbstsigniertes Zertifikat/CSR-Zertifikat

Verwenden des Bedienfelds(P. 57)
Verwenden von Remote UI(P. 58)

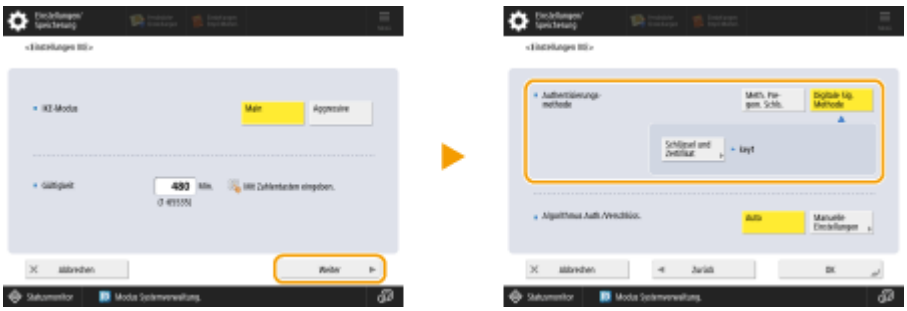
■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen IPSec>.**

3 **Wählen Sie die Richtlinie zum Zurücksetzen des Schlüssels und des Zertifikats für ▶ drücken Sie <Bearbeiten> ▶ <Einstellungen IKE>.**
Beispielbildschirm:

4 **Drücken Sie <Weiter> ▶ wählen Sie <Digitale Sig. Methode> unter <Authentisierungsmethode> ▶ drücken Sie <Schlüssel und Zertifikat>.**
Beispielbildschirm:



5 **Wählen Sie den zu verwendenden Schlüssel und das Zertifikat in der Liste aus ▶ drücken Sie <Als Std.schl. einstellen> ▶ <Ja>.**

6 **Drücken Sie <OK>.**

7 **Drücken Sie (Einstell./Speicherung) ▶ (Einstell./Speicherung) ▶ <Einstelländer. anw.> ▶ <Ja>.**

➠ Das Gerät startet neu und übernimmt die Einstellungen.

■ Verwenden von Remote UI

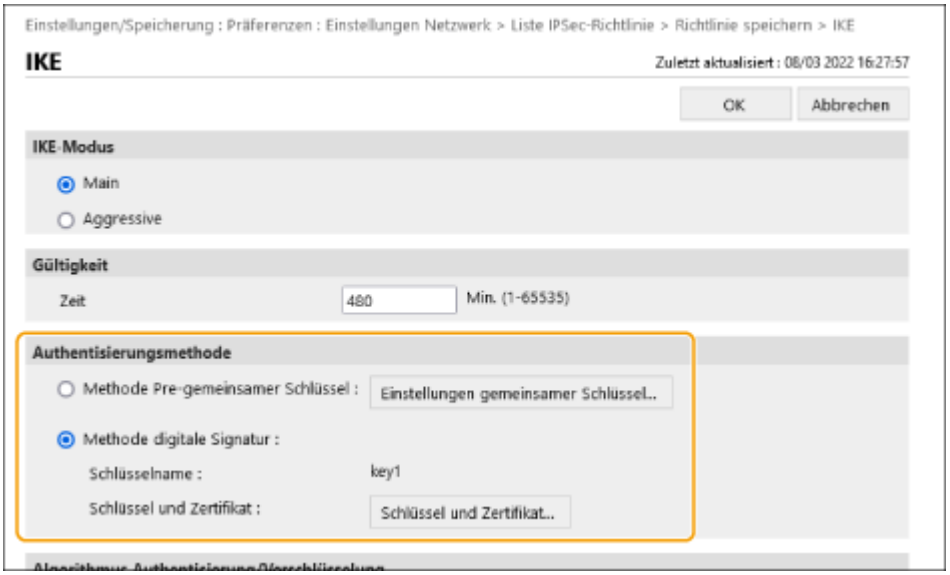
1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].**

3 **Klicken Sie auf [Einstellungen Netzwerk] ▶ [Liste IPSec-Richtlinie].**

4 **Klicken Sie in der Liste auf die Richtlinie, für die der Schlüssel und das Zertifikat zurückgesetzt werden sollen ▶ klicken Sie auf [Einstellungen IKE].**

5 **Wählen Sie [Methode digitale Signatur] unter [Authentisierungsmethode] ▶ klicken Sie auf [Schlüssel und Zertifikat].**



6 **Klicken Sie auf [Verwenden] für den zu verwendenden Schlüssel in der Liste.**

7 **Klicken Sie auf [OK].**

8 **Klicken Sie auf [Einstelländerungen anwenden], um das Gerät neu zu starten.**

➠ Das Gerät startet neu und übernimmt die Einstellungen.

Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IPSec)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

HINWEIS

- Möglicherweise müssen Sie der Zertifizierungsstelle beim Deaktivieren des Zertifikats einige Informationen übermitteln. Schauen Sie unter **Prüfen, ob Sie weitere Verfahren durchführen müssen(P. 5)** nach, und notieren Sie sich die erforderlichen Informationen, bevor Sie den Schlüssel/das Zertifikat löschen.

Verwenden des Bedienfelds(P. 60)
Verwenden von Remote UI(P. 61)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Liste Schlüssel und Zertifikat> ▶ <Schlüsselu. Zertifikatsliste für d.Gerät>.**

- <Schlüsselu. Zertifikatsliste für d.Gerät> wird nur angezeigt, wenn die Benutzersignaturfunktion auf dem Gerät aktiviert ist. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

3 **Wählen Sie den Schlüssel und das Zertifikat ▶ drücken Sie <Löschen> ▶ <Ja>.**

Beispielbildschirm:

HINWEIS:

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn nicht erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Wenn Sie einen Schlüssel und ein Zertifikat auswählen und dann <Zertifikat details> drücken, erscheinen detaillierte Informationen über das Zertifikat. Sie können auch <Zert. verifiz.> auf diesem Bildschirm drücken, um zu prüfen, ob das Zertifikat gültig ist.

■Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstell./Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].**

4 **Wählen Sie den Schlüssel und das Zertifikat ▶ klicken Sie auf [Löschen] ▶ [OK].**

HINWEIS

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Klicken Sie auf einen Schlüsselnamen, um detaillierte Informationen zu dem Zertifikat anzuzeigen. Sie können auch auf [Zertifikat verifizieren] auf diesem Bildschirm klicken, um zu überprüfen, ob das Zertifikat gültig ist.

