

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

USRM3-1249-02 2022-07 de

Copyright CANON INC. 2022

Inhalt

üfen, ob Sie weitere Verfahren durchführen müssen	
erwenden von RSA-Schlüsseln und zusätzliche Verfahren	
Verfahren für TLS	13
Schritt 1: Neugenerieren des Schlüssels und des Zertifikats (für TLS)	14
Schritt 2: Zurücksetzen des Schlüssels und des Zertifikats (für TLS)	22
Schritt 3: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für TLS)	
Schritt 4: Deaktivieren des Zertifikats (für TLS)	
Schritt 5: Aktivieren des neuen Zertifikats (für TLS)	
Verfahren für IEEE 802.1X	28
Schritt 1: Überprüfen der Authentifizierungsmethode (für IEEE 802.1X)	
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IEEE 802.1X)	
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IEEE 802.1X)	
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IEEE 802.1X)	4
Schritt 5: Deaktivieren des Zertifikats (für IEEE 802.1X)	
Schritt 6: Aktivieren des neuen Zertifikats (für IEEE 802.1X)	4
Verfahren für IPSec	4
Schritt 1: Überprüfen der Authentifizierungsmethode (für IPSec)	
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IPSec)	4
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IPSec)	5
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IPSec)	6
Schritt 5: Deaktivieren des Zertifikats (für IPSec)	6
Schritt 6: Aktivieren des neuen Zertifikats (für IPSec)	63
Verfahren für SIP	64
Schritt 1: Überprüfen der Einstellungen (für SIP)	6
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für SIP)	6
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für SIP)	
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für SIP)	7
Schritt 5: Deaktivieren des Zertifikats (für SIP)	
Schritt 6: Aktivieren des neuen Zertifikats (für SIP)	8
Verfahren für Gerätesignaturen	8
Schritt 1: Überprüfen der S/MIME-Einstellungen (für Gerätesignaturen)	
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für Gerätesignaturen)	84
Schritt 3: Deaktivieren des Zertifikats (für Gerätesignaturen)	8
Schritt 4: Aktivieren des neuen Zertifikats (für Gerätesignaturen)	8

Schritt 1: Löschen des in Canon PRINT Business registrierten Geräts (für Bluetooth)	. 91
Schritt 2: Erneutes Registrieren des Geräts bei Canon PRINT Business (für Bluetooth)	. 92

Zusätzliche Verfahren für die Einstellungen des Zugangsverwaltungssystems

Zugangsverwaltungssystems	94
Verfahren für das Zugangsverwaltungssystem	95

Vorwort

/orwort

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.

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	Ver. 59.39 bis Ver. 67.30
- 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	
- iR-ADV 4545 III / 4535 III / 4525 III	Ver. 29.39 bis Ver. 37.30
- iR-ADV 715 III / 615 III / 525 III	
- iR-ADV 6575 III / 6565 III / 6560 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	
- iR-ADV 4725 / 4735 / 4745	Ver. 17.44 bis Ver. 27.30
- iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B	

Modelle	Versionen
- iR-ADV C3730 / C3720	
- iR-ADV C7780 / C7770 / C7765	
- iR-ADV C357	Ver. 19.34 bis Ver. 27.30
- iR-ADV C477	
- 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	Ver. 200.0.301 bis Ver. 309.0.405
- iR C1533 / C1538	
- LBP720Cx / LBP722Cx / LBP722Ci / LBP722Cdw	Ver. 114.0.301 bis Ver. 309.0.405
- C1533P / C1538P	
- 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		5
---	--	---

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.

OÜberprüfen des RSA-Schlüssels(P. 5)

OÜberprüfen der Bluetooth-Einstellungen(P. 8)

ÖÜberprüfen 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>.
- Prücken 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:

Dicarlanger'	bradalite Bradalite Bradalite	
state Schloael and Zettillation		
Salvasahume	Bake	34
🔑 Default Kity		22 C
AMR 4	Reviework (M	
JP 861	Norwordet	a)
veriet signesite ets	NOTWONOD:	10
		A
		w.
Jorifikać jižučen	Veneendeter Ort.anotypen	
		× ,/
🖶 Statumentor 🛛 🔯 Modus	johnvewaltang.	Ð

5 Prüfen Sie <Öffentlicher Schlüssel>.

Beispielbildschirm:

Veste	+ 3.50%5	
 Seriennummer 	* 80	Alt +
 Algorithmus Signatur 	SRA256-858	
 Ausgednit: far 	+ CoP	Ale »
 Sarbleum Solliyaot. 	* 31/12 2021	
 Enddatum Gältigkeit 	 31/12 2023 	
 Austeiler 	= C-#	Ale +
 diferciater tubicari 	+ ISA 20482	
 3y/Mad Thursgoint 		Anarigen y
 Association (A), Name 		Alt +

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.

🔓 Drücken Sie <Verwendeten Ort anzeigen> 🕨 überprüfen Sie die Verwendung des Schlüssels.

Beispielbildschirm:

Silvieulrume	Dates	366
🔑 Default Kity		2
JAM &	Review/of	
,≥ as1	Norwordet	
Provest supresses was	NOTWONDED.	121
rifikul jühchen	Veneendeder Ort.anotypen	

Führen Sie die zusätzlichen Verfahren gemäß den folgenden Angaben durch. OVerwenden 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].

Löschen	Schlüssel generieren	Registrieren von Schlüssel und Zertifikat	
Wählen	Schlüsselname	Schlüsselverwendung	Zertifikat
0	🔎 Default Key		
0	🔎 AMS	[Zugangskontrolle]	
0	🔎 kœy1	[TLS] (IEEE 802.1X) [IPSec] [SIP	
0	🔎 Device Signature Key	[Geräte-Signatur]	C 5

3 Überprüfen Sie [Öffentlicher Schlüssel].

zinstellungen/speicherung : Einstellungen Zertifikatdetails	verwartung : Gerateverwartung > Einste	nungen schlussel	und zeroniat >
Einstellungen Schlüssel un	d Zertifikat	Zuletzt aktu	alisiert : 08/03 2022 16:34:5
			Zertifikat verifizieren
Zertifikatdetails			
Version :	X.509v3		
Seriennummer :	00		
Algorithmus Signatur :	sha256RSA		
Ausgestellt für :	C=JP		
Startdatum Gültigkeit :	31/12/2021		
Enddatum Gültigkeit :	31/12/2023		
Aussteller :	C=JP		
Öffentlicher Schlüssel :	RSA 2048Bit		
Zertifikat Thumbprint :	ED18 8EF8 EA2E 796E 3108 6644 ECE	06 2018 ABAD 4C8	7
Ausgestellt an (Alternativer Name) :			

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

Prüfen, ob Sie weitere Verfahren durchführen müssen

• 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
 - 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. Szusätzliche
 Verfahren für Bluetooth-Einstellungen(P. 89)
- Wenn <Bluetooth verwenden> auf <Aus> gesetzt ist, brauchen Sie die folgenden Schritte nicht auszuführen.

■ Verwenden von Remote UI

- 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. <a>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. ^OZusätzliche 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

- Starten Sie die Remote UI.
- **2** Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].
- **3** Klicken Sie auf [Lizenz/Andere] **>** [Einstellungen ACCESS MANAGEMENT SYSTEM].

