

À propos de la mesure contre la vulnérabilité de la génération de clé RSA

Sommaire

Préface	2
Vérifier si vous devez effectuer les procédures supplémentaires	5
Utilisation de la clé RSA et procédure supplémentaire	12
Procédure pour TLS	13
Étape 1 : Régénération de la clé et du certificat (pour TLS)	14
Étape 2 : Réinitialisation de la clé et du certificat (pour TLS)	22
Étape 3 : Suppression d'une clé/un certificat généré(e) dans le passé (pour TLS)	24
Étape 4 : Désactivation du certificat (pour TLS)	26
Étape 5 : Activation du nouveau certificat (pour TLS)	27
Procédure pour IEEE 802.1X	28
Étape 1 : Vérification de la méthode d'authentification (pour IEEE 802.1X)	29
Étape 2 : Régénération de la clé et du certificat (pour IEEE 802.1X)	31
Étape 3 : réinitialisation de la clé et du certificat (pour IEEE 802.1X)	39
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IEEE 802.1X)	42
Étape 5 : désactivation du certificat (pour IEEE 802.1X)	44
Étape 6 : Activation du nouveau certificat (pour IEEE 802.1X)	45
Procédure pour IPSec	46
Étape 1 : Vérification de la méthode d'authentification (pour IPSec)	47
Étape 2 : Régénération de la clé et du certificat (pour IPSec)	49
Étape 3 : Réinitialisation de la clé et du certificat (pour IPSec)	57
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IPSec)	60
Étape 5 : Désactivation du certificat (pour IPSec)	62
Étape 6 : Activation du nouveau certificat (pour IPSec)	63
Procédure pour SIP	64
Étape 1 : Vérification des paramètres (pour SIP)	65
Étape 2 : Régénération de la clé et du certificat (pour SIP)	68
Étape 3 : Réinitialisation de la clé et du certificat (pour SIP)	74
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour SIP)	77
Étape 5 : Désactiver le certificat (pour SIP)	79
Étape 6 : Activation du nouveau certificat (pour SIP)	80
Procédure pour la signature des appareils	81
Étape 1 : Vérification des paramètres S/MIME (pour les signatures de l'appareil)	82
Étape 2 : Régénération de la clé et du certificat (pour les signatures d'appareils)	84
Étape 3 : Désactiver le certificat (pour les signatures d'appareils)	85
Étape 4 : Activation du nouveau certificat (pour les signatures d'appareils)	86
Procédures supplémentaires pour les réglages Bluetooth	89
Procédure pour Bluetooth	90

Étape 1 : Suppression de l'appareil enregistré dans Canon PRINT Business (pour Bluetooth)	91
Étape 2 : Réenregistrer l'appareil sur Canon PRINT Business (pour Bluetooth)	92

Procédures supplémentaires pour les paramètres du système de gestion des accès	94
Procédure pour le système de gestion des accès	95

Préface

Préface 2

Préface

Vous devez mettre à jour le micrologiciel et effectuer les procédures supplémentaires décrites dans ce document, afin de mettre à niveau une clé RSA créée avec une bibliothèque de cryptage vulnérable.

Tout d'abord, vérifiez le modèle et la version de votre appareil.

Si vous trouvez le modèle et la version de votre appareil sur cette page, mettez à jour le micrologiciel, puis effectuez les procédures supplémentaires décrites dans ce document. **► Vérifier si vous devez effectuer les procédures supplémentaires (P. 5)**

Pour plus d'informations sur la mise à jour du micrologiciel, consultez le site web sur lequel vous avez obtenu ce document.

Vérification de la version de votre appareil

Suivez la procédure ci-dessous pour vérifier la version de votre appareil.

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Suivi statut/Annulation] sur la page du portail.**
- 3 Cliquez [Informations périphérique] ► vérifiez [Contrôleur] dans [Informations sur la version].**

Modèles et versions nécessitant des procédures supplémentaires

Modèles	Versions
<ul style="list-style-type: none"> - iR-ADV 4545 / 4535 / 4525 - iR-ADV 715 / 615 / 525 - iR-ADV 6575 / 6565 / 6560 / 6555 - iR-ADV 8505 / 8595 / 8585 - iR-ADV C3530 / C3520 - iR-ADV C7580 / C7570 / C7565 - iR-ADV C5560 / C5550 / C5540 / C5535 - iR-ADV C355 / C255 - iR-ADV C356 / C256 	Ver 59.39 à Ver 67.30
<ul style="list-style-type: none"> - iR-ADV 4545 III / 4535 III / 4525 III - iR-ADV 715 III / 615 III / 525 III - iR-ADV 6575 III / 6565 III / 6560 III - iR-ADV 8505 III / 8595 III / 8585 III / 8505B III / 8595B III / 8585B III - iR-ADV C3530 III / C3520 III - iR-ADV C7580 III / C7570 III / C7565 III - iR-ADV C5560 III / C5550 III / C5540 III / C5535 III - iR-ADV C356 III - iR-ADV C475 III - iPR C165 / C170 	Ver 29.39 à Ver 37.30
<ul style="list-style-type: none"> - iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B 	Ver 17.44 à Ver 27.30

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

REMARQUE

- Les captures d'écran utilisées dans ce document peuvent différer de celles que vous voyez réellement, selon le modèle de votre appareil. Pour plus de détails sur les captures d'écran, consultez le manuel de votre appareil sur le site web des manuels en ligne.

<https://oip.manual.canon/>

Vérifier si vous devez effectuer les procédures supplémentaires

Vérifier si vous devez effectuer les procédures supplémentaires 5

Vérifier si vous devez effectuer les procédures supplémentaires

Effectuez les trois opérations suivantes pour vérifier les procédures supplémentaires que vous devez effectuer. Il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de commande, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

►Vérification de la clé RSA(P. 5)

►Vérification des réglages Bluetooth(P. 8)

►Vérification des réglages du système de gestion des accès(P. 8)

La vérification d'une clé RSA n'est pas nécessaire si « Clé par défaut » ou « AMS » s'affichent pour une clé enregistrée dans votre appareil. Vérifiez les paramètres Bluetooth et les paramètres du système de gestion d'accès, et effectuez les procédures supplémentaires si nécessaire.

REMARQUE

- Les captures d'écran utilisées dans ce document ne sont qu'un exemple. Elles peuvent différer de celles que vous voyez réellement, selon le modèle de votre appareil.

Vérification de la clé RSA

Vérifiez s'il existe une clé RSA. S'il existe une clé RSA générée avec l'appareil, vérifiez l'utilisation de la clé.

►Utilisation du panneau de commande(P. 5)

►Utilisation de l'interface utilisateur distante(P. 6)

■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Liste de clés et de certificats>.

3 Appuyez sur <Liste clés et certif. pour ce périphérique>.

- <Liste clés et certif. pour ce périphérique> ne s'affiche pas, sauf si la fonction de signature utilisateur est activée sur l'appareil. Dans ce cas, passez à l'étape suivante.

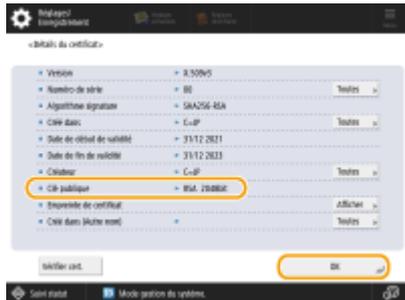
4 Sélectionnez une touche autre que <Default Key> et <AMS> qui a <Utilisé> affiché pour <Statut> ► appuyez sur <Détails du certificat>.

Exemple d'écran :



5 Vérifiez <Clé publique>.

Exemple d'écran :



Pour un certificat autre que RSA

Vous n'avez pas besoin d'effectuer les procédures supplémentaires. Appuyez sur <OK> pour fermer l'écran.

Pour un certificat RSA

Procédez à l'étape 6.

- Vous n'avez pas besoin d'effectuer les procédures supplémentaires pour les touches suivantes. Appuyez sur <OK> pour fermer l'écran.
- Une clé RSA générée en externe et enregistrée sur l'appareil
- Si vous devez effectuer les procédures supplémentaires, vous pouvez avoir besoin d'informations sur le certificat pour le désactiver. Notez les informations requises avant de supprimer la clé/le certificat. Demandez les informations requises à l'autorité de certification qui a émis le certificat.

6 Appuyez sur <Aff. emplac. d'utilisation> ► pour vérifier l'utilisation des touches.

Exemple d'écran :



Effectuez les procédures supplémentaires conformément à ce qui est indiqué ici. ► **Utilisation de la clé RSA et procédure supplémentaire(P. 12)**

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante ► cliquez sur [Réglages/Enregistrement] ► [Gestion du périphérique] ► [Réglages de clé et de certificat].

2 Cliquez sur une touche autre que [Default Key] et [AMS].



3 Vérifiez [Clé publique].



Pour un certificat autre que RSA

Vous n'avez pas besoin d'effectuer les procédures supplémentaires.

Pour un certificat RSA

Cliquez sur [Réglages de clé et de certificat] en haut de l'écran ► pour vérifier l'utilisation des clés.

- Effectuez les procédures supplémentaires conformément à ce qui est indiqué ici. **Utilisation de la clé RSA et procédure supplémentaire(P. 12)**
- Vous n'avez pas besoin d'effectuer les procédures supplémentaires pour les clés suivantes.
 - Une clé RSA générée en externe et enregistrée sur l'appareil
- Si vous devez effectuer les procédures supplémentaires, vous pouvez avoir besoin d'informations sur le certificat pour le désactiver. Notez les informations requises avant de supprimer la clé/le certificat. Demandez les informations requises à l'autorité de certification qui a émis le certificat.