Schritt 5: Deaktivieren des Zertifikats (für IPSec)

Deaktivieren Sie ein in der Vergangenheit erstelltes Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.

■ Für ein selbstsigniertes Zertifikat

Wenn ein Zertifikat mit enthaltenem Schlüssel, das zusätzliche Verfahren erfordert, in dem Gerät, das mit IPSec kommuniziert, als vertrauenswürdiges Zertifikat registriert ist, löschen Sie das registrierte Zertifikat. Nach dem Löschen des registrierten Zertifikats registrieren Sie das Zertifikat des neu generierten Schlüssels.

■ Für ein CSR/SCEP-Zertifikat

Fordern Sie die Zertifizierungsstelle auf, die das Zertifikat ausgestellt hat, das Zertifikat zu widerrufen. Die zuständige Zertifizierungsstelle finden Sie unter [Aussteller] im Zertifikat.

HINWEIS

- Wenn Sie den Widerruf von Zertifikaten mithilfe einer CRL in dem Gerät überprüfen, das mit IPSec kommuniziert, registrieren Sie die aktualisierte CRL auf dem Computer oder Webbrowser, nachdem das Zertifikat widerrufen wurde.
- Wenn Sie eine andere Methode als eine CRL (beispielsweise OCSP) zur Überprüfung des Zertifikatswiderrufs verwenden, führen Sie das Verfahren für diese Methode durch.

Schritt 6: Aktivieren des neuen Zertifikats (für IPSec)

Aktivieren Sie das Zertifikat.

■ Für ein selbstsigniertes Zertifikat

Registrieren Sie das neue Zertifikat auf dem Gerät, das mit IPSec kommuniziert, als vertrauenswürdiges Zertifikat.

■ Für ein CSR/SCEP-Zertifikat

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen.

Verfahren für SIP

Schritt 1: Überprüfen der Einstellungen (für SIP)

Sie müssen die zusätzlichen Verfahren durchführen, wenn die folgenden beiden Bedingungen erfüllt sind:

- <TLS verwenden> ist in den <Einstellungen Intranet> unter <Einstellungen SIP> aktiviert
- Der Schlüsselname für <Schlüssel und Zertifikat> in den <Einstellungen TLS> unter <Einstellungen SIP> erscheint

Befolgen Sie das nachstehende Verfahren, um die Einstellungen zu überprüfen.

Verwenden des Bedienfelds(P. 65)
Verwenden von Remote UI(P. 66)

Verwenden des Bedienfelds

■ Überprüfen Sie <TLS verwenden>

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen SIP> ▶ <Einstellungen Intranet>.

3 Prüfen Sie <TLS verwenden>.

Beispielbildschirm:

- Wenn <TLS verwenden> auf <Ein> gesetzt ist, fahren Sie mit der Prüfung von <Schlüssel und Zertifikat> fort.
- Wenn <TLS verwenden> auf <Aus> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

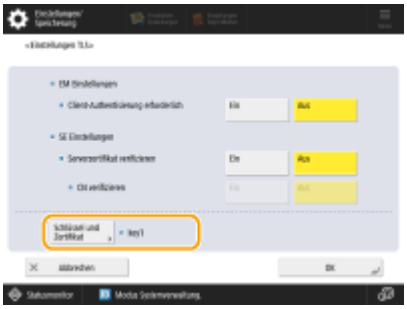
■ Überprüfen von <Schlüssel und Zertifikat>

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen SIP> ▶ <Einstellungen TLS>.

3 Prüfen Sie, ob der Schlüsselname für <Schlüssel und Zertifikat> erscheint.

Beispielbildschirm:



- Wenn ein Schlüsselname für <Schlüssel und Zertifikat> erscheint, führen Sie die folgenden Schritte aus.
- Wenn der Schlüsselname für <Schlüssel und Zertifikat> nicht erscheint, brauchen Sie die folgenden Schritte nicht auszuführen.

Verwenden von Remote UI

■Überprüfen von [TLS verwenden] und [Schlüssel und Zertifikat]

1 Starten Sie die Remote UI.

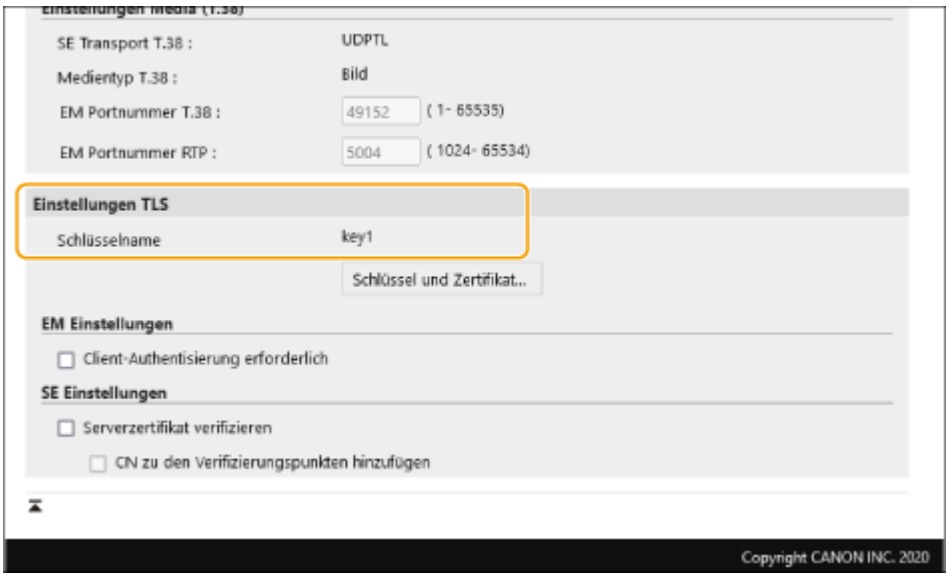
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Einstellungen Netzwerk] ▶ [Einstellungen SIP].

4 Überprüfen Sie [TLS verwenden] unter [Einstellungen Intranet].

- Wenn [TLS verwenden] ausgewählt ist, fahren Sie mit der Prüfung von [Schlüssel und Zertifikat] fort.
- Wenn [TLS verwenden] abgewählt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

5 Überprüfen Sie [Schlüsselname] unter [Einstellungen TLS].



- Wenn ein Schlüsselname erscheint, führen Sie die folgenden Schritte aus.
- Wenn der Schlüsselname nicht erscheint, brauchen Sie die folgenden Schritte nicht auszuführen.

Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für SIP)

Sie können zwei Typen von Zertifikaten für einen mit dem Gerät generierten Schlüssel erzeugen: ein selbstsigniertes Zertifikat-Zertifikat und ein CSR-Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.
Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. In diesem Fall führen Sie die Vorgänge über die Remote UI aus.

Für ein selbstsigniertes Zertifikat(P. 68)
Für ein CSR-Zertifikat(P. 71)

Für ein selbstsigniertes Zertifikat

Verwenden des Bedienfelds(P. 68)
Verwenden von Remote UI(P. 69)

■ Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Schlüssel generieren> ▶ <Netzwerk Kommunikationsschl. generieren>.**

3 **Konfigurieren Sie die erforderlichen Einstellungen, und fahren Sie mit dem nächsten Bildschirm fort.**
Beispielbildschirm:

a <Schlüsselname>

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b <Algorithmus Signatur>

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt. Wenn Sie <RSA> für c wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für d setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

c <Schlüsselalgorithmus>

Wählen Sie den Schlüsselalgorithmus. Wenn Sie <RSA> wählen, erscheint <Schlüssellänge (Bit)> als Einstelloption für d. Wenn Sie <ECDSA> wählen, wird stattdessen <Schlüsseltyp> angezeigt.

d <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für c wählen, oder legen Sie den Schlüsseltyp fest, wenn Sie <ECDSA> wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

4 Konfigurieren Sie die erforderlichen Elemente für das Zertifikat ▶ drücken Sie <Schlüssel gener.>.

Beispielbildschirm:

a <Startdatum Gültigkeit>/<Enddatum Gültigkeit>

Geben Sie das Startdatum und das Enddatum des Gültigkeitszeitraums für das Zertifikat ein.

b <Land/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

Wählen Sie die Landeskennzahl aus der Liste, und geben Sie den Standort und den Namen des Unternehmens an.

c <Allgemeiner Name>

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

■Verwenden von Remote UI

1 Starten Sie die Remote UI.

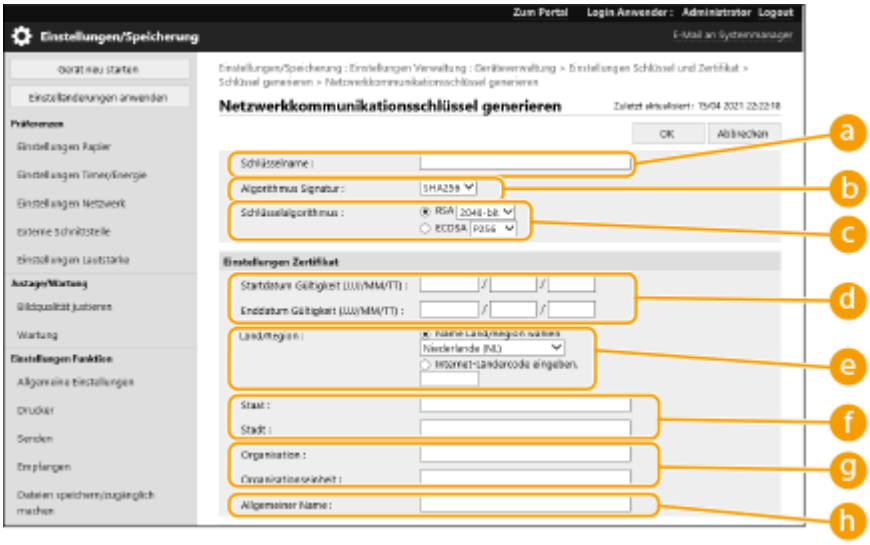
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Netzwerkkommunikation].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a [Schlüsselname]

Geben Sie einen Namen für den Schlüssel in alphanumerischen Zeichen ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den Hash-Algorithmus, der für die Signatur verwendet werden soll. Die verfügbaren Hash-Algorithmen hängen von der Schlüssellänge ab. Bei einer Schlüssellänge von 1024 Bit oder mehr werden die Hash-Algorithmen SHA384 und SHA512 unterstützt.

c [Schlüsselalgorithmus]

Wählen Sie [RSA] oder [ECDSA] als Algorithmus zur Generierung des Schlüssels. Geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen. In beiden Fällen bietet ein höherer Wert mehr Sicherheit, verringert aber die Verarbeitungsgeschwindigkeit der Kommunikation.

HINWEIS:

- Wenn Sie [SHA384] oder [SHA512] für [Algorithmus Signatur] wählen, können Sie die Schlüssellänge nicht auf [512-bit] einstellen, wenn Sie [RSA] für [Schlüsselalgorithmus] wählen.

d [Startdatum Gültigkeit (JJJJ/MM/TT)]/[Enddatum Gültigkeit (JJJJ/MM/TT)]

Geben Sie das Startdatum und Enddatum des Gültigkeitszeitraums für das Zertifikat ein. [Enddatum Gültigkeit (JJJJ/MM/TT)] kann nicht auf ein Datum vor dem Datum in [Startdatum Gültigkeit (JJJJ/MM/TT)] festgelegt werden.

e [Land/Region]

Klicken Sie auf [Name Land/Region wählen], und wählen Sie das Land/die Region aus der Dropdown-Liste. Alternativ können Sie auch auf [Internet-Ländercode eingeben.] klicken und einen Ländercode eingeben, wie beispielsweise "US" für die Vereinigten Staaten.

f [Staat]/[Stadt]

Geben Sie den Standort in alphanumerischen Zeichen ein, sofern erforderlich.

g [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation in alphanumerischen Zeichen ein, sofern erforderlich.

h [Allgemeiner Name]

Geben Sie gegebenenfalls den allgemeinen Namen (Common Name) des Zertifikats ein, und verwenden Sie dabei alphanumerische Zeichen. Der "Common Name" wird häufig mit "CN" abgekürzt.

7 Klicken Sie auf [OK].

- Die Erzeugung eines Schlüssels und eines Zertifikats kann einige Zeit dauern.
- Generierte Schlüssel und Zertifikate werden automatisch auf dem Gerät registriert.

Für ein CSR-Zertifikat

Generieren Sie einen Schlüssel und eine Zertifizierungsanforderung (CSR) auf dem Gerät. Verwenden Sie die auf dem Bildschirm angezeigten oder in eine Datei ausgegebenen CSR-Daten, um die Zertifizierungsstelle zur Ausstellung eines Zertifikats aufzufordern. Registrieren Sie dann das ausgestellte Zertifikat für den Schlüssel.
Sie können diese Einstellung nur über die Remote UI konfigurieren.