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	12
Verfahren für TLS	13
Schritt 1: Neugenerieren des Schlüssels und des Zertifikats (für TLS)	14
Schritt 2: Zurücksetzen des Schlüssels und des Zertifikats (für TLS)	22
Schritt 3: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für TLS)	24
Schritt 4: Deaktivieren des Zertifikats (für TLS)	26
Schritt 5: Aktivieren des neuen Zertifikats (für TLS)	27
Verfahren für IEEE 802.1X	28
Schritt 1: Überprüfen der Authentifizierungsmethode (für IEEE 802.1X)	29
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IEEE 802.1X)	31
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IEEE 802.1X)	39
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IEEE 802.1X)	42
Schritt 5: Deaktivieren des Zertifikats (für IEEE 802.1X)	44
Schritt 6: Aktivieren des neuen Zertifikats (für IEEE 802.1X)	45
Verfahren für IPSec	46
Schritt 1: Überprüfen der Authentifizierungsmethode (für IPSec)	47
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IPSec)	49
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IPSec)	57
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IPSec)	60
Schritt 5: Deaktivieren des Zertifikats (für IPSec)	62
Schritt 6: Aktivieren des neuen Zertifikats (für IPSec)	63
Verfahren für SIP	64
Schritt 1: Überprüfen der Einstellungen (für SIP)	65
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für SIP)	68
Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für SIP)	74
Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für SIP)	77
Schritt 5: Deaktivieren des Zertifikats (für SIP)	79
Schritt 6: Aktivieren des neuen Zertifikats (für SIP)	80
Verfahren für Gerätesignaturen	81
Schritt 1: Überprüfen der S/MIME-Einstellungen (für Gerätesignaturen)	82
Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für Gerätesignaturen)	84

Schritt 3: Deaktivieren des Zertifikats (für Gerätesignaturen)	85
Schritt 4: Aktivieren des neuen Zertifikats (für Gerätesignaturen)	86

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.	SVerfahren für TLS(P. 13)
IEEE 802.1X	Sie müssen die zusätzlichen Verfahren durchführen, wenn die IEEE 802.1X-Authentifizierungsmethode auf EAP-TLS eingestellt ist.	Overfahren für IEEE 802.1X(P. 28)
IPSec	Sie müssen die zusätzlichen Verfahren durchführen, wenn die IKE- Authentifizierungsmethode auf die digitale Signaturmethode eingestellt ist.	OVerfahren für IPSec(P. 46)
SIP	Sie müssen die zusätzlichen Verfahren durchführen, wenn TLS verwendet wird.	SVerfahren 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 	Overfahren 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)(P. 14)
- Schritt 2: Zurücksetzen des Schlüssels und des Zertifikats (für TLS)(P. 22)
- Schritt 3: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für TLS)(P. 24)
- Schritt 4: Deaktivieren des Zertifikats (für TLS)(P. 26)
- Schritt 5: Aktivieren des neuen Zertifikats (für TLS)(P. 27)

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

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:



60 <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 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 🕝 wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für 🕝 setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

🧿 <Schlüsselalgorithmus>

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

📵 <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für 🧿 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 f ür das Zertifikat h dr ücken Sie Schl üssel gener.>.

Beispielbildschirm:



63<Startdatum Gültigkeit>/<Enddatum Gültigkeit>

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

Cand/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

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

🔁 <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

- Starten Sie die Remote UI.
- 2 Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].
- 4 Klicken Sie auf [Schlüssel generieren].
- 5 Klicken Sie auf [Netzwerkkommunikation].

5 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.

		Zum Pertal	Login Anwender: Ad	ministrator Logout
Einstellungen/Speicherung				i an Systemnanage
Gorat neu starten	Einstellungen/Speicherung : Einstellungen	Verwillung : Gerikterwillung > Ein	stellungen Schlüssel und	Zerffkat >
Einstellanderungen anwenden	Netzwerkkommunikation	schlüssel generieren	Zaletzt ektoelisiert:	15/04 2021 22:22:18
Tällenerupen		,	CK	Althorhom
Antiellungen Rapier	(- Sh	Harristen
Gintfell ungen Timer/Energie	Schlüsseiname :			
Einstell ungen Netzwerk	Algorithmus Signatur :	3HA256 Y		
nome unoitstelle	Schlässelaigorithmus :	© RSH 2046-58 ₩ ○ 8005A P256 ₩		
Enstaningen Leitstanis	Einstellungen Zertifikat	- 1-1 1-1		
dage/Wartung	Startdatum Göltigkeit LUU/MM/TTL:			
Jildqualität justieren	Enddatum Göltigkalt (JUU/MM/TT) :			
Wartung	Land/Region :	S have Lang/region values		
instellungen Punktion		Internet-candercode aingeben.		
Aligoreaine Einstellungen			J	
Drudker	Staat:			
	Stadt :			
Anden	Organization :			
tre plangen	descention and a back of			
Oataien speichern/zugänglich	Canangaton of an erit			
methon	Algemeiner Name :			

[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.

🕞 [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.

🕒 [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.

🚯 [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.

[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.

🚹 [Staat]/[Stadt]

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

[Organisation]/[Organisationseinheit]

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

🚹 [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.

Gerät new starten	Einstellungen/speicherung i Einstell schlassel generieren > schlassel un	lungen Verwaltung : tierateverwaltung > Eins di sienierten zertifikotantradi (CXII) generieren	tellungen 5chlessel und	zertifikat >
Einstelländerungen anwenden	Schlüssel und signierte	en Zertifikatantrag (CSR) ge	norieren	
taferessen	Semasser and signer o	en zerennaranne og (esn) ger	Duletist skouskalert	85/11 2020 8:03:04
Einstellungen Papier			DK.	Abbrechen
Erotellungen Time/Energie	Schlässelname :			<u> </u>
Einstellungen Netzwerk	Algorithmus Signatur :	9H4256 ¥		$ \longrightarrow$
Externe schnittstelle	Schlässeleigorithmus :	(# FSA 2040-bà ∀		
Einstellungen Lautstarke		○ R0064 P156 ♥		
stage/Wartung	Einstellungen signierter Zertiffikz	stantrag (CSR)		
Sidqualität justienen	Land/Region :	(ii) Norre Land/Region within Confliction (CD)		
exichangen Funktion		 Internet:Ländercode eingeben. 		
digemeine Einstellungen				
Copie	Staat:			L
Tucker	Studt:			
	Organisation :			1
41081	Organizationseinheit :			
Emplangen, Weiterleiten	Allgemeiner Name :			
Debelen speichem/zagänglich machan	x			
impfänger einstellen				
installances Versoltung				

[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.

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.

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

2. Registrieren des ausgestellten Zertifikats für den Schlüssel

- 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 2 f
ür das Zertifikat, das Sie registrieren möchten.

inspectrumpi advance be	8.401086.7	B-ADV COME/	Zum Portal	Login Anwender: Administrator Logeut
Einstellungen/Speicherung	,			E-Mail an Systemmanager
delät neu starten	Einstellungen	/Spuicherung : Einstellungen	Verwaltung : Geräteverwaltung + Ein	stellungen Schlosel und Zertifikat
Eisstelländerungen anwenden	Einstellu	ngen Schlüssel un	d Zertifikat	Zuletat aktualisiert: 85/11 2020 83349
Palfmenam	Löschen	Schlüssel generieren	Registrieren voe Schlüssel und Zert	tilikat
Einstellungen Papier	Wählen	Schlüsselname	Schlüsselve reendung	Zertificat
Einstellungen Timer/Energie	0	🔎 Default Key		63
Einstellungen Netzwerk	0	🔎 Default Key	[712]	<u>63</u>
Externe Schnittstelle	0	🔎 AMS	[Zugangskontrolle]	600
Einstellungen Lautstärke	0	🔎 csr		
Justage/Wartung	×			
Ridqualitätjuttieren				
Einstellungen Funktion				
Allgemeine Einstellungen				
Kopie				
Drucker				
Senden				
Empfangen/Weiterfeiten				
trateien speichern/zugänglich				
machen				
Emplänger einstellen				
Einstellungen Verwahung				
Asvercienenwitzeg				

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].

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.