Vérification des réglages Bluetooth

Vérifiez si Bluetooth est réglé sur <Oui>. Vous devez effectuer les procédures supplémentaires s'il est réglé sur <Oui>.

- ▶ **Utilisation du panneau de commande(P. 8)**
- ▶ **Utilisation de l'interface utilisateur distante(P. 8)**

■ Utilisation du panneau de commande

1 Appuyer sur  (Réglages/Enregistr.).

2 Appuyez sur <Préférences> ▶ <Réseau> ▶ <Réglages Bluetooth>.

3 Vérifiez <Utiliser Bluetooth>.

- Si <Utiliser Bluetooth> est réglé sur <Oui>, effectuez les procédures suivantes ▶ **Procédures supplémentaires pour les réglages Bluetooth(P. 89)**
- Si <Utiliser Bluetooth> est réglé sur <Non>, vous n'avez pas besoin d'effectuer les procédures suivantes.

■ Utilisation de l'interface utilisateur distante

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Réseau] ▶ [Réglages Bluetooth].

4 Vérifiez [Utiliser Bluetooth].

- Si [Utiliser Bluetooth] est sélectionné, effectuez les procédures suivantes ▶ **Procédures supplémentaires pour les réglages Bluetooth(P. 89)**
- Si [Utiliser Bluetooth] est désélectionné, vous n'avez pas besoin d'effectuer les procédures suivantes.

Vérification des réglages du système de gestion des accès

Vérifiez si le système de gestion des accès est réglé sur <Oui>. Vous devez effectuer les procédures supplémentaires s'il est réglé sur <Oui>.

Ce réglage peut ne pas apparaître, en fonction de votre appareil. Dans ce cas, vous n'avez pas besoin d'effectuer les procédures supplémentaires.

- ▶ **Utilisation du panneau de commande(P. 9)**
- ▶ **Utilisation de l'interface utilisateur distante(P. 9)**

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).**
- 2 Appuyez sur <Réglages de gestion> ► <Licence/Autre> ► <Utiliser ACCESS MANAGEMENT SYSTEM>.**
- 3 Vérifiez <Utiliser ACCESS MANAGEMENT SYSTEM>.**
 - Si <Utiliser ACCESS MANAGEMENT SYSTEM> est réglé sur <Oui>, effectuez les procédures suivantes ► **Procédures supplémentaires pour les paramètres du système de gestion des accès(P. 94)**
 - Si <Utiliser ACCESS MANAGEMENT SYSTEM> est réglé sur <Non>, vous n'avez pas besoin d'effectuer les procédures suivantes.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Licence/Autre] ► [Réglages d'ACCESS MANAGEMENT SYSTEM].**
- 4 Vérifiez [Utiliser ACCESS MANAGEMENT SYSTEM].**
 - Si [Utiliser ACCESS MANAGEMENT SYSTEM] est sélectionné, effectuez les procédures suivantes ► **Procédures supplémentaires pour les paramètres du système de gestion des accès(P. 94)**
 - Si [Utiliser ACCESS MANAGEMENT SYSTEM] est désélectionné, vous n'avez pas besoin d'effectuer les procédures suivantes.

Utilisation de la clé RSA et procédure supplémentaire

Utilisation de la clé RSA et procédure supplémentaire	12
Procédure pour TLS	13
Étape 1 : Régénération de la clé et du certificat (pour TLS)	14
Étape 2 : Réinitialisation de la clé et du certificat (pour TLS)	22
Étape 3 : Suppression d'une clé/un certificat généré(e) dans le passé (pour TLS)	24
Étape 4 : Désactivation du certificat (pour TLS)	26
Étape 5 : Activation du nouveau certificat (pour TLS)	27
Procédure pour IEEE 802.1X	28
Étape 1 : Vérification de la méthode d'authentification (pour IEEE 802.1X)	29
Étape 2 : Régénération de la clé et du certificat (pour IEEE 802.1X)	31
Étape 3 : réinitialisation de la clé et du certificat (pour IEEE 802.1X)	39
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IEEE 802.1X)	42
Étape 5 : désactivation du certificat (pour IEEE 802.1X)	44
Étape 6 : Activation du nouveau certificat (pour IEEE 802.1X)	45
Procédure pour IPSec	46
Étape 1 : Vérification de la méthode d'authentification (pour IPSec)	47
Étape 2 : Régénération de la clé et du certificat (pour IPSec)	49
Étape 3 : Réinitialisation de la clé et du certificat (pour IPSec)	57
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IPSec)	60
Étape 5 : Désactivation du certificat (pour IPSec)	62
Étape 6 : Activation du nouveau certificat (pour IPSec)	63
Procédure pour SIP	64
Étape 1 : Vérification des paramètres (pour SIP)	65
Étape 2 : Régénération de la clé et du certificat (pour SIP)	68
Étape 3 : Réinitialisation de la clé et du certificat (pour SIP)	74
Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour SIP)	77
Étape 5 : Désactiver le certificat (pour SIP)	79
Étape 6 : Activation du nouveau certificat (pour SIP)	80
Procédure pour la signature des appareils	81
Étape 1 : Vérification des paramètres S/MIME (pour les signatures de l'appareil)	82
Étape 2 : Régénération de la clé et du certificat (pour les signatures d'appareils)	84

Étape 3 : Désactiver le certificat (pour les signatures d'appareils)	85
Étape 4 : Activation du nouveau certificat (pour les signatures d'appareils)	86

Utilisation de la clé RSA et procédure supplémentaire

Reportez-vous à la section « Procédures supplémentaires » et exécutez-les en fonction de l'utilisation de la clé.

Utilisation de la clé RSA	Conditions	Procédures supplémentaires
TLS	Vous devez effectuer les procédures supplémentaires dans toutes les conditions.	➤ Procédure pour TLS(P. 13)
IEEE 802.1X	Vous devez effectuer les procédures supplémentaires si la méthode d'authentification IEEE 802.1X est définie sur EAP-TLS.	➤ Procédure pour IEEE 802.1X(P. 28)
IPSec	Vous devez effectuer les procédures supplémentaires si la méthode d'authentification IKE est définie sur la méthode de signature numérique.	➤ Procédure pour IPSec(P. 46)
SIP	Vous devez exécuter les procédures supplémentaires si TLS est utilisé.	➤ Procédure pour SIP(P. 64)
Signature de l'appareil	Vous devez effectuer les procédures supplémentaires dans les cas suivants : <ul style="list-style-type: none"> • Lorsqu'une signature numérique est ajoutée à des fichiers envoyés à l'aide d'une clé pour les signatures d'appareils • Lorsque le cryptage est activé dans les paramètres de cryptage S/MIME 	➤ Procédure pour la signature des appareils(P. 81)

REMARQUE

- Les captures d'écran utilisées dans ce document ne sont qu'un exemple. Elles peuvent différer de celles que vous voyez réellement, selon le modèle de votre appareil.

Procédure pour TLS

- ▶ **Étape 1 : Régénération de la clé et du certificat (pour TLS)(P. 14)**
- ▶ **Étape 2 : Réinitialisation de la clé et du certificat (pour TLS)(P. 22)**
- ▶ **Étape 3 : Suppression d'une clé/un certificat généré(e) dans le passé (pour TLS)(P. 24)**
- ▶ **Étape 4 : Désactivation du certificat (pour TLS)(P. 26)**
- ▶ **Étape 5 : Activation du nouveau certificat (pour TLS)(P. 27)**

Étape 1 : Régénération de la clé et du certificat (pour TLS)

Vous pouvez générer trois types de certificats pour une clé générée avec l'appareil : un certificat auto-signé, un certificat CSR et un certificat SCEP. La procédure diffère selon le type de certificat.

Il se peut que vous ne puissiez pas effectuer les opérations à partir du panneau de contrôle, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

- ▶ Pour un certificat auto-signé(P. 14)
- ▶ Pour un certificat CSR(P. 17)
- ▶ Pour un certificat SCEP(P. 19)

Pour un certificat auto-signé

- ▶ Utilisation du panneau de commande(P. 14)
- ▶ Utilisation de l'interface utilisateur distante(P. 15)

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Réglages de gestion> ▶ <Gestion du périphérique> ▶ <Réglages de certificat> ▶ <Générer une clé> ▶ <Générer clé communication réseau>.
- 3 Configurez les paramètres requis et passez à l'écran suivant.

Exemple d'écran :



a <Nom de clé>

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b <Algorithme signature>

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512. Si vous sélectionnez <RSA> pour **c**, et que vous définissez <Longueur de la clé (bit)> à <1024> ou plus pour **d**, vous pouvez sélectionner les algorithmes de hachage SHA384 et SHA512.

c <Algorithme de clé>

Sélectionnez l'algorithme de clé. Si vous sélectionnez <RSA>, <Longueur de la clé (bit)> s'affiche comme élément de réglage pour **d**. Si vous sélectionnez <ECDSA>, <Type de clé> s'affiche à la place.

d) <Longueur de la clé (bit)>/<Type de clé>

Spécifiez la longueur de la clé si vous sélectionnez <RSA> pour **c**, ou spécifiez le type de clé si vous sélectionnez <ECDSA>. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement de la communication.