■1. Generieren eines Schlüssels und einer CSR

1 Starten Sie die Remote UI.

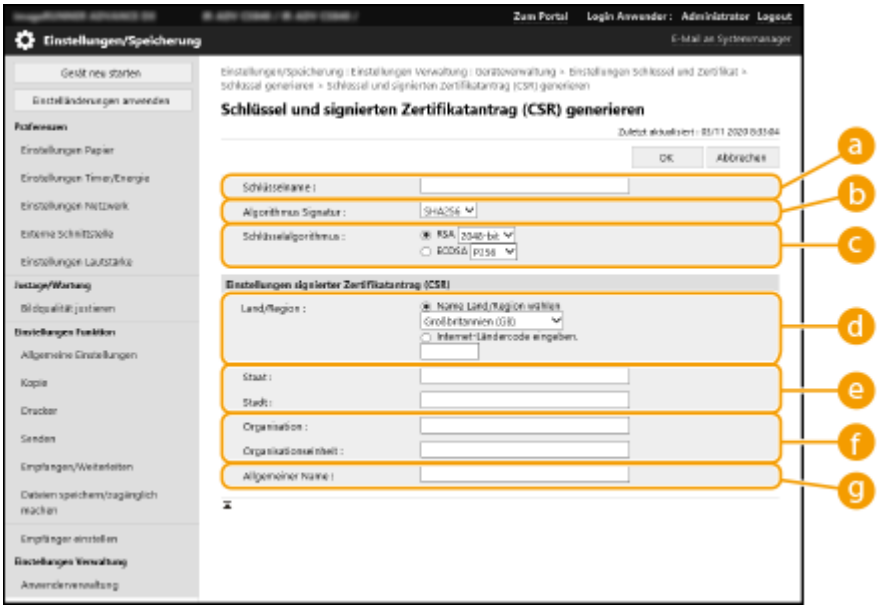
2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie auf [Schlüssel generieren].

5 Klicken Sie auf [Schlüssel und signierter Zertifikatantrag (CSR)].

6 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.



a **[Schlüsselname]**

Geben Sie einen Namen für den Schlüssel ein. Geben Sie einen Namen ein, der in einer Liste leicht zu finden ist.

b [Algorithmus Signatur]

Wählen Sie den für die Signatur zu verwendenden Hash-Algorithmus.

c [Schlüsselalgorithmus]

Wählen Sie den Schlüsselalgorithmus aus, und geben Sie die Schlüssellänge an, wenn Sie [RSA] wählen, oder geben Sie den Schlüsseltyp an, wenn Sie [ECDSA] wählen.

d [Land/Region]

Wählen Sie den Ländercode aus der Liste, oder geben Sie ihn direkt ein.

e [Staat]/[Stadt]

Geben Sie den Standort ein.

f [Organisation]/[Organisationseinheit]

Geben Sie den Namen der Organisation ein.

g [Allgemeiner Name]

Geben Sie die IP-Adresse oder FQDN ein.

- Wenn IPPS-Druck in einer Windows-Umgebung durchgeführt wird, geben Sie die IP-Adresse des Geräts ein.
- Für die Eingabe des FQDN des Geräts ist ein DNS-Server erforderlich. Wenn Sie keinen DNS-Server verwenden, geben Sie die IP-Adresse des Geräts ein.

7 Klicken Sie auf [OK].

➠ Die CSR-Daten werden angezeigt.

- Wenn Sie die CSR-Daten in einer Datei speichern möchten, klicken Sie auf [In Datei speichern], und legen Sie den Speicherort fest.

HINWEIS:

- Der Schlüssel, der die CSR generiert hat, wird auf dem Schlüssel- und- Zertifikatlistenbildschirm angezeigt, jedoch können Sie den Schlüssel selbst nicht verwenden. Um diesen Schlüssel zu verwenden, müssen Sie das Zertifikat registrieren, das später auf der Grundlage der CSR ausgestellt wird.

8 Fordern Sie die Zertifizierungsstelle auf, ein Zertifikat auf der Grundlage der CSR-Daten auszustellen.

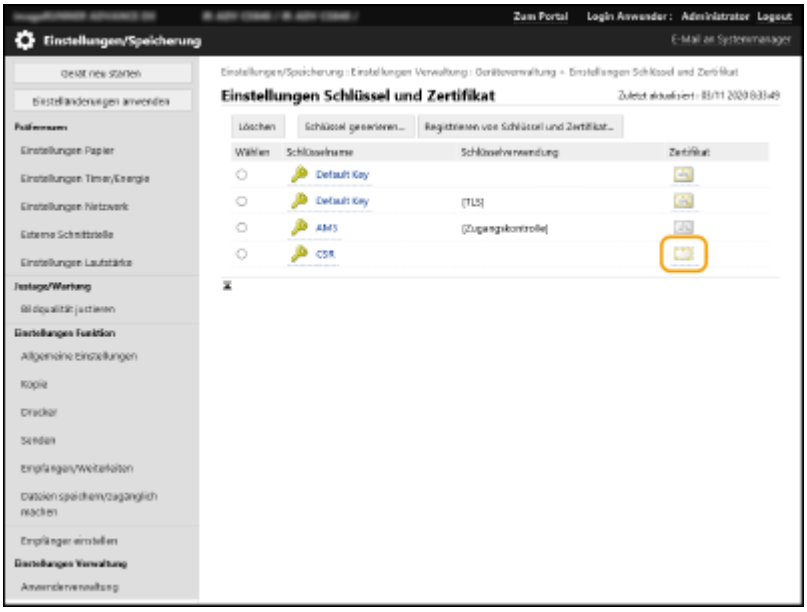
■2. Registrieren des ausgestellten Zertifikats für den Schlüssel

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].

4 Klicken Sie in der Liste [Zertifikat] auf für das Zertifikat, das Sie registrieren möchten.



5 Klicken Sie auf [Zertifikat speichern...].

6 Registrieren Sie das Zertifikat.

- Klicken Sie auf [Durchsuchen...] ▶ geben Sie die zu registrierende Datei (Zertifikat) an ▶ klicken Sie auf [Speichern].

Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für SIP)

Legen Sie den generierten Schlüssel und das Zertifikat als Schlüssel und Zertifikat für die TLS-verschlüsselte Kommunikation von SIP fest.