Einstellungen für Anforderung Eersteenvarbung Bartelangen für Anforderung der Zertflichtesenlefung SCIP Statun der Anforderung der Zertflichtesenlefung Kommunikationseinstellungen Anforderung der Zertflichtesenstellung Einstellungen für anneralische antorderung der) der Zertifikatsonsstellung (58 Einstellungen für Anfordarung der Zer Anforderung der Zertifik Anforderung der Zertifikatsonstel Schlassehame: Algehtmus Signaur: Schlassehame: Reisen für	EEP) tillietseustellung (SCD) : Anforderung der Zerfölketseustellung katsausstellung Anforderung senden Abbrechen Iking
Certiterenvertung Distribunges für Auforderung der Zertifikationeninflung (SCIP) Statu der Arbitisterung der Zertifikationenintellung en Anforderung der Zertifikationseinstellung Einzellungen für automatische antorderung	Einstellungen für Anforderung der Zer Anforderung der Zertiffe Anforderung der Zertiffe Schlassehame: Algehtmus Signatur: Schlassehame: Retrocklage für	tilikebecastellung katsausstellung Antoiderung senden Abbrechen Iking
Bartelanges für Antordenung der Zertifikationentillung (KCP) Zertifikationentillung Kommunikationseinstellung en Anfordenung der Zertifikationseinstellung Einstellungen für antorenalische antordenungen für antorenalische	Anforderung der Zertifi Anforderung der Zertifikstausstol schlussehame Algorithmus Signatur: Schlussehame Hitt	katsausstellung Antoidening senden Abbrechen Itang
Status der Anforderung der Zertrifikationseinstellung Kommunikationseinstellung en Anforderung der Zertrifikatiousschlite in Einstellungen für anternatische Anforderung der	Antonionung der Zertifikotsausstal Schlusseine me: Algorithmus Signatur: Schlüsseilände (ärtz	Anto dening senten Abbrechen
Zertrikksbauzolellung Kommunikationseinstellung en Anforderung der Zertrikksbauzstellung Einstellungen für anternatiosthe Anforderung einer	Antonionung der Zertifikatsausstof schlusseinemet Algorithmus Signatur: Schlüsselänse (ärts	lang [
Kommunikationseimstellungen Anforderung der Zort fiketzeusstellung Einstellungen für automatische Antonieuse der	Schlasseiname: Algorithmus Signatur: Schlässelänce (Bitt:	
Anforcherung der zort Restausstellung Einstellungen für automatische Anforderung der	Algorithmus Signatur: Schlüsselänge (Bift)	(1944256 M)
zert Rikatsausstellung Einstellungen für automatische	Schlüsselänge (Bitz	
Einstellungen für automatische Auforzierung der		(R5A2048 \V
hafroriesung das	organisation:	
Test Electrony and	Aligemeiner Name:	
2041863BGUIDHU 1g	challenge-messwort	
	ort der schlasselverwendung	Catheline OTUS Office Backton Office Backton Office Backton
	x	

อ [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.

🧿 [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

📵 [Organisation:]

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.

[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.

🕑 [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 【Ⅰ】 (Einstell./Speicherung) ► <Einstelländerungen anwenden> ► <Ja>.

Das Gerät startet neu und übernimmt die Einstellungen.

■ Verwenden von Remote UI

- 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] f
 ür den Schl
 üssel und das Zertifikat, die f
 ür die TLSverschl
 üsselte Kommunikation verwendet werden sollen.

			Zam Portal	Login Anwend	er: Administrator Logest
Distellungen/Speicherung					E-Meil en Systemmenager
Gerät neu starten	Entelungen/Speicherung: E Zeit/Rat	Fräherenzen : Einstellungen Nietzw	erk > Einstellung	en TLS > Sindeli	ungen Schlässel und
Einstellinderungen anwenden	Finstellungen Schl	lissel und Zertifikat		Zuietz situalitie	** shissi isis was n
Puzifecenzes	cinstenangen sch	usper und zer unkart			
	Schlüssel und Zertifikst, di	is verwendet worden			
Lanssellungen Papier	Gespeicherter/s Schlässel	and Zertifikat			
Einstellungen Timer/Energie	Schlüsselname	5drill melverwendung	2	etifikat	
Einsbellungen Netzwerk	🔎 Default Key		1	S (v	erwanden
Externe Schnittstelle	🔎 Detault Key	[TLS]	1	15 V	erwanden.
tänstellungen Lautstarke	X				

• 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

🚺 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].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].

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



HINWEIS

- Wenn X 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)(P. 29)
- Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IEEE 802.1X)(P. 31)
- Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IEEE 802.1X)(P. 39)
- Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IEEE 802.1X)(P. 42)
- Schritt 5: Deaktivieren des Zertifikats (für IEEE 802.1X)(P. 44)
- Schritt 6: Aktivieren des neuen Zertifikats (für IEEE 802.1X)(P. 45)

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



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

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

Beispielbildschirm:

Continuer 🔊 🖻 Titlig.	📫 İnstrum	Contraction of the contractio	😭 Indale 🦉 Instance	
<10039kages 1010 802.10.4		<1842#Jungen 1000 802.22>		
 IEEE 882, TX verwenden 	tin as	• T/S measured or Schlaped and Socializet	De A	u
Light Rame		• TES retreater		u
 3intificat Authorever restinanes 	En Au	 REAP retreated 		
Kate Autent over will level Autent over				
X aldereden	Relay +	× abbreden	- Jurish	ж "/

- 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].

nstellungen IEEE 802.1X		Zuletzi	aktualisiert	08/03 2022 16:26:
			OK	Abbrechen
IEEE 802.1X verwenden				
Login-Name :	1			
Zertifikat Authentisierungsserver ver	rifizieren			
Name Authentisierungsserver	verifizieren			
Name Authentisierungsserver :				
Z TLS verwenden				
*Standardschlüssel in Einstellungen Se	hlüssel und Zertifikat unter [Einstellungen '	TLS] einstellen	, um TLS zu	verwenden.
Schlüsselname :	key1			
Schlüssel und Zertifikat :	Schlüssel und Zertifikat			
TTLS verwenden				
Einstellungen TTLS (TTLS Protokol): MSCHAPv2 verwenden PAP 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

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:



60 <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 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 🕝 wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für 🕝 setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

🧿 <Schlüsselalgorithmus>

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

📵 <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für 🧿 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 f ür das Zertifikat h dr ücken Sie Schl üssel gener.>.

Beispielbildschirm:



63<Startdatum Gültigkeit>/<Enddatum Gültigkeit>

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

Cand/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

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

🔁 <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

- 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].

5 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.

		Zum Pertal	Login Anwender: Ad	ministrator Logout
Einstellungen/Speicherung				i an Systemnanage
Gorat neu starten	Einstellungen/Speicherung : Einstellungen	Verwillung : Gerikterwillung > Ein	stellungen Schlüssel und	Zerffkat >
Einstellanderungen anwenden	Netzwerkkommunikation	schlüssel generieren	Zaletzt ektoelisiert:	15/04 2021 22:22:18
Tällenerupen		,	CK	Althorhom
Antiellungen Rapier	(- Sh	Harristen
Gintfell ungen Timer/Energie	Schlüsseiname :			
Einstell ungen Netzwerk	Algorithmus Signatur :	3HA256 Y		
nome unoitstelle	Schlässelaigorithmus :	© RSH 2046-58 ₩ ○ 8005A P256 ₩		
Enstaningen Leutstanis	Einstellungen Zertifikat	- 1-1 1-1		
dage/Wartung	Startdatum Göltigkeit LUU/MM/TTL:			
Jildqualität justieren	Enddatum Göltigkalt (JUU/MM/TT) :			
Wartung	Land/Region :	S have Lang/region values		
instellungen Punktion		Internet-candercode aingeben.		
Aligoreaine Einstellungen			J	
Drudker	Staat:			
	Stadt :			
Anden	Organization :			
tre plangen	descention and a back of			
Oataien speichern/zugänglich	Canangaton of an erit			
methon	Algemeiner Name :			

[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.

🕞 [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.