4 Configurez les éléments nécessaires pour le certificat ► appuyez sur <Générer une clé>.

Exemple d'écran :



a) <Date de début de validité>/<Date de fin de validité>

Saisissez la date de début et les données de fin de la période de validité du certificat.

b) <Pays/Région>/<Etat>/<Ville>/<Organisation>/<Unité org.>

Sélectionnez le code du pays dans la liste et saisissez l'emplacement et le nom de l'organisation.

c) <Nom commun>

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

■ Utilisation de l'interface utilisateur distante

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].

4 Cliquez sur [Générer une clé].

5 Cliquez sur [Communication réseau].

6 Configurez les paramètres de la clé et du certificat.

a [Nom de clé]

Saisissez un nom pour la clé en utilisant des caractères alphanumériques. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512.

c [Algorithme de clé]

Sélectionnez [RSA] ou [ECDSA] comme algorithme de génération de clé. Spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA]. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement des communications.

REMARQUE :

- Si vous sélectionnez [SHA384] ou [SHA512] pour [Algorithme signature], vous ne pouvez pas définir la longueur de clé sur [512 bits] lorsque vous sélectionnez [RSA] pour [Algorithme de clé].

d [Date de début de validité (AAAA/MM/JJ)]/[Date de fin de validité (AAAA/MM/JJ)]

Saisissez la date de début et les données de fin de la période de validité du certificat. Vous ne pouvez pas définir [Date de fin de validité (AAAA/MM/JJ)] sur une date antérieure à celle de [Date de début de validité (AAAA/MM/JJ)].

e [Pays/Région]

Cliquez sur [Choisir un pays/une région] et sélectionnez le pays/la région dans la liste déroulante. Vous pouvez également cliquer sur [Saisir le code pays Internet] et saisir un code de pays, tel que « US » pour les États-Unis.

f [Etat]/[Ville]

Saisissez l'emplacement en utilisant les caractères alphanumériques nécessaires.

g [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation en utilisant les caractères alphanumériques nécessaires.

h [Nom commun]

Saisissez le nom commun du certificat en utilisant les caractères alphanumériques nécessaires. Le « nom commun » est souvent abrégé par « CN ».

7 Cliquez sur [OK].

- La génération d'une clé et d'un certificat peut prendre un certain temps.
- Les clés et les certificats générés sont automatiquement enregistrés sur l'appareil.

Pour un certificat CSR

Générez une clé et un CSR sur l'appareil. Utilisez les données CSR affichées à l'écran ou sorties dans un fichier pour demander à l'autorité de certification d'émettre un certificat. Ensuite, enregistrez le certificat émis pour la clé. Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

■ 1. Génération d'une clé et d'un CSR

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Cliquez sur [Générer une clé].
- 5 Cliquez sur [Clé et demande de signature de certificat (CSR)].
- 6 Configurez les paramètres de la clé et du certificat.

The screenshot shows the 'Générer clé et demande de signature de certificat (CSR)' interface. The interface is in French and shows various configuration options for generating a key and CSR. The options are grouped into sections: 'Générer clé et demande de signature de certificat (CSR)' and 'Réglages de demande de signature de certificat (CSR)'. The first section includes fields for 'Nom de clé', 'Algorithme signature', and 'Algorithme de clé'. The second section includes fields for 'Pays/Région', 'Etat', 'Ville', 'Organisation', 'Unité d'organisation', and 'Nom complet'. The interface also has a sidebar with navigation options and a top navigation bar.

a [Nom de clé]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Algorithme de clé]

Sélectionnez l'algorithme de clé, et spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA].

d [Pays/Région]

Sélectionnez le code du pays dans la liste ou bien saisissez-le directement.

e [Etat]/[Ville]

Saisissez le lieu.

f [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation.

g [Nom commun]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

7 Cliquez sur [OK].

▢ Les données CSR s'affichent.

- Si vous voulez sauvegarder les données CSR dans un fichier, cliquez sur [Mémoriser dans un fichier] et spécifiez l'emplacement de sauvegarde.

REMARQUE :

- La clé qui a généré la CSR s'affiche sur l'écran de la liste des clés et des certificats, mais vous ne pouvez pas l'utiliser seule. Pour utiliser cette clé, vous devez enregistrer le certificat qui sera émis ultérieurement sur la base de la CSR.

8 Demandez à l'autorité de certification d'émettre un certificat basé sur les données CSR.

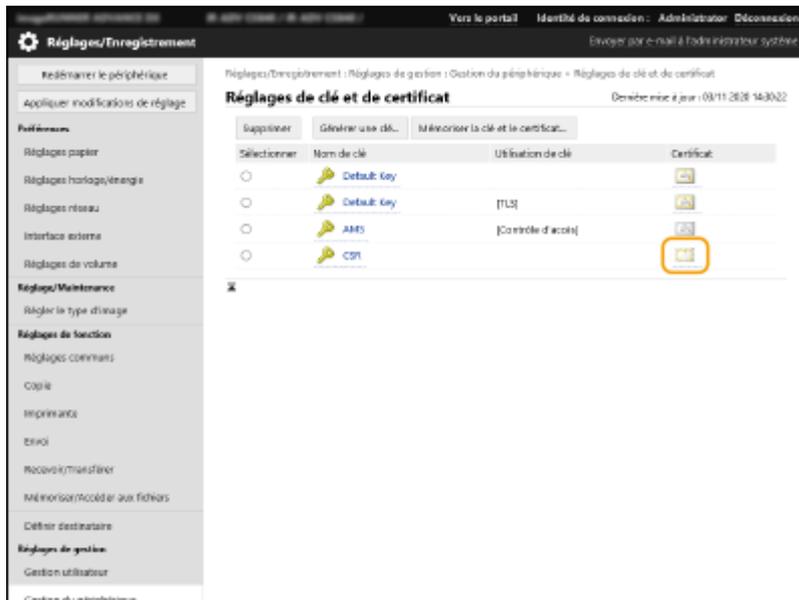
■ 2. Enregistrement du certificat délivré sur la clé

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].

4 Dans la liste [Certificat], cliquez sur pour le certificat que vous voulez enregistrer.



5 Cliquez sur [Mémoriser certificat...].

6 Enregistrez le certificat.

- Cliquez sur [Parcourir...] ► spécifiez le fichier (certificat) à enregistrer ► cliquez sur [Mémoriser].

Pour un certificat SCEP

Demander manuellement au serveur SCEP d'émettre un certificat.
Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

REMARQUE

- Vous ne pouvez pas envoyer une demande manuelle d'émission de certificat si [Activer le minuteur pour la demande automatique de délivrance de certificat] est sélectionné. Désélectionnez-la si elle est sélectionnée.

Lancez l'interface utilisateur distante ► cliquez sur [Réglages/Enregistrement] ► [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)] ► [Réglages pour Demande automatique de délivrance de certificat] ► désélectionnez [Activer le minuteur pour la demande automatique de délivrance de certificat] ► cliquez sur [Mettre à jour].

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)].

4 Cliquez sur [Demande de délivrance de certificat].

5 Configurez les paramètres requis pour la demande d'un certificat.

a [Nom de clé :]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature :]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Longueur de la clé (bit) :]

Sélectionnez la longueur de la clé.

d [Organisation :]

Saisissez le nom de l'organisation.

e [Nom commun :]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

f [Mot de passe de stimulation :]

Lorsqu'un mot de passe est défini côté serveur SCEP, saisissez le mot de passe de challenge inclus dans les données de la demande (PKCS#9) pour demander l'émission d'un certificat.

g [Emplacement d'utilisation de la clé :]

Sélectionnez [TLS].

REMARQUE :

- Si vous sélectionnez une option autre que [Aucun], activez chaque fonction à l'avance. Si un certificat est obtenu avec succès alors que chaque fonction est désactivée, le certificat est affecté à l'emplacement d'utilisation de la clé, mais chaque fonction n'est pas automatiquement activée.

6 Cliquez sur [Envoyer la demande].

7 Cliquez sur [Redémarrer].

Étape 2 : Réinitialisation de la clé et du certificat (pour TLS)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante. Cette procédure n'est pas requise pour un certificat SCEP.

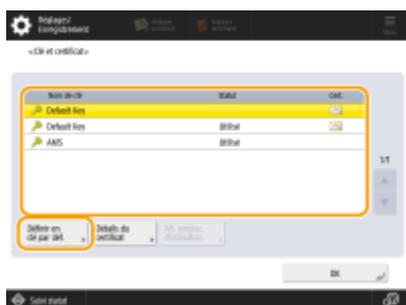
Pour un certificat auto-signé/un certificat CSR

- Utilisation du panneau de commande (P. 22)
- Utilisation de l'interface utilisateur distante (P. 23)

■ Utilisation du panneau de commande

- 1 Appuyez sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Préférences> ► <Réseau> ► <Réglages TCP/IP> ► <Réglages TLS>.
- 3 Appuyez sur <Clé et certificat>.
- 4 Sélectionnez la clé et le certificat à utiliser pour la communication cryptée TLS ► appuyez sur <Définir en clé par déf.> ► <Oui>.

Exemple d'écran :



- Si vous voulez utiliser la clé et le certificat préinstallés, sélectionnez <Default Key>.

REMARQUE :

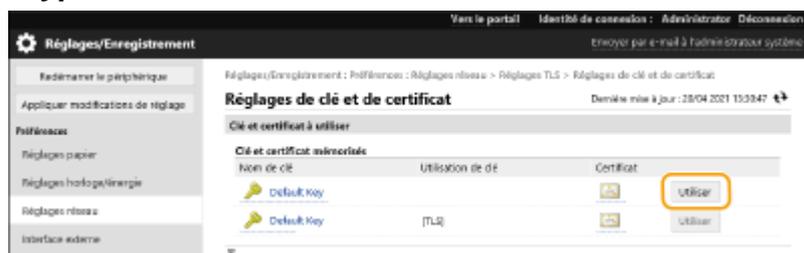
- Les communications cryptées par TLS ne peuvent pas utiliser <Device Signature Key>, qui est utilisé pour les signatures d'appareils, ou <AMS>, qui est utilisé pour les restrictions d'accès.