Verwenden des Bedienfelds(P. 74)
Verwenden von Remote UI(P. 75)

■Verwenden des Bedienfelds

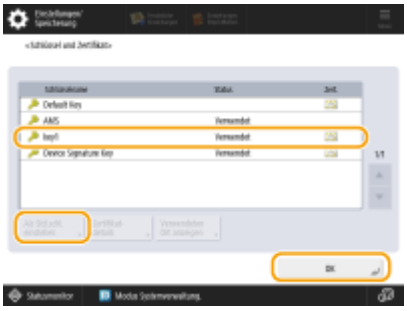
1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Präferenzen> ▶ <Netzwerk> ▶ <Einstellungen TCP/IP> ▶ <Einstellungen SIP> ▶ <Einstellungen TLS>.**

3 **Konfigurieren Sie die verschiedenen Einstellungen unter <EM Einstellungen> und <SE Einstellungen> ▶ drücken Sie <Schlüssel und Zertifikat>.**
Beispielbildschirm:

<EM Einstellungen>	
<Client-Authentisierung erforderlich>	Wählen Sie <Ein> oder <Aus>. Wenn Sie <Ein> wählen, fordert das Gerät beim Empfang eines IP-Faxes eine Client-Authentifizierung an.
<SE Einstellungen>	
<Serverzertifikat verifizieren>	Wählen Sie <Ein> oder <Aus>. Wenn Sie <Ein> wählen, prüft das Gerät beim Empfang eines IP-Faxes, ob das TLS-Serverzertifikat gültig ist.
<CN verifizieren>	Wählen Sie <Ein> oder <Aus>. Wenn Sie <Ein> wählen, prüft das Gerät beim Empfang eines IP-Faxes den CN (allgemeinen Namen).

4 **Wählen Sie den Schlüssel und das Zertifikat für die TLS-verschlüsselte Kommunikation von SIP aus ▶ drücken Sie <Als Std.schl. einstellen> ▶ <OK>.**
Beispielbildschirm:



HINWEIS

- Sie können den Schlüssel und das Zertifikat nicht auswählen, wenn deren Status "Verwendet" ist.
- Sie können <Zertifikat details> drücken, um detaillierte Informationen über das Zertifikat zu prüfen.
- Sie können <Verwendeten Ort anzeigen> drücken, um die Verwendung des Schlüssels/Zertifikats zu überprüfen.

5 **Drücken Sie <OK>.**

6 **Drücken Sie (Einstell./Speicherung) ▶ (Einstell./Speicherung) ▶ <Einstelländerungen anwenden> ▶ <Ja>.**

➠ Das Gerät startet neu und übernimmt die Einstellungen.

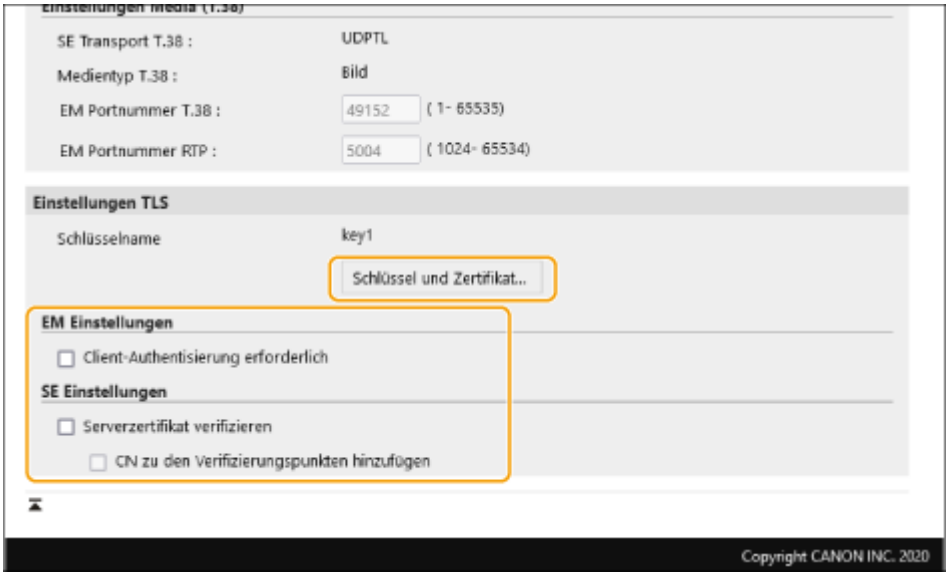
■ Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].**

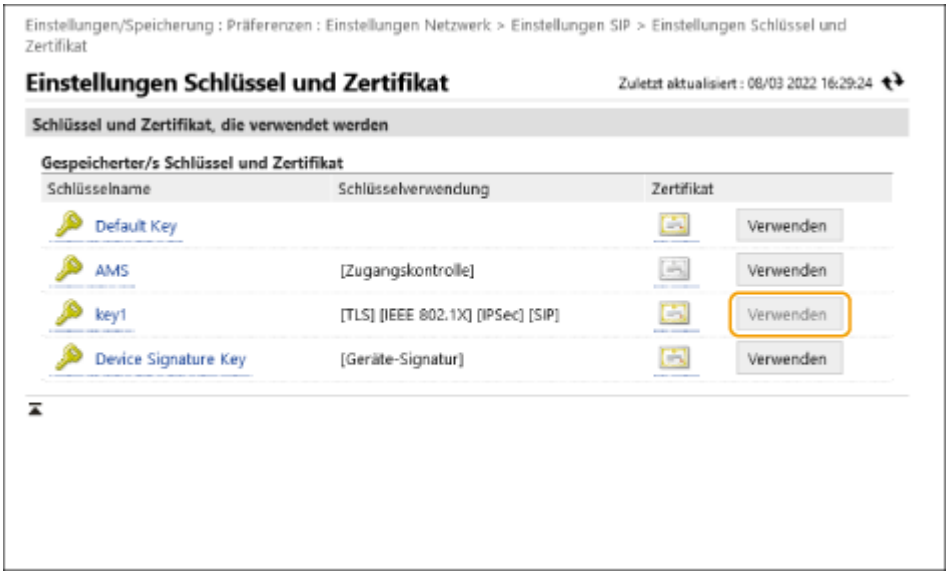
3 **Klicken Sie auf [Einstellungen Netzwerk] ▶ [Einstellungen SIP].**

4 **Konfigurieren Sie die verschiedenen Einstellungen unter [Einstellungen TLS] ▶ klicken Sie auf [Schlüssel und Zertifikat].**



[EM Einstellungen]	
[Client-Authentisierung erforderlich]	Wenn Sie dieses Kontrollkästchen aktivieren, fordert das Gerät beim Empfang eines IP-Faxes eine Client-Authentifizierung an.
[SE Einstellungen]	
[Serverzertifikat verifizieren]	Wenn Sie dieses Kontrollkästchen aktivieren, prüft das Gerät beim Empfang eines IP-Faxes, ob das TLS-Serverzertifikat gültig ist.
[CN zu den Verifizierungspunkten hinzufügen]	Wählen Sie [Ein] oder [Aus]. Wenn Sie dieses Kontrollkästchen aktivieren, überprüft das Gerät beim Empfang eines IP-Faxes den CN (allgemeinen Namen).