🕒 [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.

🚯 [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.

[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.

🚹 [Staat]/[Stadt]

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

[Organisation]/[Organisationseinheit]

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

🚹 [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 age come a age code	zum Portal	Login Anwender: Ad	er restrator Lagout
C Einstellungen/Speicherun	9		E-M1	el an Systemernanager
Gesät new starten	Einstellungen/Speicherung i Einstell	ungen Verwaltung : tiersteverwaltung > bin	stellungen 5chlessel und	zertifikat >
Einstelländerungen anvereden	Schlüssel und signierte	an Zertifikatantran (CSR) oo	norieron	
haferesaen	Schusser und signierte	in zer unkaranti ağı (cək) ge	Duktat skivalisieri	85/11 2020 8:03:04
Einstellungen Papier			UK.	Abbrechen
Einstellungen Timer/Energie	Schlüsseiname :			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Einstellungen Netzwerk	Algorithmus Signatur :	SH4256 M		
Externe Schnittstelle	Schlässelølgorithmus :	(® #SA 2040-bit ₩		
Einstellungen Lautstarke		○ 80064 p154 ♥		
intage/Wartung	Einstellungen signierter Zertifikz	tantrag (CSR)		
Di dquaitætjusteren	Land/Region :	Name Land/Region walking Gent between (GD)		
Basiclungen Funktion		 Internet-Ländercode eingeben. 		
Allgemeine Einstellungen				
Kapie	Staat:			L
Drucker	Studt:			
for a design of the second sec	Organisation :			1
Senden	Organizationseinheit :			
Emplangen/Weiterleiten	Allgemeiner Name I			
Dateien speichem/zagänglich				
machan	•			
Empfänger einstellen				
linctellungen Verwaltung				
Americanalism				

[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.

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.

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

2. Registrieren des ausgestellten Zertifikats für den Schlüssel

- 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 2 f
ür das Zertifikat, das Sie registrieren möchten.

inspectrum atranca to	8.401086.7	B-ADV COME/	Zum Portal	Login Anwender: Administrator Logeut
Einstellungen/Speicherung	,			E-Mail an Systemmanager
delät neu starten	Einstellungen	/Spuicherung : Einstellungen	Verwaltung : Geräteverwaltung + Ein	stellungen Schlosel und Zertifikat
Eisstelländerungen anwenden	Einstellu	ngen Schlüssel un	d Zertifikat	Zuletat aktualisiert (85/11 2020 83349
Palfmenam	Löschen	Schlüssel generieren	Registrieren voe Schlüssel und Zert	til kat
Einstellungen Papier	Wählen	Schlüsselname	Schlüsselve reendung	Zertificat
Einstellungen Timer/Energie	0	🔎 Default Key		63
Einstellungen Netzwerk	0	🔎 Default Key	[712]	<u>68</u>
Externe Schnittstelle	0	🔎 AMS	[Zugangskontrolle]	6.0
Einstellungen Lautstärke	0	🔎 csr		
Jestage/Wartung	×			
Ridqualitätjuttieren				
Einstellungen Funktion				
Allgemeine Einstellungen				
Kopie				
Drucker				
Senden				
Empfangen/Weiterfeiten				
trateien speichern/zugänglich				
machen				
Emplänger einstellen				
Einstellungen Verwahung				
Asvercienenwitzeg				

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].

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.

	8.401 (186.7 8.401 (186.7		Zum Portal	Logis Anwender: Adv	ninistrator Lageut
Extense markanges für Antondung der Zertfilkatseusstellung (SCDP): Anforderung der Zertfilkatseusstellung Extensionanderung SCDP Anforderung der Zertfilkatseusstellung Kommunikationseintellungen <p< th=""><th>🔅 Einstellungen für Anforde</th><th>rung der Zertifikatsausstellung (SCE</th><th>(P)</th><th></th><th></th></p<>	🔅 Einstellungen für Anforde	rung der Zertifikatsausstellung (SCE	(P)		
Bindbackster Anforderung der Zertifikatsausstellung Zartifikatsausstellung Anforderung der Zertifikatsausstellung Zartifikatsausstellung Anforderung der Zertifikatsausstellung Kommunikationseinstellungen Anforderung der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Anforderung senden Anforderung der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Kommunikationseinstellungen Algenthema Signatur: Partifikatsausstellung Schlussehange (Bits Schlussehange (Bits Enstander / Bits Zertifikatsausstellung Organisation Autorderung der Zertifikatsausstellung Organisation Schlussehange (Bits Enstander / Bits Zertifikatsausstellung Organisation Organisation Algenetienen Name: Challenge Presswirti: Ort der schlüssellenwendung Ort der schlüssellenwendung Ensteinen / Bits Pieset I Pieset I	+ Geräteiverwaltung	Einstellungen für Anforderung der Zertif	ikebasastellung (SCBP) : Anforderung d	r Zerfilikebaustellung	
Saha dar Arlosdening dar Senteunkalsene instellungen Anfordening der Zertfikstsaustellung Anfordening der Zertfikstsaustellung Schluselung der Zertfikstsaustellung Schluselung der Zertfikstsaustellung Schluselung (der Zertfikstaustellung Schluselung (der Zertfikst	Einstellungen für Antorderung der Zertifikationentellung (SCDP)	Anforderung der Zertifik	atsausstellung		
Zertifikatuzzetellung Anfordinung der Zertifikatuzzetellung Kommunikationseinstellungen Softe Zertifikatuzzetellung Anfordinung der Zertifikatuzzetellung Softe Zertifikatuzzetellung Zertifikatuzzetellung Softe Zertifikatuzzetellung Zertifikatuzzetellung Organisztione Zertifikatuzzetellung Organisztione Zertifikatuzzetellung Organisztione Zertifikatuzzetellung Organisztione Zertifikatuzzetellung Organisztione Zertifikatuzzetellung Organisztione Order Schlüsselerwondung Organisztione Ort der Schlüsselerwondung Organisztione	Status der Anforderung der			Anto identing senden	Abbrechen
Kommunikationseinstellungen Schlüssehane: Anforderung der Zorflikutsasstellung Algerithmus Signatur: Einsahlunge für antomasische Antorderung der Zertlikatsaustellung Organisation: Zertlikatsaustellung Organisation: Challenge für antomasische Antorderung der Zertlikatsaustellung Organisation: Organisation: Impact of the schlüssellenwendung Ort der schlüssellenwendung Office schlüssellenwendung Impact office: Impact office:	Zertifikebæzodellung	Anforderung der Zertifikatsausstellu	ng		
Anforcherung der Zortflikatzusstelle ig Einstlinger für antomatische Anforderunge für antomatische Antorderung der Zertflikatzusstellung Anforderunge meta- Zertflikatzusstellung Antorderung der Zertflikatzusstellung Antorderung der Zertflikatzusstellung Antorderung der Zertflikatzusstellung Antorderung der Zertflikatzusstellung Antorderung der Zertflikatzusstellung Antorderung der Zertflikatzusstellung Zertflikat	Kommunikationseinstellungen	schlasseine mei			
Zertifikatsusstellung Zertifikatsusstellung Einstellunge (RE: EINSADUR V Organisation: Organis	Anforderung der	Algorithmus Signatur:	SHA256 M		
Einstellungen für anomalische Antorderung der Zechlikaskaussiellung Challenge Pesserunti Ont der schlasselverwendung Einstellung Challenge Pesserunti Ont der schlasselverwendung Bisse Haz 1X Officier Implicit i	Zert Tikets ausshallung	Schlüsselänge (Bit):	(RSA2048 M		
Adordeusg del Zertfikatsundelung Challenge Pesavicti Ort der schlasseherwendung Ort der schlasseherwendung Office Mazi IX Office Mazi IX Office Mazi IX	Einstellungen für automatische	organisation:			
Challenge Plasswirtt ort der schlasselverwendung Office Baz i X Office Baz i X Office Baz i X	Antorderung der	Aligemeiner Name:			
ort der schlasselverwandung: OTUS Office B22.1X OFFice IPSect M	zernezitazitetetete	Challman Passwort			
TIS OFFER 182.1X OFFER 1956CT V		cat de striktskerendene	California -		$ \longrightarrow $
Offee #22.1X Offee #25601 ™		and any second second second a	01L5		
			OIEEE 882.1X		
x			OIRSEC INSECT V		
		x			

🔁 [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.