- 5 Appuyez sur <OK>.
- 6 Appuyez sur  (Réglages/Enregistr.) ► <Appliquer modifications réglages> ► <Oui>.

⇒ L'appareil redémarre, et les réglages sont appliqués.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Réseau] ► [Réglages TLS].**
- 4 Cliquez sur [Clé et certificat].**
- 5 Cliquez sur [Utiliser] pour la clé et le certificat à utiliser pour la communication cryptée TLS.**



- Si vous voulez utiliser la clé et le certificat pré-installés, sélectionnez [Default Key].

- 6 Cliquez sur [Appl. modif. régl.] pour redémarrer l'appareil.**

⇒ L'appareil redémarre, et les réglages sont appliqués.

Étape 3 : Suppression d'une clé/un certificat généré(e) dans le passé (pour TLS)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

REMARQUE

- Vous devrez peut-être transmettre des informations à l'autorité de certification lors de la désactivation du certificat. Consultez **►Vérifier si vous devez effectuer les procédures supplémentaires(P. 5)** et notez les informations requises avant de supprimer la clé/le certificat.

►Utilisation du panneau de commande(P. 24)

►Utilisation de l'interface utilisateur distante(P. 25)

■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Liste de clés et de certificats> ► <Liste clés et certif. pour ce périphérique>.

- <Liste clés et certif. pour ce périphérique> ne s'affiche pas, sauf si la fonction de signature utilisateur est activée sur l'appareil. Dans ce cas, passez à l'étape suivante.

3 Sélectionnez la clé et le certificat ► appuyez sur <Supprimer> ► <Oui>.

Exemple d'écran :



REMARQUE :

- Si  s'affiche, la clé est corrompue ou non valide.
- Si  ne s'affiche pas, le certificat pour la clé n'existe pas.
- Si vous sélectionnez une clé et un certificat et appuyez sur <Détails du certificat>, des informations détaillées sur le certificat s'affichent. Vous pouvez également appuyer sur <Vérifier cert.> sur cet écran pour vérifier si le certificat est valide.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Sélectionnez la clé et le certificat ► cliquez sur [Supprimer] ► [OK].



REMARQUE

- Si s'affiche, la clé est corrompue ou non valide.
- Si s'affiche, le certificat pour la clé n'existe pas.
- Cliquez sur un nom de clé pour afficher des informations détaillées sur le certificat. Vous pouvez aussi appuyer sur [Vérifier le certificat] sur cet écran pour vérifier si le certificat est valide.

Étape 4 : Désactivation du certificat (pour TLS)

Désactivez un certificat généré dans le passé. La procédure diffère selon le type de certificat.

■ Pour un certificat auto-signé

Si un certificat comprenant une clé qui nécessite les procédures supplémentaires est enregistré dans un ordinateur ou un navigateur web en tant que certificat de confiance, supprimez le certificat enregistré.

■ Pour un certificat CSR/SCEP

Demandez à l'autorité de certification qui a émis le certificat de le révoquer. Reportez-vous à [Créateur] dans le certificat pour connaître l'autorité de certification à demander.

REMARQUE

- Si vous vérifiez la révocation des certificats à l'aide d'une CRL dans un ordinateur ou un navigateur web qui communique avec l'appareil, enregistrez la CRL mise à jour sur l'ordinateur ou le navigateur web après la révocation du certificat.
- Si vous utilisez une méthode autre qu'une CRL (par exemple, OCSP) pour vérifier la révocation des certificats, effectuez la procédure correspondant à cette méthode.

Étape 5 : Activation du nouveau certificat (pour TLS)

Activez le certificat qui vient d'être généré sur l'appareil.

■ Pour un certificat auto-signé

Enregistrez le nouveau certificat sur l'ordinateur ou le navigateur Web en tant que certificat de confiance.

■ Pour un certificat CSR/SCEP

Vous n'avez pas besoin d'effectuer les procédures supplémentaires.

Procédure pour IEEE 802.1X

- ▶ **Étape 1 : Vérification de la méthode d'authentification (pour IEEE 802.1X)(P. 29)**
- ▶ **Étape 2 : Régénération de la clé et du certificat (pour IEEE 802.1X)(P. 31)**
- ▶ **Étape 3 : réinitialisation de la clé et du certificat (pour IEEE 802.1X)(P. 39)**
- ▶ **Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IEEE 802.1X)(P. 42)**
- ▶ **Étape 5 : désactivation du certificat (pour IEEE 802.1X)(P. 44)**
- ▶ **Étape 6 : Activation du nouveau certificat (pour IEEE 802.1X)(P. 45)**

Étape 1 : Vérification de la méthode d'authentification (pour IEEE 802.1X)

Vous devez effectuer les procédures suivantes si la méthode d'authentification IEEE 802.1X est définie sur EAP-TLS. Suivez la procédure ci-dessous pour vérifier la méthode d'authentification.

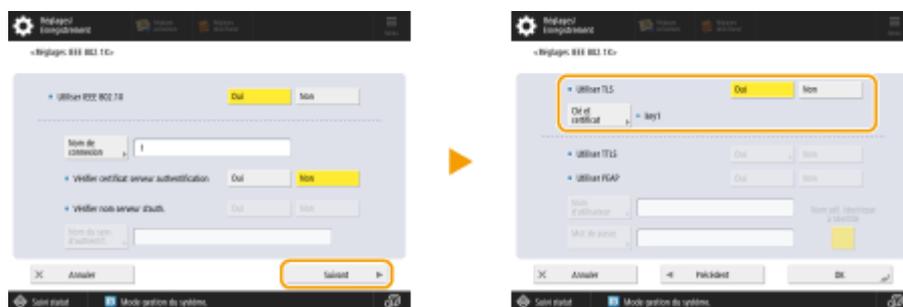
Il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

- ▶ Utilisation du panneau de commande(P. 29)
- ▶ Utilisation de l'interface utilisateur distante(P. 29)

■ Utilisation du panneau de commande

- 1 Appuyez sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Préférences> ▶ <Réseau> ▶ <Réglages IEEE 802.1X>.
- 3 Appuyez sur <Suivant> ▶ vérifiez <Utiliser TLS>.

Exemple d'écran :



- Si <Utiliser TLS> est réglé sur <Oui> et qu'un nom de clé s'affiche pour <Clé et certificat>, effectuez les procédures suivantes.
- Si <Utiliser TLS> est réglé sur <Non>, vous n'avez pas besoin d'effectuer les procédures suivantes.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Réseau] ▶ [Réglages IEEE 802.1X].

4 Vérifiez [Utiliser TLS].

Réglages/Enregistrement : Préférences : Réglages réseau > Réglages IEEE 802.1X
Réglages IEEE 802.1X Dernière mise à jour : 08/03 2022 15:18:53

Utiliser IEEE 802.1X
Nom de connexion :

Vérifier le certificat du serveur d'authentification
 Vérifier le nom du serveur d'authentification
Nom du serveur d'authentification :

Utiliser TLS
*Définir la clé par défaut dans les Réglages de clé et de certificat sous [Réglages TLS] pour utiliser TLS.
Nom de clé :
Clé et certificat :

Utiliser TTLS
Réglages TTLS (Protocole TTLS) : Utiliser MSCHAPv2 Utiliser PAP

- Si [Utiliser TLS] est sélectionné et qu'un nom de clé s'affiche, effectuez les procédures suivantes.
- Si [Utiliser TLS] est désélectionné, vous n'avez pas besoin d'effectuer les procédures suivantes.

Étape 2 : Régénération de la clé et du certificat (pour IEEE 802.1X)

Vous pouvez générer trois types de certificats pour une clé générée avec l'appareil : un certificat auto-signé, un certificat CSR et un certificat SCEP. La procédure diffère selon le type de certificat.

Il se peut que vous ne puissiez pas effectuer les opérations à partir du panneau de contrôle, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

- ▶ Pour un certificat auto-signé(P. 31)
- ▶ Pour un certificat CSR(P. 34)
- ▶ Pour un certificat SCEP(P. 36)

Pour un certificat auto-signé

- ▶ Utilisation du panneau de commande(P. 31)
- ▶ Utilisation de l'interface utilisateur distante(P. 32)

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Réglages de gestion> ▶ <Gestion du périphérique> ▶ <Réglages de certificat> ▶ <Générer une clé> ▶ <Générer clé communication réseau>.
- 3 Configurez les paramètres requis et passez à l'écran suivant.

Exemple d'écran :



a <Nom de clé>

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b <Algorithme signature>

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512. Si vous sélectionnez <RSA> pour **c**, et que vous définissez <Longueur de la clé (bit)> à <1024> ou plus pour **d**, vous pouvez sélectionner les algorithmes de hachage SHA384 et SHA512.

c <Algorithme de clé>

Sélectionnez l'algorithme de clé. Si vous sélectionnez <RSA>, <Longueur de la clé (bit)> s'affiche comme élément de réglage pour **d**. Si vous sélectionnez <ECDSA>, <Type de clé> s'affiche à la place.

d) <Longueur de la clé (bit)>/<Type de clé>

Spécifiez la longueur de la clé si vous sélectionnez <RSA> pour **c**, ou spécifiez le type de clé si vous sélectionnez <ECDSA>. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement de la communication.