5 Klicken Sie auf [Verwenden] für den zu verwendenden Schlüssel in der Liste.



6 Klicken Sie auf [OK].

7 Klicken Sie auf [Einstelländerungen anwenden], um das Gerät neu zu starten.

➠ Das Gerät startet neu und übernimmt die Einstellungen.

Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für SIP)

Je nach Modell Ihres Geräts können Sie möglicherweise keine Vorgänge über das Bedienfeld ausführen. Führen Sie in diesem Fall die Vorgänge über Remote UI aus.

HINWEIS

- Möglicherweise müssen Sie der Zertifizierungsstelle beim Deaktivieren des Zertifikats einige Informationen übermitteln. Schauen Sie unter **Prüfen, ob Sie weitere Verfahren durchführen müssen(P. 5)** nach, und notieren Sie sich die erforderlichen Informationen, bevor Sie den Schlüssel/das Zertifikat löschen.

Verwenden des Bedienfelds(P. 77)
Verwenden von Remote UI(P. 78)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Liste Schlüssel und Zertifikat> ▶ <Schlüsselu. Zertifikatsliste für d.Gerät>.**

- <Schlüsselu. Zertifikatsliste für d.Gerät> wird nur angezeigt, wenn die Benutzersignaturfunktion auf dem Gerät aktiviert ist. In diesem Fall fahren Sie mit dem nächsten Schritt fort.

3 **Wählen Sie den Schlüssel und das Zertifikat ▶ drücken Sie <Löschen> ▶ <Ja>.**

Beispielbildschirm:

HINWEIS:

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn nicht erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Wenn Sie einen Schlüssel und ein Zertifikat auswählen und dann <Zertifikat details> drücken, erscheinen detaillierte Informationen über das Zertifikat. Sie können auch <Zert. verifiz.> auf diesem Bildschirm drücken, um zu prüfen, ob das Zertifikat gültig ist.

■Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstell./Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].**

4 **Wählen Sie den Schlüssel und das Zertifikat ▶ klicken Sie auf [Löschen] ▶ [OK].**

HINWEIS

- Wenn erscheint, ist der Schlüssel beschädigt oder ungültig.
- Wenn erscheint, ist kein Zertifikat für den Schlüssel vorhanden.
- Klicken Sie auf einen Schlüsselnamen, um detaillierte Informationen zu dem Zertifikat anzuzeigen. Sie können auch auf [Zertifikat verifizieren] auf diesem Bildschirm klicken, um zu überprüfen, ob das Zertifikat gültig ist.

Schritt 5: Deaktivieren des Zertifikats (für SIP)

Deaktivieren Sie ein in der Vergangenheit erstelltes Zertifikat. Das Verfahren unterscheidet sich je nach Zertifikatstyp.

■ Für ein selbstsigniertes Zertifikat

Wenn ein Zertifikat mit enthaltenem Schlüssel, das zusätzliche Verfahren erfordert, auf einem anderen IP-Faxgerät als vertrauenswürdiges Zertifikat registriert ist, löschen Sie das registrierte Zertifikat. Nach dem Löschen des registrierten Zertifikats registrieren Sie das Zertifikat des neu generierten Schlüssels.

■ Für ein CSR-Zertifikat

Fordern Sie die Zertifizierungsstelle auf, die das Zertifikat ausgestellt hat, das Zertifikat zu widerrufen. Die zuständige Zertifizierungsstelle finden Sie unter [Aussteller] im Zertifikat.

HINWEIS

- Wenn Sie den Widerruf von Zertifikaten mithilfe eines anderen IP-Geräts überprüfen, registrieren Sie die aktualisierte CRL auf dem Computer oder Webbrowser, nachdem das Zertifikat widerrufen wurde.
- Wenn Sie eine andere Methode als eine CRL (beispielsweise OCSP) zur Überprüfung des Zertifikatswiderrufs verwenden, führen Sie das Verfahren für diese Methode durch.

Schritt 6: Aktivieren des neuen Zertifikats (für SIP)

Aktivieren Sie das Zertifikat.

■ Für ein selbstsigniertes Zertifikat

Registrieren Sie das neue Zertifikat auf dem anderen IP-Faxgerät als vertrauenswürdiges Zertifikat.

■ Für ein CSR-Zertifikat

Sie brauchen die zusätzlichen Verfahren nicht durchzuführen.

Verfahren für Gerätesignaturen

Schritt 1: Überprüfen der S/MIME-Einstellungen (für Gerätesignaturen)

Prüfen Sie, ob Sie die zusätzlichen Verfahren für S/MIME und die Gerätesignaturen durchführen müssen.

Befolgen Sie den nachstehenden Ablauf zur Überprüfung der S/MIME-Einstellungen.

Verwenden des Bedienfelds(P. 82)
Verwenden von Remote UI(P. 82)

■Verwenden des Bedienfelds

1 Drücken Sie (Einstell./Speicherung).

2 Drücken Sie <Einstellungen Funktion> ▶ <Senden> ▶ <Einstellungen E-Mail/I-Fax> ▶ <Einstellungen S/MIME>.

3 Überprüfen Sie <Einstellungen Verschlüsselung> und <Digitale Signaturen hinzu>.

Beispielbildschirm:

- Wenn <Einstellungen Verschlüsselung> auf <Nicht verschlüsseln> und <Digitale Signaturen hinzu> auf <Aus> gesetzt sind, führen Sie die folgenden Verfahren nur für die Gerätesignaturen durch.
- Wenn andere Einstellungen festgelegt sind, führen Sie die folgenden Verfahren sowohl für S/MIME als auch für die Gerätesignaturen durch.