🕒 [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

📵 [Organisation:]

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.

[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.

🕑 [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) **Overwenden von Remote UI(P. 40)**

Verwenden des Bedienfelds

Drücken Sie 🔯 (Einstell./Speicherung).

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:



🙃 <Login-Name>

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

<Zertifikat Auth.server verifizieren>

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

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.

👍 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

Starten Sie die Remote UI.

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

Klicken Sie auf [Einstellungen Netzwerk] > [Einstellungen IEEE 802.1X].

Wählen Sie[IEEE 802.1X verwenden] > konfigurieren Sie die erforderlichen Einstellungen.

		Zan Portal	Logie Anvender: Admini	itrotor Logost
🔅 Einstellungen/Speicherung				
Gerik nos starten	Einstellungen/Speicherung: Pollenenzen: Einstellu	ngen Netzwerk > Einstellun	pen IGEE 002.11K	
Einstelländerungen anwenden	Einstellungen IEEE 802.1X		Zaletzt oktasi laiert : 15/6	4.2021.259.09
tationstan			DR:	Abrechen .
tilstellungen Papier	REF BOD. TX vervendes			
tisztelungen times/tnergie	Login-Name :			
Einstellungen Netzwerk	😟 Zertifikat Aufhentisierungsserver volfiziere	·)		
Externe Schnittstelle	Name Buthertikierungconver verifizier Mane Buthertikierungconver	nen.		
Gittellungen Lautstärke	TLS revendes			
niage/Warlung	"Standardschillosel in Einstellungen Schlüssel i	nd Zentifikal unter Elinstellung	en TLSD einstellen, um TLS zu verw	enden.
nikipusitat justeren	Schlüppelname : Nic	ht eingestellt.		
Wartung	Schlosel und Zertfikat : 5c	hlissel und Zertillkat		
intellangen Funktion Allgemeine Einstellungen	TILS verwanden Einstellungen TILS (TILS Wessekol) :	MICHARY Investigation		
Tanden	PEAP servenden Enginitikerse ab Anvendemanse verwi	en de n		
Empforgen	tintellangen anwendenssee/Pacovort: A	wendemane/Passwert and	en	
Dateien speichernstagiinglich	_			

[Login-Name]

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

🕞 [Zertifikat Authentisierungsserver verifizieren]

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

🕒 [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

🚺 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].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].

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



HINWEIS

- Wenn X 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)(P. 47)
- Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für IPSec)(P. 49)
- Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für IPSec)(P. 57)
- Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für IPSec)(P. 60)
- Schritt 5: Deaktivieren des Zertifikats (für IPSec)(P. 62)
- Schritt 6: Aktivieren des neuen Zertifikats (für IPSec)(P. 63)

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

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:



Drücken Sie <Weiter> > überprüfen Sie <Authentisierungsmethode>.

Beispielbildschirm:

Contrary Contrary Contrary	😭 rootaya 🦉 Instaga 🗮	Citeringe ID-	initian 📕 Latent
• IKZ-Modus	Mér Approxim	+ Außternüberunge- werheite	Mith. He- gen. Schille.
+ sinper	(490) Min. Sig Mit Editoriation simplore. 0 495551	* Algorithma Auft Avectolics.	Allo Maudio
X alizeden	kota (samerensitara, dji)	i Mittendren ∰ Saturmenter ■ Moder fe	م عنده مد struccustors. d3

• 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].

KE	Zuletzt aktualisiert	:: 08/03 2022 16:27:5
	OK	Abbrechen
IKE-Modus		
Main		
Aggressive		
Gültigkeit		
Zeit 480 Min. (1-65535)		
Authentisierungsmethode		
O Methode Pre-gemeinsamer Schlüssel : Einstellungen gemeinsamer Schlüssel		
Methode digitale Signatur :		
Schlüsselname : key1		
Schlüssel und Zertifikat : Schlüssel und Zertifikat		

- 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

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:



60 <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 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 🕝 wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für 🕝 setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

🧿 <Schlüsselalgorithmus>

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

📵 <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für 🧿 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 f ür das Zertifikat h dr ücken Sie Schl üssel gener.>.

Beispielbildschirm:



63<Startdatum Gültigkeit>/<Enddatum Gültigkeit>

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

Cand/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

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

🔁 <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

- 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].

5 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.

		Zum Portal	Login Anwender: Ad	ministrator Logout
Einstellungen/Speicherung			E-Ma	i an Systemnanage
Gorat neu starten	Einstellungen/Speicherung : Einstellungen	Verwillung : Gerittererwillung > Ein	stellungen Schlüssel und	Zerffkat >
Einstellanderungen anwenden	Netzwerkkommunikation	schlüssel generieren	Zalietzt aktivalisiert:	15/04 2021 22:22:18
Tällenerupen		,	CK	Althorhom
Antiellungen Rapier	(- Sh	Harristen
Gintfell ungen Timer/Energie	Schlüsseiname :			
Einstell ungen Netzwerk	Algorithmus Signatur :	[3HA256 V]		
nome unoitstelle	Schlässelaigorithmus :	© RGM 2046-58 ♥ ○ RCDSA P256 ♥		
Enstaningen Leitstanis	Einstellungen Zertifikat			
dage/Wartung	Startdatum Göltigkeit LUU/MM/TTL:		_	
Jildqualität justieren	Enddatum Göltigkalt (JUU/MM/TT) :			
Wartung	Land/Region :	(c) Name Landynegion watten		
instellungen Punktion		Internet-candercode aingeben.		
Aligoreaine Einstellungen			J	
Drudker	Staat:			
	Stadt :			
Anden	Organization :			
treplangen	descent and the second state of the			
Oataien speichern/zugänglich	Canangaton of an erit			
methon	Algemeiner Name :			

[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.

🕞 [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.

🕒 [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.

🚯 [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.

[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.

🚹 [Staat]/[Stadt]

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

[Organisation]/[Organisationseinheit]

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

🚹 [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.

Gesät new starten Einstellun schlassol	ngen/spoicherung : Einstel Loonariaren > tuthirscal ur	lungen Verwaltung : tiersteverwaltung > bin di sienierten zertifikatantzan 10381 geneeleer	stellungen 5chlessel un n	d zertifikat >
Eistheländerungen anwenden Schliß	ssel und signiert	en Zertifikatantrag (CSR) ge	nerieren	
aferenzen	soer and signer	en zer ennarenn og (esn) ge	Duletzt sktualisie	71: 95/71 2020 8:53:04
Instellungen Papier			UK.	Abbrechen
Snotellungen Timer/Energie	lässelname :			<u> </u>
Sinstellungen twitzwerk	orithmus Signatur :	9H4256 M		$ \longrightarrow$
sterne schriftstelle sch	asselalgorithmus :	(1) FSA 2048-bit M		
instellungen Lautstarke		○ 60064 p154 ¥		
Entel Entel	ungen signierter Zertifik	itantrag (CSR)		
Ndguaitæjustieren Land	1/Region :	Nome Land/Region within Cost Instruming (CD)		
oriellungen Funktion		 Internet-Ländercode eingeben. 		
Algemeine Einstellungen				
Copie Staa	dt i			L
Trucker Stad	R:			
Orp	aniadion :			
Org	a tikation sei tiheit :			
ingfangen/Weiterleiten Allg	emeiner Name I			
Datelen speichem/bagänglich 🕱				
mpfänger einstellen				
schellungen Verwaltung				

[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.