4 Configurez les éléments nécessaires pour le certificat ► appuyez sur <Générer une clé>.

Exemple d'écran :



a) <Date de début de validité>/<Date de fin de validité>

Saisissez la date de début et les données de fin de la période de validité du certificat.

b) <Pays/Région>/<Etat>/<Ville>/<Organisation>/<Unité org.>

Sélectionnez le code du pays dans la liste et saisissez l'emplacement et le nom de l'organisation.

c) <Nom commun>

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].**
- 4 Cliquez sur [Générer une clé].**
- 5 Cliquez sur [Communication réseau].**

6 Configurez les paramètres de la clé et du certificat.

a [Nom de clé]

Saisissez un nom pour la clé en utilisant des caractères alphanumériques. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512.

c [Algorithme de clé]

Sélectionnez [RSA] ou [ECDSA] comme algorithme de génération de clé. Spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA]. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement des communications.

REMARQUE :

- Si vous sélectionnez [SHA384] ou [SHA512] pour [Algorithme signature], vous ne pouvez pas définir la longueur de clé sur [512 bits] lorsque vous sélectionnez [RSA] pour [Algorithme de clé].

d [Date de début de validité (AAAA/MM/JJ)]/[Date de fin de validité (AAAA/MM/JJ)]

Saisissez la date de début et les données de fin de la période de validité du certificat. Vous ne pouvez pas définir [Date de fin de validité (AAAA/MM/JJ)] sur une date antérieure à celle de [Date de début de validité (AAAA/MM/JJ)].

e [Pays/Région]

Cliquez sur [Choisir un pays/une région] et sélectionnez le pays/la région dans la liste déroulante. Vous pouvez également cliquer sur [Saisir le code pays Internet] et saisir un code de pays, tel que « US » pour les États-Unis.

f [Etat]/[Ville]

Saisissez l'emplacement en utilisant les caractères alphanumériques nécessaires.

g [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation en utilisant les caractères alphanumériques nécessaires.

h [Nom commun]

Saisissez le nom commun du certificat en utilisant les caractères alphanumériques nécessaires. Le « nom commun » est souvent abrégé par « CN ».

7 Cliquez sur [OK].

- La génération d'une clé et d'un certificat peut prendre un certain temps.
- Les clés et les certificats générés sont automatiquement enregistrés sur l'appareil.

Pour un certificat CSR

Générez une clé et un CSR sur l'appareil. Utilisez les données CSR affichées à l'écran ou sorties dans un fichier pour demander à l'autorité de certification d'émettre un certificat. Ensuite, enregistrez le certificat émis pour la clé. Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

■ 1. Génération d'une clé et d'un CSR

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Cliquez sur [Générer une clé].
- 5 Cliquez sur [Clé et demande de signature de certificat (CSR)].
- 6 Configurez les paramètres de la clé et du certificat.

a [Nom de clé]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Algorithme de clé]

Sélectionnez l'algorithme de clé, et spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA].

d [Pays/Région]

Sélectionnez le code du pays dans la liste ou bien saisissez-le directement.

e [Etat]/[Ville]

Saisissez le lieu.

f [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation.

g [Nom commun]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

7 Cliquez sur [OK].

▢ Les données CSR s'affichent.

- Si vous voulez sauvegarder les données CSR dans un fichier, cliquez sur [Mémoriser dans un fichier] et spécifiez l'emplacement de sauvegarde.

REMARQUE :

- La clé qui a généré la CSR s'affiche sur l'écran de la liste des clés et des certificats, mais vous ne pouvez pas l'utiliser seule. Pour utiliser cette clé, vous devez enregistrer le certificat qui sera émis ultérieurement sur la base de la CSR.

8 Demandez à l'autorité de certification d'émettre un certificat basé sur les données CSR.

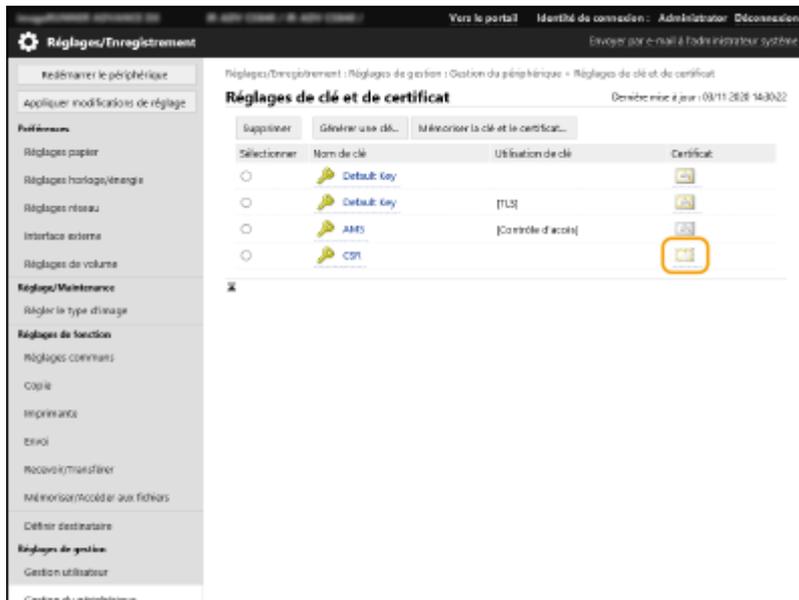
■ 2. Enregistrement du certificat délivré sur la clé

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].

4 Dans la liste [Certificat], cliquez sur pour le certificat que vous voulez enregistrer.



5 Cliquez sur [Mémoriser certificat...].

6 Enregistrez le certificat.

- Cliquez sur [Parcourir...] ► spécifiez le fichier (certificat) à enregistrer ► cliquez sur [Mémoriser].

Pour un certificat SCEP

Demander manuellement au serveur SCEP d'émettre un certificat.
Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

REMARQUE

- Vous ne pouvez pas envoyer une demande manuelle d'émission de certificat si [Activer le minuteur pour la demande automatique de délivrance de certificat] est sélectionné. Désélectionnez-la si elle est sélectionnée.

Lancez l'interface utilisateur distante ► cliquez sur [Réglages/Enregistrement] ► [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)] ► [Réglages pour Demande automatique de délivrance de certificat] ► désélectionnez [Activer le minuteur pour la demande automatique de délivrance de certificat] ► cliquez sur [Mettre à jour].

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)].

4 Cliquez sur [Demande de délivrance de certificat].

5 Configurez les paramètres requis pour la demande d'un certificat.

a [Nom de clé :]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature :]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Longueur de la clé (bit) :]

Sélectionnez la longueur de la clé.

d [Organisation :]

Saisissez le nom de l'organisation.

e [Nom commun :]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

f [Mot de passe de stimulation :]

Lorsqu'un mot de passe est défini côté serveur SCEP, saisissez le mot de passe de challenge inclus dans les données de la demande (PKCS#9) pour demander l'émission d'un certificat.

g [Emplacement d'utilisation de la clé :]

Sélectionnez [IEEE 802.1X].

REMARQUE :

- Si vous sélectionnez une option autre que [Aucun], activez chaque fonction à l'avance. Si un certificat est obtenu avec succès alors que chaque fonction est désactivée, le certificat est affecté à l'emplacement d'utilisation de la clé, mais chaque fonction n'est pas automatiquement activée.

6 Cliquez sur [Envoyer la demande].

7 Cliquez sur [Redémarrer].

Étape 3 : réinitialisation de la clé et du certificat (pour IEEE 802.1X)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante. Cette procédure n'est pas requise pour un certificat SCEP.

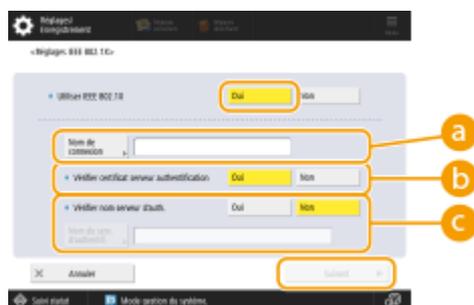
Pour un certificat auto-signé/un certificat CSR

- ▶ Utilisation du panneau de commande (P. 39)
- ▶ Utilisation de l'interface utilisateur distante (P. 40)

■ Utilisation du panneau de commande

- 1 Appuyez sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Préférences> ▶ <Réseau> ▶ <Réglages IEEE 802.1X>.
- 3 Appuyez sur <Oui> pour <Utiliser IEEE 802.1X> ▶ configurez les paramètres requis ▶ appuyez sur <Suivant>.

Exemple d'écran :



a <Nom de connexion>

Saisissez le nom (identité EAP) de l'utilisateur se connectant pour recevoir l'authentification IEEE 802.1X.

b <Vérifier certificat serveur authentification>

Définissez ce réglage sur <Oui> lors de la vérification des certificats du serveur envoyés à partir d'un serveur d'authentification.

c <Vérifier nom serveur d'auth.>

Pour vérifier un nom commun dans le certificat du serveur, sélectionnez <Oui>. Saisissez ensuite le nom du serveur d'authentification où l'utilisateur de connexion est enregistré dans <Nom du serv. d'authentif.>.

- 4 Appuyez sur <Oui> pour <Utiliser TLS> ▶ appuyez sur <Clé et certificat>.