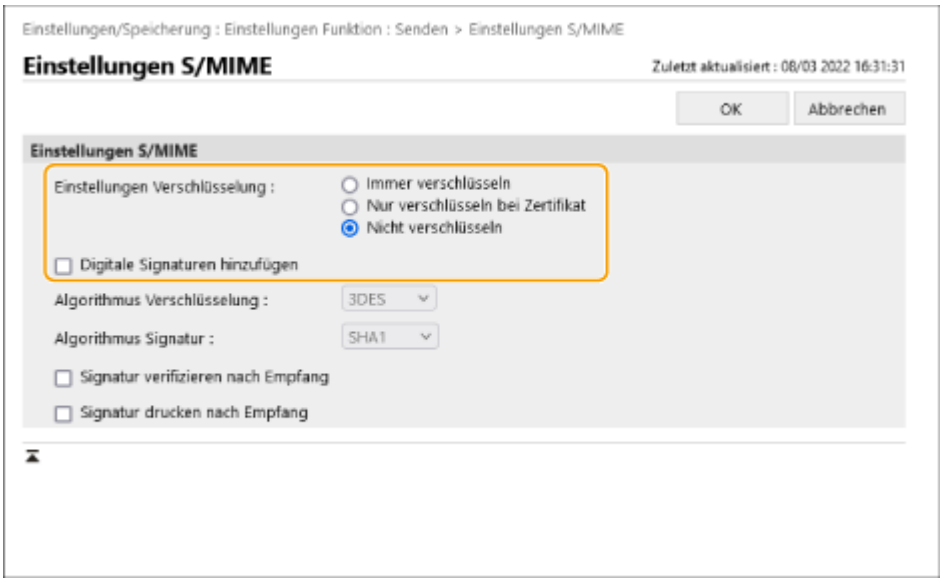
■Verwenden von Remote UI

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Senden] ▶ [Einstellungen S/MIME].

4 Überprüfen Sie [Einstellungen Verschlüsselung] und [Digitale Signaturen hinzufügen].



- Wenn [Nicht verschlüsseln] für [Einstellungen Verschlüsselung] und [Digitale Signaturen hinzufügen] ausgewählt ist, führen Sie die folgenden Verfahren nur für die Gerätesignaturen durch.
- Wenn andere Einstellungen festgelegt sind, führen Sie die folgenden Verfahren sowohl für S/MIME als auch für die Gerätesignaturen durch.

Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für Gerätesignaturen)

Verwenden des Bedienfelds(P. 84)
Verwenden von Remote UI(P. 84)

■Verwenden des Bedienfelds

1 **Drücken Sie (Einstell./Speicherung).**

2 **Drücken Sie <Einstellungen Verwaltung> ▶ <Geräteverwaltung> ▶ <Einstellungen Zertifikat> ▶ <Schlüssel generieren>.**

3 **Drücken Sie <Schlüssel Geräte-Signatur generierieren/aktualisier.> ▶ <Ja> ▶ <OK>.**

■Verwenden von Remote UI

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen Schlüssel und Zertifikat].**

4 **Klicken Sie auf [Schlüssel generieren] ▶ [Geräte-Signatur].**

5 **Klicken Sie auf [Generieren/Aktualisieren] ▶ [OK].**

Schritt 3: Deaktivieren des Zertifikats (für Gerätesignaturen)

Deaktivieren Sie ein in der Vergangenheit erstelltes Zertifikat.

■Wenn ein Zertifikat für Gerätesignaturen in Acrobat registriert ist

Wenn ein Zertifikat für Gerätesignaturen in Acrobat registriert ist, löschen Sie das registrierte Zertifikat.

■Wenn ein von diesem Gerät exportiertes S/MIME-Zertifikat in ein anderes Gerät importiert wurde

Wenn Sie das öffentliche Schlüsselzertifikat (S/MIME-Zertifikat), das für die Verschlüsselung von E-Mails/Faxen über S/MIME verwendet wird, aus diesem Gerät exportiert und das Zertifikat in ein anderes Gerät importiert haben, gehen Sie wie folgt vor, um das Zertifikat von dem Gerät zu löschen, in welches das Zertifikat importiert wurde.

1 **Starten Sie die Remote UI.**

2 **Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].**

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen S/MIME Zertifikat].**

4 **Wählen Sie das zugehörige Zertifikat ▶ klicken Sie auf [Löschen] ▶ [OK].**

Schritt 4: Aktivieren des neuen Zertifikats (für Gerätesignaturen)

Aktivieren Sie das Zertifikat.

■Wenn ein Zertifikat für Gerätesignaturen in Acrobat registriert ist

Wenn ein Zertifikat für Gerätesignaturen in Acrobat registriert ist, exportieren Sie das regenerierte Zertifikat für Gerätesignaturen, und registrieren Sie das neue Zertifikat in Acrobat.

Exportieren des Zertifikats aus dem Gerät(P. 86)

■Wenn ein von diesem Gerät exportiertes S/MIME-Zertifikat in ein anderes Gerät importiert wurde

Wenn Sie das öffentliche Schlüsselzertifikat (S/MIME-Zertifikat), das für die Verschlüsselung von E-Mail/Faxen über S/MIME verwendet wird, aus diesem Gerät exportiert und das Zertifikat in ein anderes Gerät importiert haben, exportieren Sie das neu generierte Zertifikat, und registrieren Sie es auf dem anderen Gerät.

Exportieren des Zertifikats aus dem Gerät(P. 86)
Registrieren des Zertifikats für das andere Gerät(P. 86)

■Exportieren des Zertifikats aus dem Gerät

Gehen Sie wie folgt vor, um das Zertifikat zu exportieren.

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 Klicken Sie auf [Geräteverwaltung] ▶ [Geräte-Signatur exportieren].

4 Klicken Sie auf [Exportstart] ▶ speichern Sie die Datei an einem Ort Ihrer Wahl.

■Registrieren des Zertifikats für das andere Gerät

Gehen Sie wie folgt vor, um das Zertifikat auf dem anderen Gerät zu registrieren.

1 Starten Sie die Remote UI.

2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].

3 **Klicken Sie auf [Geräteverwaltung] ▶ [Einstellungen S/MIME Zertifikat].**

4 **Klicken Sie auf [S/MIME Zertifikat speichern].**

5 **Registrieren Sie ein S/MIME-Zertifikat.**

- Klicken Sie auf [Durchsuchen...] ▶ geben Sie die zu registrierende Datei (S/MIME-Zertifikat) an ▶ klicken Sie auf [Speichern].

Zusätzliche Verfahren für Bluetooth-Einstellungen

Zusätzliche Verfahren für Bluetooth-Einstellungen

Der Schlüssel für Bluetooth wird nach der Aktualisierung der Firmware des Geräts automatisch aktualisiert. Wenn Sie die Canon PRINT Business App für Mobilgeräte verwenden, müssen Sie das Gerät erneut registrieren.