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.

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

2. Registrieren des ausgestellten Zertifikats für den Schlüssel

- 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 2 f
ür das Zertifikat, das Sie registrieren möchten.

inspectrumpi advance be	8.401086.7	B-ADV COME/	Zum Portal	Login Anwender: Administrator Logeut
Einstellungen/Speicherung	,			E-Mail an Systemmanager
delät neu starten	Einstellungen	/Spuicherung : Einstellungen	Verwaltung : Geräteverwaltung + Ein	stellungen Schlosel und Zertifikat
Eisstelländerungen anwenden	Einstellu	ngen Schlüssel un	d Zertifikat	Zuletat aktualisiert (85/11 2020 83349
Palfmenam	Löschen	Schlüssel generieren	Registrieren voe Schlüssel und Zert	til kat
Einstellungen Papier	Wählen	Schlüsselname	Schlüsselve reendung	Zertificat
Einstellungen Timer/Energie	0	🔎 Default Key		63
Einstellungen Netzwerk	0	🔎 Default Key	[712]	<u>68</u>
Externe Schnittstelle	0	🔎 AMS	[Zugangskontrolle]	6.0
Einstellungen Lautstärke	0	🔎 csr		
Jestage/Wartung	×			
Ridqualitätjuttieren				
Einstellungen Funktion				
Allgemeine Einstellungen				
Kopie				
Drucker				
Senden				
Empfangen/Weiterfeiten				
trateien speichern/zugänglich				
machen				
Emplänger einstellen				
Einstellungen Verwahung				
Asvercienenwitzeg				

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].

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.

Einstellungen für Anforderung der Zertifikatsausstellung (SCEP): Anforderung der Zertifikatsausstellung Einstellungen für Anforderung der Zertifikatsausstellung Einstellung SCEP Schlausen der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Schlausen der Zertifikatsausstellung Schlausen der Zertifikatsausstellung Anforderung der Zertifikatsausstellung Schlausen der Zertifikatsausstellung Schlau	stellungen för Anforderung der Zertifikatsausstellung (SCEP) menting per för Anforderung der Zertifikatsausstellung per för Anforderung der Zertifikatsausstellung neter bezeitellungen neter bezeitellungen neter bezeitellungen stellungen för Anforderung der Zertifikatsausstellung Stellungen	(SCEP) : Anfordening of	der Zerfölketswootelleng Anfoldenung senden	Abbrechen
Extense extense Extense extense for Anforderung der Zertfilksbasse bling (SCB): Anfordunge der Zertfilksbasse bling Extense einstellung Exten	envelting Exclusioning dar Schröderung der Zertifikationstellung (SCDP) ; Anforderung der Zertifikationstellung machen derung der Schröderung der Zertifikationstellung Anforderung der Zertifikationstellung machen derung der Schröderung der Zertifikationstellung Anforderung der Zertifikationstellung machen derung der Schröderung der Zertifikationstellung Anforderung der Zertifikationstellung machen derung der Schröderung der Zertifikationstellung Anforderung der Zertifikationstellung machen derung der Zertifikationstellung Schlüssellung (BP; Bracous M) schlässellung (BP; Bracous M) Schlässellung (BP; Bracous M) organisation: Challenge frasentri oft der schlässellenwendung Schlässellenwendung Stellungen framer Stellungen (BP; Bracous M) Stellungen framer Stellungen (BP; Bracous M) oft der schlässellenwendung Stellungen (BP; Bracous M) Stellungen (BP; Bracous M) Stellungen (BP; Bracous M) Stellungen (BP; Bracous M)<	(SCEP) : Anforderung : ung	der Zerfilferbausstellung Anforderung senden	Abbrochen
Bindaques tra Astrónique der Zartifikatisausstellung Anforderung der Zertifikatisausstellung Zartifikatisausstellung Anforderung der Zertifikatisausstellung Zartifikatisausstellung Anforderung der Zertifikatisausstellung Kommunikationseinstellungen Schlusseinen der Schlusseinen der Anforderung der Zertifikatisausstellung Anforderung senden Atbedeus Anforderung der Zertifikatisausstellung Schlusseinane Anforderung der Zertifikatisausstellung Schlusseinane Schlusseinane Image: Schlusseinane	per tra Antonioneg dar wannsteng SCHP er Anforderung der Zertifikatsausstellung inkelbeneinstellungen ning die songe für antonseksiche song die songe für antonseksiche song die songe für antonseksiche song die songen für antonseksiche songen für antonseksiche song die songen für antonseksiche songen für antonseksiche	ung	Anfordening senden	Abbrechen
Statu der Anforderung der Zerflikutsaustellung Anforderung der Zerfflikutsaustellung Kommunikationsinistellungen Schluseitenneit Anforderung der Zerfflikutsaustellung Schluseitenneit Zerflikutsaustellung Schluseitenneit Zerflikutsaustellung Schluseitenneit Zerflikutsaustellung Geschluseitenneit Zerflikutsaustellung Organisation Zerflikutsaustellung Organisation Zerflikutsaustellung Organisation Order Schlüsselerwendung Immerini Ort der Schlüsselerwendung Immerini Offlikutsaustellung Immerini	ar Anlasterung der haczuleing missioneninstellungen nung der Exastellung mon für automatische nung der Exastellung mon für automatische nung der Exastellung der Exastellung mon für automatische nung der Exastellung der Exastellung organisation inter Schlässellenwendung out der Schlässellenwendung out der Schlässellenwendung inter Schlässellenwendung inte		Anto idening senden	
Zertifikatuurutellung Anforderung der Zertifikatuurutellung Kommunikationseinstellungen Schütschaustig der Zertifikatuurutellung Anforderung der Zertifikatuurutellung Schütschaustig lingtur: Zertifikatuurutellungen Algorithmus Signatur: Zertifikatuurutellungen Schütschaustig lingtur: Zertifikatuurutellungen Gebütschaustig lingtur: Zertifikatuurutellungen Organisation: Zertifikatuurutellung Organisation: Zertifikatuurutellung Organisation: Zertifikatuurutellung Organisation: Zertifikatuurutellung Organisation: Zertifikatuurutellung Organisation: Zertifikatuurutellung Organisation:	hauzuhling hauzuhling en bedannen der ZertHkutseastellung en bedannen intellung en gen für schwarziche signatur: [9:4:39 M] Algendeinen kann der für schwarziche sing der taaschelung (Bitr: [9:4:39 M] Congenitationen kann der für schwarziche sing der Generationen kann der Gener			\Rightarrow
Kommunikationseinstellungen Schlussehane: Anforderung der Zorffikatsusstellung Algorithmus Signatur: Schlussehange (Bit): Imazon signatur: Einstellungen für anomasche Antorderung et Zertfikatsusstellung Organisation: Zertfikatsusstellung Organisation: Challongie missonistic Imazon Zertfikatsusstellung Organisation: Challongie missonistic Imazon Ort der Schlüsseherwendung Imazon Uffike Habitik Imazon Unterstellung Imazon	niveformeintellungen ning der Estatistellung noge für autowarische ning der Estatistellung Dorgenisation Algenetinnus Signatur: Dorgenisation Algenetinnus Challenge filts Challenge filtswirti Dorgenisation Challenge filtswirti			\equiv
Anfordening der Zertflikatzusstellung Algerithenus Signatus: [94A254 M] [55A254 M]	ning der tausstellung Algerähmus lignatur: [9:4296 M] socht automalische ning der tausstellung Socht ausetänge (Bit): [8:52046 M] Organisation: [8:52046 M] Ord der schlässellenwandung: [8:5506 M] Offset da2:1X [9:560 M]			
ZertRistausstellung Schlissellarge (ktr. [R5A2046 M]	Sausshilung Schlüssellarge (lit): (IS32346 M)			
Einstellungen für anomalische organisation: Auforderung der Allgemeinner Name: Challenge Missellerwandung Challenge Missellerwandung Ort der schlissellerwandung Ort der s	Ingen für antomatische sung der hannes internet			>
Antonderung der Allgemeinen Name: Chollenge Pisswert: Chollenge P	Aligenativer Name: challenge naswint: out der schlassellenwendung: UFSec Insect M			
Challenge Masswirts Ont der schlässelverwandungs Office 182 12 Office 182 12 Office 182 12	challenge-resswerti ort der schlassellenwendung: Offisie Bazitz Offisie Bazitz Offisie Bazitz Offisie Bazitz			
Ort der schlisselverwendung TLS Office Haz IX OFfice IPSect M	ort der schlassellerwendung: Otts Otts Otse Disse Bazitz Offsec Broact w			
OTUS Office Backty Office Backty Backty M	CHSec BESET V			``
Ciffee lastic M				
Crisk IPSell M	Z	X		
	2. Desperators at the	1250E1 V		
*	Lappe MARK AD			
	Carry Carry Carry Carry			
×				

🔁 [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.