5 Sélectionnez la clé et le certificat à utiliser dans la liste ► appuyez sur <Définir en clé par déf.> ► <Oui>.

6 Appuyez sur <OK>.

7 Appuyez sur  (Réglages/Enregistr.) ►  (Réglages/Enregistr.) ► <Appl. modif. régl.> ► <Oui>.

►► L'appareil redémarre, et les réglages sont appliqués.

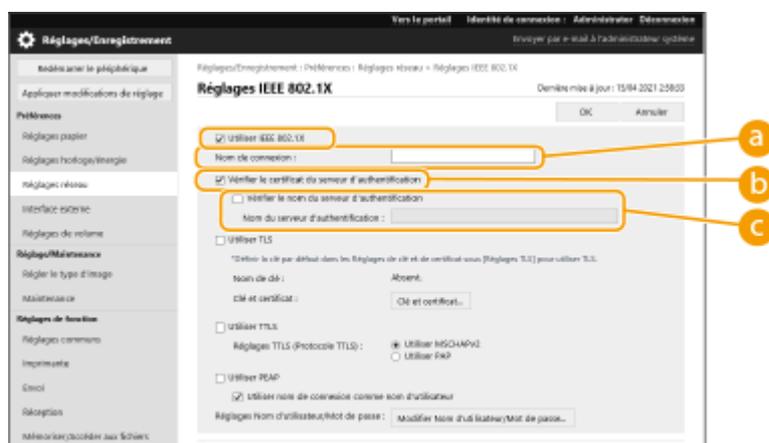
■ Utilisation de l'interface utilisateur distante

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Réglages réseau] ► [Réglages IEEE 802.1X].

4 Sélectionnez [Utiliser IEEE 802.1X] ► pour configurer les paramètres requis.



a [Nom de connexion]

Saisissez le nom (identité EAP) de l'utilisateur se connectant pour recevoir l'authentification IEEE 802.1X.

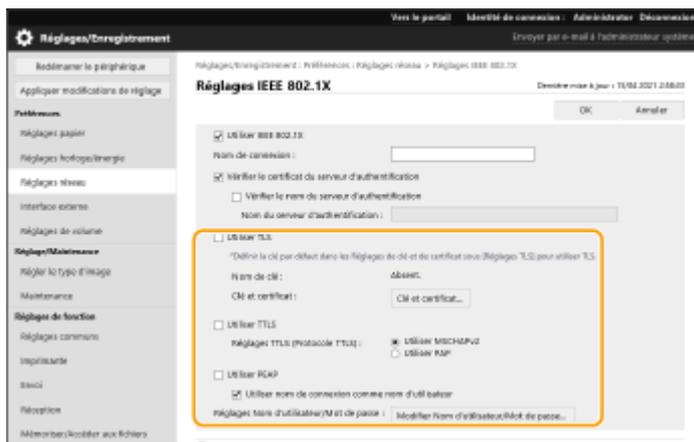
b [Vérifier le certificat du serveur d'authentification]

Cochez cette case lors de la vérification des certificats du serveur envoyés à partir d'un serveur d'authentification.

c [Vérifier le nom du serveur d'authentification]

Pour vérifier le nom commun dans le certificat du serveur, cochez cette case. Ensuite, entrez le nom du serveur d'authentification où l'utilisateur de connexion est enregistré dans [Nom du serveur d'authentification].

5 Sélectionnez [Utiliser TLS] ► cliquez sur [Clé et certificat].



6 Cliquez sur [Utiliser] pour la clé à utiliser dans la liste.

7 Cliquez sur [OK].

8 Cliquez sur [Appliquer modifications de réglage] pour redémarrer l'appareil.

⇒ L'appareil redémarre, et les réglages sont appliqués.

Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IEEE 802.1X)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

REMARQUE

- Vous devrez peut-être transmettre des informations à l'autorité de certification lors de la désactivation du certificat. Consultez **►Vérifier si vous devez effectuer les procédures supplémentaires(P. 5)** et notez les informations requises avant de supprimer la clé/le certificat.

►Utilisation du panneau de commande(P. 42)

►Utilisation de l'interface utilisateur distante(P. 43)

■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Liste de clés et de certificats> ► <Liste clés et certif. pour ce périphérique>.

- <Liste clés et certif. pour ce périphérique> ne s'affiche pas, sauf si la fonction de signature utilisateur est activée sur l'appareil. Dans ce cas, passez à l'étape suivante.

3 Sélectionnez la clé et le certificat ► appuyez sur <Supprimer> ► <Oui>.

Exemple d'écran :



REMARQUE :

- Si  s'affiche, la clé est corrompue ou non valide.
- Si  ne s'affiche pas, le certificat pour la clé n'existe pas.
- Si vous sélectionnez une clé et un certificat et appuyez sur <Détails du certificat>, des informations détaillées sur le certificat s'affichent. Vous pouvez également appuyer sur <Vérifier cert.> sur cet écran pour vérifier si le certificat est valide.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Sélectionnez la clé et le certificat ► cliquez sur [Supprimer] ► [OK].



REMARQUE

- Si s'affiche, la clé est corrompue ou non valide.
- Si s'affiche, le certificat pour la clé n'existe pas.
- Cliquez sur un nom de clé pour afficher des informations détaillées sur le certificat. Vous pouvez aussi appuyer sur [Vérifier le certificat] sur cet écran pour vérifier si le certificat est valide.

Étape 5 : désactivation du certificat (pour IEEE 802.1X)

Désactivez un certificat généré dans le passé. La procédure diffère selon le type de certificat.

■ Pour un certificat auto-signé

Si un certificat comprenant une clé qui nécessite les procédures supplémentaires est enregistré auprès du serveur d'authentification IEEE 802.1X en tant que certificat de confiance, supprimez le certificat enregistré.

■ Pour un certificat CSR/SCEP

Demandez à l'autorité de certification qui a émis le certificat de le révoquer. Reportez-vous à [Créateur] dans le certificat pour connaître l'autorité de certification à demander.

REMARQUE

- Si vous vérifiez la révocation des certificats à l'aide d'une CRL dans un serveur d'authentification IEEE 802.1X, enregistrez la CRL mise à jour sur l'ordinateur ou le navigateur web après la révocation du certificat.
- Si vous utilisez une méthode autre qu'une CRL (par exemple, OCSP) pour vérifier la révocation des certificats, effectuez la procédure correspondant à cette méthode.

Étape 6 : Activation du nouveau certificat (pour IEEE 802.1X)

Activez le certificat.

■ Pour un certificat auto-signé

Enregistrez le nouveau certificat auprès du serveur d'authentification IEEE 802.1X en tant que certificat de confiance.

■ Pour un certificat CSR/SCEP

Vous n'avez pas besoin d'effectuer les procédures supplémentaires.

Procédure pour IPSec

- ▶ **Étape 1 : Vérification de la méthode d'authentification (pour IPSec)(P. 47)**
- ▶ **Étape 2 : Régénération de la clé et du certificat (pour IPSec)(P. 49)**
- ▶ **Étape 3 : Réinitialisation de la clé et du certificat (pour IPSec)(P. 57)**
- ▶ **Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IPSec)(P. 60)**
- ▶ **Étape 5 : Désactivation du certificat (pour IPSec)(P. 62)**
- ▶ **Étape 6 : Activation du nouveau certificat (pour IPSec)(P. 63)**

Étape 1 : Vérification de la méthode d'authentification (pour IPSec)

Vous devez effectuer les procédures suivantes si la méthode d'authentification pour le paramètre IKE dans IPSec est définie sur <Méthode sign. num.>.

Suivez la procédure ci-dessous pour vérifier la méthode d'authentification.

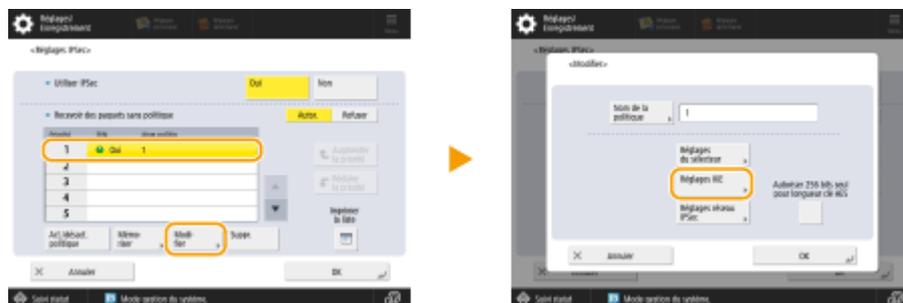
Il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de commande, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

- ▶ Utilisation du panneau de commande(P. 47)
- ▶ Utilisation de l'interface utilisateur distante(P. 48)

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Préférences> ▶ <Réseau> ▶ <Réglages TCP/IP> ▶ <Réglages IPSec>.
- 3 Sélectionnez la politique enregistrée ▶, appuyez sur <Modifier> ▶ <Réglages IKE>.

Exemple d'écran :



- 4 Appuyez sur <Suivant> ▶ vérifiez <Méthode d'authentification>.

Exemple d'écran :



- Si <Méthode d'authentification> est réglé sur <Méthode sign. num.> et qu'un nom de clé s'affiche pour <Clé et certificat>, effectuez les procédures suivantes.
- Si <Méthode d'authentification> est réglé sur <Méth. clé prépartagée>, vous n'avez pas besoin d'effectuer les procédures suivantes.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Réglages réseau] ► [Liste de politique IPSec].**
- 4 Cliquez sur la politique dans la liste ► cliquez sur [Réglages IKE].**
- 5 Vérifiez [Méthode d'authentification].**



- Si [Méthode d'authentification] est réglé sur [Méthode de signature numérique] et qu'un nom de clé s'affiche, effectuez les procédures suivantes.
- Si <Méthode d'authentification> est réglé sur <Méthode clé prépartagée>, vous n'avez pas besoin d'effectuer les procédures suivantes.