Verfahren für Bluetooth(P. 90)

Verfahren für Bluetooth

Schritt 1: Löschen des in Canon PRINT Business registrierten Geräts (für Bluetooth)

Wenn Bluetooth auf <Ein> gesetzt ist, gehen Sie wie folgt vor.

Vorgehensweise bei iOS(P. 91)
Vorgehensweise bei Android(P. 91)

■Vorgehensweise bei iOS

1 Tippen Sie oben links auf dem Startbildschirm von Canon PRINT Business auf [ ].

Der Bildschirm [Drucker ausw.] wird angezeigt.

2 Löschen Sie das Gerät aus der Liste, indem Sie auf [ ] ▶ [Löschen] tippen.

■Vorgehensweise bei Android

1 Tippen Sie oben links auf dem Startbildschirm von Canon PRINT Business auf [ ].

Der Bildschirm [Drucker ausw.] wird angezeigt.

2 Drücken Sie etwas länger auf den Gerätenamen ▶ tippen Sie im angezeigten Dialogfeld auf [Löschen].

Schritt 2: Erneutes Registrieren des Geräts bei Canon PRINT Business (für Bluetooth)

Wenn Bluetooth auf <Ein> gesetzt ist, gehen Sie wie folgt vor.

Vorgehensweise bei iOS(P. 92)
Vorgehensweise bei Android(P. 92)

■Vorgehensweise bei iOS

1 Tippen Sie oben links auf dem Startbildschirm von Canon PRINT Business auf [ ].

Der Bildschirm [Drucker ausw.] wird angezeigt.

2 Tippen Sie auf [Drucker in der Nähe].

Die erkannten Geräte werden angezeigt.

■Wenn Geräte nicht erkannt werden

Gehen Sie näher an das Gerät heran, und tippen Sie auf [Suchen]. Bluetooth kann Geräte in einer Entfernung von bis zu 2 Metern oder 80 Zoll erkennen.

3 Wählen Sie das Gerät ▶ tippen Sie auf [Hinzufügen].

■Vorgehensweise bei Android

1 Tippen Sie oben links auf dem Startbildschirm von Canon PRINT Business auf [ ].

Der Bildschirm [Drucker ausw.] wird angezeigt.

2 Tippen Sie auf [Drucker in der Nähe].

Die erkannten Geräte werden angezeigt.

■Wenn Geräte nicht erkannt werden

Gehen Sie näher an das Gerät heran, und tippen Sie auf [Suchen]. Bluetooth kann Geräte in einer Entfernung von bis zu 2 Metern oder 80 Zoll erkennen.

3 Wählen Sie das Gerät aus.

4 Überprüfen Sie die Geräteinformationen im angezeigten Dialogfeld ▶ tippen Sie auf [Hinzufügen].

Wenn der Bildschirm für die Wi-Fi-Netzwerkeinstellungen angezeigt wird, befolgen Sie die Anweisungen auf dem Bildschirm.

Zusätzliche Verfahren für die Einstellungen des Zugangsverwaltungssystems

Zusätzliche Verfahren für die Einstellungen des Zugangsverwaltungssystems

Der Schlüssel für das Zugangsverwaltungssystem wird nach der Aktualisierung der Firmware des Geräts automatisch aktualisiert.

Die Einschränkungsinformationen werden etwa 30 Minuten nach der automatischen Aktualisierung des Schlüssels automatisch wieder abgerufen. Das Drucken kann dann ganz normal mit der Zugangsverwaltungssystemfunktion durchgeführt werden.

Wenn Sie unmittelbar nach der Aktualisierung der Firmware mit der Zugangsverwaltungssystemfunktion des Druckertreibers drucken möchten, müssen Sie die Einschränkungsinformationen des Zugangsverwaltungssystems erneut manuell abrufen.

Verfahren für das Zugangsverwaltungssystem(P. 95)

Ein Fehler tritt auf, wenn Sie versuchen zu drucken, ohne die Einschränkungsinformationen erneut abzurufen.

Verfahren für das Zugangsverwaltungssystem

Wenn Sie unmittelbar nach der Aktualisierung der Firmware mit der Zugangsverwaltungssystemfunktion des Druckertreibers drucken möchten, müssen Sie die Einschränkungsinformationen des Zugangsverwaltungssystems manuell abrufen.

Gehen Sie dazu wie folgt vor.

Das nachstehende Verfahren ist etwa 30 Minuten nach der Aktualisierung der Firmware nicht mehr erforderlich, da die Einschränkungsinformationen zu diesem Zeitpunkt bereits automatisch abgerufen worden sind.

1 Melden Sie sich am Computer an.

2 Öffnen Sie die Eigenschaften des Druckers, der mit dem Druckertreiber verwendet werden soll, bei dem die Zugangsverwaltungssystemfunktion aktiviert ist.

■Für Windows Vista

- Klicken Sie auf [Start] ▶ [Systemsteuerung] ▶ [Hardware und Sound] ▶ wählen Sie [Drucker].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Eigenschaften] aus.

■Für Windows Server 2008

- Klicken Sie auf [Start] ▶ [Systemsteuerung] ▶ [Hardware und Sound] ▶ wählen Sie [Drucker].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Eigenschaften] aus.

■Für Windows Server 2008 R2

- Klicken Sie auf [Start] ▶ [Systemsteuerung] ▶ [Hardware] ▶ wählen Sie [Geräte und Drucker].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Druckereigenschaften] aus.

■Für Windows 7

- Klicken Sie auf [Start] ▶ [Systemsteuerung] ▶ [Hardware und Sound] ▶ wählen Sie [Geräte und Drucker].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Druckereigenschaften] aus.

■Für Windows 8.1/Windows Server 2012

- Navigieren Sie zum Desktop, und öffnen Sie die Charms auf der rechten Seite des Bildschirms.
- Klicken Sie auf [Einstellungen] ▶ [Systemsteuerung] ▶ wählen Sie [Geräte und Drucker anzeigen].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Druckereigenschaften] aus.

■Für Windows 10/Windows Server 2016

- Rechtsklicken Sie auf [Start] ▶ wählen Sie [Systemsteuerung] ▶ [Geräte und Drucker anzeigen].
- Klicken Sie mit der rechten Maustaste auf das Druckersymbol ▶ wählen Sie [Druckereigenschaften] aus.

3 Klicken Sie auf die Registerkarte [AMS].

4 Klicken Sie auf [Beschränkungsinformationen abrufen].

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.