🕒 [Schlüssellänge (Bit):]

Wählen Sie die Schlüssellänge aus.

📵 [Organisation:]

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.

[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.

🕑 [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) **Overwenden von Remote UI(P. 58)**

Verwenden des Bedienfelds

1 Drücken Sie 🚺 (Einstell./Speicherung).

- Drücken Sie <Präferenzen> > <Netzwerk> > <Einstellungen TCP/IP> > <Einstellungen</p> IPSec>.
- З 🛛 Wählen Sie die Richtlinie zum Zurücksetzen des Schlüssels und des Zertifikats für 🕨 drücken Sie <Bearbeiten> > <Einstellungen IKE>. Beispielbildschirm:



Distributions' Spectreturg	19. milita 🐒	infere.	Ξ.	ن ة ال	iethengen' chesung	Sintis 🐒 inte	E.
 Ex meda 		De	- Reg	clines	deatebu-		
Pakete shre Richtl	inie empfungen		Jute. Zarder.		Hichd name	inier "	_
4	A 1		t. Votanj atklas			Einchelangen Acon.contcht. Dischelangen	
4	_	-	liste ducken			incellarger PSec-Vetraent	Schlassellinge etailoe
Kothe Enver	dan , bebs	, loches			× Aldesch		ÓK .
Salamentar 🚺	Moda Spinnerwaltung.	-	G.	\ominus Satur	unitor 🛄 W	odus Systemverwaltung,	

🛕 Drücken Sie <Weiter> 🕨 wählen Sie <Digitale Sig. Methode> unter <Authentisierungsmethode> > drücken Sie <Schlüssel und Zertifikat>. Beispielbildschirm:

Christman'	🛱 belaite Balaite 🐞 barant	🔅 Spectreage 🦛 🕬 IIIII	r 👘 insinger
<1059kape H2+		<1intHagen IIS>	
 IK2-Modus 	Main Approxim	* Judhantianunga- methode	Mitts Pa- pan Schill
• cations	487 Min. % We Jahlenfacher einsplore.	-	Mine and a start
	0 411001	, Algorithmus Auft, Arecthico.	Allo Manufe Decklarger ,
× alanden	Robay In-	X atstanden 4	Jariah DK
🖨 Subsenation 🛛 🔳	Moda Salamenalizas. 🖓	\ominus Statumentor 🛛 🛄 Modas Sprinner	nvetans, di

- 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].



🦌 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

🚺 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].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].

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



HINWEIS

- Wenn X 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)(P. 65)
- Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für SIP)(P. 68)
- Schritt 3: Zurücksetzen des Schlüssels und des Zertifikats (für SIP)(P. 74)
- Schritt 4: Löschen eines in der Vergangenheit generierten Schlüssels/Zertifikats (für SIP)(P. 77)
- Schritt 5: Deaktivieren des Zertifikats (für SIP)(P. 79)
- Schritt 6: Aktivieren des neuen Zertifikats (für SIP)(P. 80)

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)



Überprüfen Sie <TLS verwenden>

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:

Contraction (19) martin (1	inter:		
distringer 1.1-				
* EM Sinalellun	uen .			
 Client-Auth 	enticierung erhalderlich	tin .	aus -	
 SE Einstellung 	per			
 Severanti 	Rad verificience	Dir.	Au	
* Otveril	kiens			
Schlook und Jorifikat	, • ieji			
X albriden			DX.	
🖗 Salumentor 🛛 🚺	🗵 Modus Systemverwaltung.			- GD

- 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

Uberprüfen von [TLS verwenden] und [Schlüssel und Zertifikat]

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].

Einstellungen SIP	Zu	Zuletzt aktualisiert: 08/03 2022 16:28:47 📢		
		OK	Abbrechen	
Einstellungen Intranet				
Intranet verwenden				
URI Haupteinheit :)	
EM Portnummer SIP :	5060 (1-65535)			
SE Transport SIP :	UDP TCP			
Z TLS verwenden				
*Standardschlüssel in Einstellungen Sch verwenden.	lüssel und Zertifikat unter [Einstellung	en TLS] einstellen, un	n TLS zu	
 Definierten SIP Server immer verwende 	n			
Erwerbsmethode SIP Serveradresse :	Manuell DHCP DHCPv6			
*Abhängig von den Einstellungen zu IPv	4 oder IPv6, kann die verwendete Met	thode [Manuel]] sein.		

- 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].

Einstellungen Media (1.36)		
SE Transport T.38 :	UDPTL.	
Medientyp T.38 :	Bild	
EM Portnummer T.38 :	49152 (1-65535)	
EM Portnummer RTP :	5004 (1024- 65534)	
Einstellungen TLS		
Schlüsselname	key1	
	Schlüssel und Zertifikat	
EM Einstellungen		
Client-Authentisierung erfor	derlich	
SE Einstellungen		
 Serverzertifikat verifizieren 		
🗌 CN zu den Verifizierung	spunkten hinzufügen	
x		
		Copyright CANON INC. 2020

- 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

🚺 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:



60 <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 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 🕝 wählen und <Schlüssellänge (Bit)> auf <1024> oder mehr für 🕝 setzen, können Sie die Hash-Algorithmen SHA384 und SHA512 wählen.

🤆 <Schlüsselalgorithmus>

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

🔂 <Schlüssellänge (Bit)>/<Schlüsseltyp>

Legen Sie die Schlüssellänge fest, wenn Sie <RSA> für 🧿 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 f ür das Zertifikat h dr ücken Sie Schl üssel gener.>.

Beispielbildschirm:



👩 <Startdatum Gültigkeit>/<Enddatum Gültigkeit>

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

Cand/Region>/<Staat>/<Stadt>/<Organisation>/<Org.einheit>

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

🔁 <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

- Starten Sie die Remote UI.
- **2** Klicken Sie auf der Portalseite auf [Einstellungen/Speicherung].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].
- 4 Klicken Sie auf [Schlüssel generieren].
- 5 Klicken Sie auf [Netzwerkkommunikation].
5 Konfigurieren Sie die Schlüssel- und Zertifikatseinstellungen.