Étape 2 : Régénération de la clé et du certificat (pour IPSec)

Vous pouvez générer trois types de certificats pour une clé générée avec l'appareil : un certificat auto-signé, un certificat CSR et un certificat SCEP. La procédure diffère selon le type de certificat.

Il se peut que vous ne puissiez pas effectuer les opérations à partir du panneau de contrôle, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

- ▶ Pour un certificat auto-signé(P. 49)
- ▶ Pour un certificat CSR(P. 52)
- ▶ Pour un certificat SCEP(P. 54)

Pour un certificat auto-signé

- ▶ Utilisation du panneau de commande(P. 49)
- ▶ Utilisation de l'interface utilisateur distante(P. 50)

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Réglages de gestion> ▶ <Gestion du périphérique> ▶ <Réglages de certificat> ▶ <Générer une clé> ▶ <Générer clé communication réseau>.
- 3 Configurez les paramètres requis et passez à l'écran suivant.

Exemple d'écran :



a <Nom de clé>

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b <Algorithme signature>

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512. Si vous sélectionnez <RSA> pour **c**, et que vous définissez <Longueur de la clé (bit)> à <1024> ou plus pour **d**, vous pouvez sélectionner les algorithmes de hachage SHA384 et SHA512.

c <Algorithme de clé>

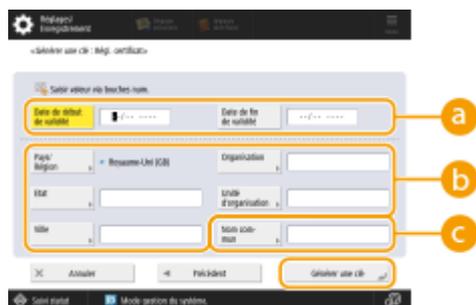
Sélectionnez l'algorithme de clé. Si vous sélectionnez <RSA>, <Longueur de la clé (bit)> s'affiche comme élément de réglage pour **d**. Si vous sélectionnez <ECDSA>, <Type de clé> s'affiche à la place.

d <Longueur de la clé (bit)>/<Type de clé>

Spécifiez la longueur de la clé si vous sélectionnez <RSA> pour **c**, ou spécifiez le type de clé si vous sélectionnez <ECDSA>. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement de la communication.

4 Configurez les éléments nécessaires pour le certificat ► appuyez sur <Générer une clé>.

Exemple d'écran :



a <Date de début de validité>/<Date de fin de validité>

Saisissez la date de début et les données de fin de la période de validité du certificat.

b <Pays/Région>/<Etat>/<Ville>/<Organisation>/<Unité org.>

Sélectionnez le code du pays dans la liste et saisissez l'emplacement et le nom de l'organisation.

c <Nom commun>

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

■ Utilisation de l'interface utilisateur distante

- 1** Lancez l'interface utilisateur distante.
- 2** Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3** Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4** Cliquez sur [Générer une clé].
- 5** Cliquez sur [Communication réseau].

6 Configurez les paramètres de la clé et du certificat.

a [Nom de clé]

Saisissez un nom pour la clé en utilisant des caractères alphanumériques. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512.

c [Algorithme de clé]

Sélectionnez [RSA] ou [ECDSA] comme algorithme de génération de clé. Spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA]. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement des communications.

REMARQUE :

- Si vous sélectionnez [SHA384] ou [SHA512] pour [Algorithme signature], vous ne pouvez pas définir la longueur de clé sur [512 bits] lorsque vous sélectionnez [RSA] pour [Algorithme de clé].

d [Date de début de validité (AAAA/MM/JJ)]/[Date de fin de validité (AAAA/MM/JJ)]

Saisissez la date de début et les données de fin de la période de validité du certificat. Vous ne pouvez pas définir [Date de fin de validité (AAAA/MM/JJ)] sur une date antérieure à celle de [Date de début de validité (AAAA/MM/JJ)].

e [Pays/Région]

Cliquez sur [Choisir un pays/une région] et sélectionnez le pays/la région dans la liste déroulante. Vous pouvez également cliquer sur [Saisir le code pays Internet] et saisir un code de pays, tel que « US » pour les États-Unis.

f [Etat]/[Ville]

Saisissez l'emplacement en utilisant les caractères alphanumériques nécessaires.

g [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation en utilisant les caractères alphanumériques nécessaires.

h [Nom commun]

Saisissez le nom commun du certificat en utilisant les caractères alphanumériques nécessaires. Le « nom commun » est souvent abrégé par « CN ».

7 Cliquez sur [OK].

- La génération d'une clé et d'un certificat peut prendre un certain temps.
- Les clés et les certificats générés sont automatiquement enregistrés sur l'appareil.

Pour un certificat CSR

Générez une clé et un CSR sur l'appareil. Utilisez les données CSR affichées à l'écran ou sorties dans un fichier pour demander à l'autorité de certification d'émettre un certificat. Ensuite, enregistrez le certificat émis pour la clé. Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

■ 1. Génération d'une clé et d'un CSR

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Cliquez sur [Générer une clé].
- 5 Cliquez sur [Clé et demande de signature de certificat (CSR)].
- 6 Configurez les paramètres de la clé et du certificat.

The screenshot shows the 'Générer clé et demande de signature de certificat (CSR)' interface. The interface is in French and shows various configuration options for generating a key and CSR. The options are highlighted with orange boxes and labeled with letters a through g. The labels are: a (Nom de clé), b (Algorithme signature), c (Algorithme de clé), d (Pays/Région), e (Etat), f (Organisation), g (Nom complet).

a [Nom de clé]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Algorithme de clé]

Sélectionnez l'algorithme de clé, et spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA].

d [Pays/Région]

Sélectionnez le code du pays dans la liste ou bien saisissez-le directement.

e [Etat]/[Ville]

Saisissez le lieu.

f [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation.

g [Nom commun]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

7 Cliquez sur [OK].

▢ Les données CSR s'affichent.

- Si vous voulez sauvegarder les données CSR dans un fichier, cliquez sur [Mémoriser dans un fichier] et spécifiez l'emplacement de sauvegarde.

REMARQUE :

- La clé qui a généré la CSR s'affiche sur l'écran de la liste des clés et des certificats, mais vous ne pouvez pas l'utiliser seule. Pour utiliser cette clé, vous devez enregistrer le certificat qui sera émis ultérieurement sur la base de la CSR.

8 Demandez à l'autorité de certification d'émettre un certificat basé sur les données CSR.

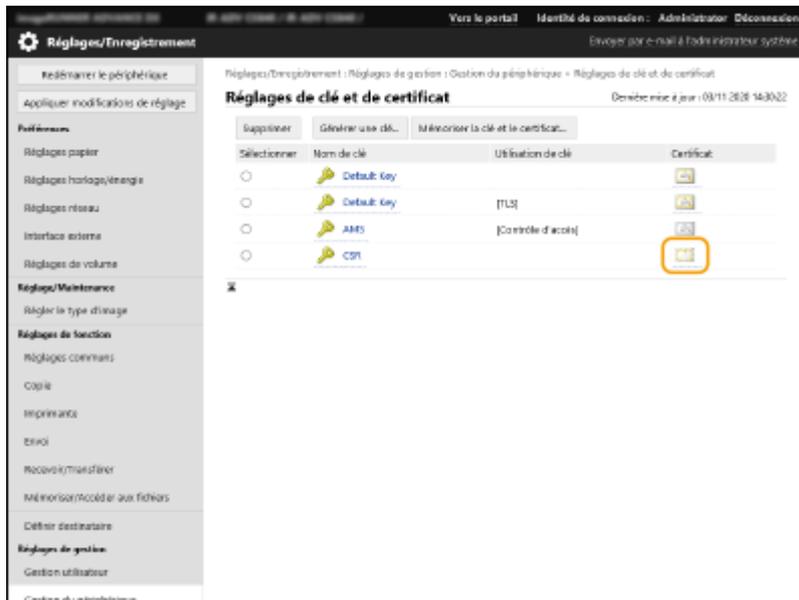
■ 2. Enregistrement du certificat délivré sur la clé

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].

4 Dans la liste [Certificat], cliquez sur pour le certificat que vous voulez enregistrer.



5 Cliquez sur [Mémoriser certificat...].

6 Enregistrez le certificat.

- Cliquez sur [Parcourir...] ► spécifiez le fichier (certificat) à enregistrer ► cliquez sur [Mémoriser].

Pour un certificat SCEP

Demander manuellement au serveur SCEP d'émettre un certificat.
Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

REMARQUE

- Vous ne pouvez pas envoyer une demande manuelle d'émission de certificat si [Activer le minuteur pour la demande automatique de délivrance de certificat] est sélectionné. Désélectionnez-la si elle est sélectionnée.

Lancez l'interface utilisateur distante ► cliquez sur [Réglages/Enregistrement] ► [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)] ► [Réglages pour Demande automatique de délivrance de certificat] ► désélectionnez [Activer le minuteur pour la demande automatique de délivrance de certificat] ► cliquez sur [Mettre à jour].

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages pour Demande de délivrance de certificat (SCEP)].