		Zum Pertal	Login Anwender: Ad	ministrator Logout
Einstellungen/Speicherung				i an Systemnanage
Gorat neu starten	Einstellungen/Speicherung : Einstellungen	Verwillung : Gerikterwillung > Ein	stellungen Schlüssel und	Zerffkat >
Einstellanderungen anwenden	Netzwerkkommunikation	schlüssel generieren	Zaletzt ektoelisiert:	15/04 2021 22:22:18
Tällenerupen		,	CK	Althorhom
Antiellungen Rapier	(- Sh	Harristen
Gintfell ungen Timer/Energie	Schlüsseiname :			
Einstell ungen Netzwerk	Algorithmus Signatur :	3HA256 Y		
nome unoitstelle	Schlässelaigorithmus :	© RSH 2046-58 ₩ ○ 8005A P256 ₩		
Enstaningen Leitstanis	Einstellungen Zertifikat	- 1-1 1-1		
dage/Wartung	Startdatum Göltigkeit LUU/MM/TTL:			
Jildqualität justieren	Enddatum Göltigkalt (JUU/MM/TT) :			
Wartung	Land/Region :	S have Lang/region values		
instellungen Punktion		Internet-candercode aingeben.		
Aligoreaine Einstellungen			J	
Drudker	Staat:			
	Stadt :			
Anden	Organization :			
tre plangen	descention and a back of			
Oataien speichern/zugänglich	Canangaton of an erit			
methon	Algemeiner Name :			

[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.

🕞 [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.

🕒 [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.

🚯 [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.

[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.

🚹 [Staat]/[Stadt]

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

[Organisation]/[Organisationseinheit]

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

🚹 [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.

Gelat new starten	Schlassel generieren > Schlassel un	id signierten zertifikatantrag (CSR) generieren	en nigeri och koold and	AND THE .
Eisttelländerungen anvenden	Schlüssel und signiert	en Zertifikatantrag (CSR) ger	erieren	
lafereizen			Duktat skauskaiert	15/11 2020 5:33:44
Einstellungen Papier			ŪK.	Abbrechen
Crotellungen Timer/Energie	Schlüsseiname :			
Einstellungen Netzwerk	Algorithmus Signatur :	9HA256 ¥		
Externe schnittstelle	Schlässeleigorithmus :	(# RSA 2040-bit ₩		
Einstellungen Laufstarke		○ R006A P154 ♥		
stage/Wartung	Einstellungen signierter Zertifik	atantrag (CSR)		
50 deputit # justieren	Land/Region :	(ii) Norris Land/Region within Coal between (CD) Md		
exicilungen Funktion		 Internet:Ländercode eingeben. 		
Algemeine Einstellungen				
Copile	Staat:			L
Drucker	Stadt:			
landen	Organisation :			
	Organizationseinheit :			
imprangen, Weiterfeiten	Allgemeiner Name :)_
Debelern speicherm/bagäinglich Nachan	I			
Empfänger einstellen				
and a second a Warmond & second				

[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.

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.

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

2. Registrieren des ausgestellten Zertifikats für den Schlüssel

- 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.

inspectrumpi advanci (d	8.401084	B ADV COME/	Zum Portal	Login Anwender: Administrator Logeut
Einstellungen/Speicherung				E-Mail an Systemmanager
delät new stanlen	Einstellungen	/Speicherung : Einstellungen	Verwaltung : Geritteverwaltung = Ein	stellungen Schikssel und Zertifikat
Eisstelländenungen anwenden	Einstellu	ngen Schlüssel un	l Zertifikat	Zuletzt aktualisiert: 83/11 2020 83349
Pulferman	Löschen	Schlüssel generieren	Registrieren voe Schlüssel und Zert	Ekst_
Einstellungen Papier	Wählen	Schlüsselname	Schlüsselverwendung	Zertificat
Einstellungen Timer/Energie	0	🔎 Default Key		63
Einstellungen Netzwerk	0	🔎 Default Key	[112]	63
Externe Schnittstelle	0	🔎 AMS	(Zugangskontrolle)	200
Einstellungen Lautstärke	0	🔎 csr		
Justage/Wartung	×			
Bidqualität justieren				
Einstellungen Funktion				
Allgemeine Einstellungen				
Kopie				
Drucker				
Senden				
empfangen/weiterfeiten				
Dateien speichen/zaganglich reaches				
Emplänger einstellen				
Eastebangen Verwaltung				
Anvenderverweitung				

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> b drücken Sie <Schlüssel und Zertifikat>. Beispielbildschirm:



<em einstellungen="">	
<client-authentisierung erforderlich></client-authentisierung 	Wählen Sie <ein> oder <aus>. Wenn Sie <ein> wählen, fordert das Gerät beim Empfang eines IP-Faxes eine Client-Authentifizierung an.</ein></aus></ein>
<se einstellungen=""></se>	
<serverzertifikat verifizieren></serverzertifikat 	Wählen Sie <ein> oder <aus>. Wenn Sie <ein> wählen, prüft das Gerät beim Empfang eines IP-Faxes, ob das TLS-Serverzertifikat gültig ist.</ein></aus></ein>
<cn verifizieren=""></cn>	Wählen Sie <ein> oder <aus>. Wenn Sie <ein> wählen, prüft das Gerät beim Empfang eines IP-Faxes den CN (allgemeinen Namen).</ein></aus></ein>

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

1410 Acres		
Default Fire	4.80	
ANS	Terrandel.	
Je lagt	Versendet.	23
P Device Signature Rep	Versenbet.	100
indefies , debits ,		
	_	

- 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].

Verwenden von RSA-Schlüsseln und zusätzliche Verfahren

SE Transport T.38 :	UDPTL	
Medientyp T.38 :	Bild	
EM Portnummer T.38 :	49152 (1-65535)	
EM Portnummer RTP :	5004 (1024-65534)	
nstellungen TLS		
Schlüsselname	key1	
	Schlüssel und Zertifikat	
M Einstellungen		
Client-Authentisierung erfo	derlich	
E Einstellungen		
 Serverzertifikat verifizieren 		
🗌 CN zu den Verifizierun	gspunkten hinzufügen	
	Cop	right CANON INC.

[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.

espe Schlüs	icherter/s Schlüssel und Ze sseiname	rtifikat Schlüsselverwendung	Zertifikat	
۶	Default Key			Verwenden
۶	AMS	[Zugangskontrolle]	65	Verwenden
۶	key1	[TLS] [IEEE 802.1X] [IPSec] [SIP]	C 2	Verwenden
۵	Device Signature Key	[Geräte-Signatur]	C 2	Verwenden

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

🚺 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].
- 子 Klicken Sie auf [Geräteverwaltung] 🕨 [Einstellungen Schlüssel und Zertifikat].

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



HINWEIS

- Wenn X 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)(P. 82)

Schritt 2: Neugenerieren des Schlüssels und des Zertifikats (für Gerätesignaturen)(P. 84)

Schritt 3: Deaktivieren des Zertifikats (für Gerätesignaturen)(P. 85)

Schritt 4: Aktivieren des neuen Zertifikats (für Gerätesignaturen)(P. 86)

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

- 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>.



- 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

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].

		OK	Abbrecher	
stellungen S/MIME				
Einstellungen Verschlüsselung :	 Immer verschlüsseln Nur verschlüsseln bei Zertifikat Nicht verschlüsseln 			
 Digitale Signaturen hinzufügen 				
Algorithmus Verschlüsselung :	3DES V			
Algorithmus Signatur :	SHA1 V			
Signatur verifizieren nach Empf	ang			
Signatur drucken nach Empfang	9			

- 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.

Starten Sie die Remote UI.

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

子 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.

- 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	89
Verfahren für Bluetooth	90
Schritt 1: Löschen des in Canon PRINT Business registrierten Geräts (für Bluetooth)	91
Schritt 2: Erneutes Registrieren des Geräts bei Canon PRINT Business (für Bluetooth)	. 92

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.

Overfahren für Bluetooth(P. 90)

Verfahren für Bluetooth

Schritt 1: Löschen des in Canon PRINT Business registrierten Geräts (für Bluetooth)(P. 91)
 Schritt 2: Erneutes Registrieren des Geräts bei Canon PRINT Business (für Bluetooth)(P. 92)

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



Der Bildschirm [Drucker ausw.] wird angezeigt.



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.

子 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.
- 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	. 9	94
Verfahren für das Zugangsverwaltungssystem	9	95

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.

OVerfahren 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.

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.