4 Cliquez sur [Demande de délivrance de certificat].

5 Configurez les paramètres requis pour la demande d'un certificat.

a [Nom de clé :]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature :]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Longueur de la clé (bit) :]

Sélectionnez la longueur de la clé.

d [Organisation :]

Saisissez le nom de l'organisation.

e [Nom commun :]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

f [Mot de passe de stimulation :]

Lorsqu'un mot de passe est défini côté serveur SCEP, saisissez le mot de passe de challenge inclus dans les données de la demande (PKCS#9) pour demander l'émission d'un certificat.

g [Emplacement d'utilisation de la clé :]

Sélectionnez [IPSec].

REMARQUE :

- Si vous sélectionnez une option autre que [Aucun], activez chaque fonction à l'avance. Si un certificat est obtenu avec succès alors que chaque fonction est désactivée, le certificat est affecté à l'emplacement d'utilisation de la clé, mais chaque fonction n'est pas automatiquement activée.

6 Cliquez sur [Envoyer la demande].

7 Cliquez sur [Redémarrer].

Étape 3 : Réinitialisation de la clé et du certificat (pour IPSec)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante. Cette procédure n'est pas requise pour un certificat SCEP.

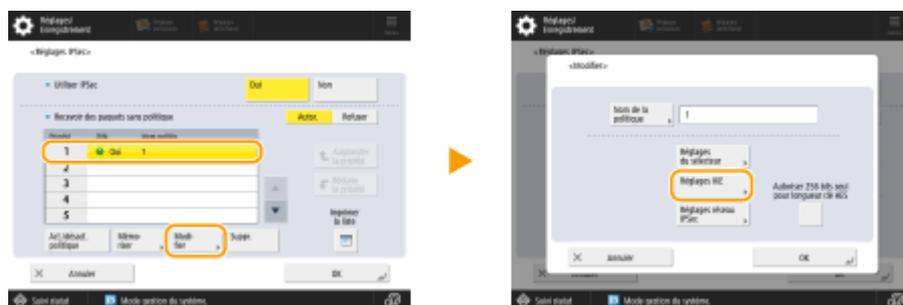
Pour un certificat auto-signé/un certificat CSR

- Utilisation du panneau de commande (P. 57)
- Utilisation de l'interface utilisateur distante (P. 58)

■ Utilisation du panneau de commande

- 1 Appuyer sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Préférences> ► <Réseau> ► <Réglages TCP/IP> ► <Réglages IPSec>.
- 3 Sélectionnez la politique de réinitialisation de la clé et du certificat pour ► appuyez sur <Modifier> ► <Réglages IKE>.

Exemple d'écran :



- 4 Appuyez sur <Suivant> ► sélectionnez <Méthode sign. num.> dans <Méthode d'authentification> ► appuyez sur <Clé et certificat>.

Exemple d'écran :



5 Sélectionnez la clé et le certificat à utiliser dans la liste ► appuyez sur <Définir en clé par déf.> ► <Oui>.

6 Appuyez sur <OK>.

7 Appuyez sur  (Réglages/Enregistr.) ►  (Réglages/Enregistr.) ► <Appl. modif. régl.> ► <Oui>.

⇒ L'appareil redémarre, et les réglages sont appliqués.

■ Utilisation de l'interface utilisateur distante

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Réglages réseau] ► [Liste de politique IPsec].

4 Cliquez sur la politique à réinitialiser la clé et le certificat pour dans la liste ► cliquez sur [Réglages IKE].

5 Sélectionnez [Méthode de signature numérique] dans [Méthode d'authentification] ► cliquez sur [Clé et certificat].



Réglages/Enregistrement : Préférences : Réglages réseau > Liste de politique IPsec > Mémoriser politique > IKE

IKE Dernière mise à jour : 08/03 2022 15:19:45

OK Annuler

Mode IKE

Principal

Agressif

Validité

Durée min (1-65535)

Méthode d'authentification

Méthode de prépartagée :

Méthode de signature numérique :

Nom de clé :

Clé et certificat :

6 Cliquez sur [Utiliser] pour la clé à utiliser dans la liste.

7 Cliquez sur [OK].

8 Cliquez sur [Appliquer modifications de réglage] pour redémarrer l'appareil.

⇒ L'appareil redémarre, et les réglages sont appliqués.

Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour IPSec)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

REMARQUE

- Vous devrez peut-être transmettre des informations à l'autorité de certification lors de la désactivation du certificat. Consultez **►Vérifier si vous devez effectuer les procédures supplémentaires(P. 5)** et notez les informations requises avant de supprimer la clé/le certificat.

►Utilisation du panneau de commande(P. 60)

►Utilisation de l'interface utilisateur distante(P. 61)

■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Liste de clés et de certificats> ► <Liste clés et certif. pour ce périphérique>.

- <Liste clés et certif. pour ce périphérique> ne s'affiche pas, sauf si la fonction de signature utilisateur est activée sur l'appareil. Dans ce cas, passez à l'étape suivante.

3 Sélectionnez la clé et le certificat ► appuyez sur <Supprimer> ► <Oui>.

Exemple d'écran :



REMARQUE :

- Si  s'affiche, la clé est corrompue ou non valide.
- Si  ne s'affiche pas, le certificat pour la clé n'existe pas.
- Si vous sélectionnez une clé et un certificat et appuyez sur <Détails du certificat>, des informations détaillées sur le certificat s'affichent. Vous pouvez également appuyer sur <Vérifier cert.> sur cet écran pour vérifier si le certificat est valide.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Sélectionnez la clé et le certificat ► cliquez sur [Supprimer] ► [OK].



REMARQUE

- Si s'affiche, la clé est corrompue ou non valide.
- Si s'affiche, le certificat pour la clé n'existe pas.
- Cliquez sur un nom de clé pour afficher des informations détaillées sur le certificat. Vous pouvez aussi appuyer sur [Vérifier le certificat] sur cet écran pour vérifier si le certificat est valide.

Étape 5 : Désactivation du certificat (pour IPSec)

Désactivez un certificat généré dans le passé. La procédure diffère selon le type de certificat.

■ Pour un certificat auto-signé

Si un certificat comprenant une clé qui nécessite les procédures supplémentaires est enregistré dans l'appareil qui communique avec IPSec en tant que certificat de confiance, supprimez le certificat enregistré. Après avoir supprimé le certificat enregistré, enregistrez le certificat de la clé régénérée.

■ Pour un certificat CSR/SCEP

Demandez à l'autorité de certification qui a émis le certificat de le révoquer. Reportez-vous à [Créateur] dans le certificat pour connaître l'autorité de certification à demander.

REMARQUE

- Si vous vérifiez la révocation des certificats à l'aide d'une CRL sur l'appareil qui communique avec IPSec, enregistrez la CRL mise à jour sur l'ordinateur ou le navigateur web après la révocation du certificat.
- Si vous utilisez une méthode autre qu'une CRL (par exemple, OCSP) pour vérifier la révocation des certificats, effectuez la procédure correspondant à cette méthode.

Étape 6 : Activation du nouveau certificat (pour IPSec)

Activez le certificat.

■ Pour un certificat auto-signé

Enregistrez le nouveau certificat sur l'appareil qui communique avec IPSec en tant que certificat de confiance.

■ Pour un certificat CSR/SCEP

Vous n'avez pas besoin d'effectuer les procédures supplémentaires.

Procédure pour SIP

- ▶ **Étape 1 : Vérification des paramètres (pour SIP)(P. 65)**
- ▶ **Étape 2 : Régénération de la clé et du certificat (pour SIP)(P. 68)**
- ▶ **Étape 3 : Réinitialisation de la clé et du certificat (pour SIP)(P. 74)**
- ▶ **Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour SIP)(P. 77)**
- ▶ **Étape 5 : Désactiver le certificat (pour SIP)(P. 79)**
- ▶ **Étape 6 : Activation du nouveau certificat (pour SIP)(P. 80)**

Étape 1 : Vérification des paramètres (pour SIP)

Vous devez effectuer les procédures supplémentaires lorsque les deux conditions suivantes sont réunies :

- <Utiliser TLS> est activé dans <Réglages de l'Intranet> dans <Réglages SIP>
- Le nom de la clé s'affiche pour <Clé et certificat> dans <Réglages TLS> dans <Réglages SIP>

Suivez la procédure ci-dessous pour vérifier les paramètres.

- **Utilisation du panneau de commande(P. 65)**
- **Utilisation de l'interface utilisateur distante(P. 66)**

Utilisation du panneau de commande

■ Vérification de <Utiliser TLS>

- 1 Appuyer sur  (Réglages/Enregistr.).**
- 2 Appuyez sur <Préférences> ► <Réseau> ► <Réglages TCP/IP> ► <Réglages SIP> ► <Réglages de l'Intranet>.**
- 3 Vérifiez <Utiliser TLS>.**

Exemple d'écran :



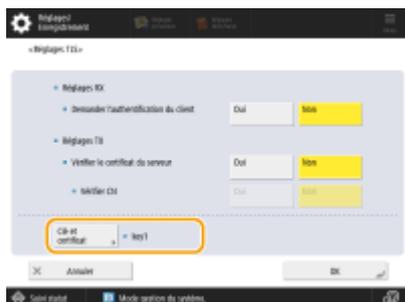
- Si <Utiliser TLS> est réglé sur <Oui>, passez à la vérification de <Clé et certificat>.
- Si <Utiliser TLS> est réglé sur <Non>, vous n'avez pas besoin d'effectuer les procédures suivantes.

■ Vérification de <Clé et certificat>

- 1 Appuyer sur  (Réglages/Enregistr.).**
- 2 Appuyez sur <Préférences> ► <Réseau> ► <Réglages TCP/IP> ► <Réglages SIP> ► <Réglages TLS>.**

3 Vérifiez si le nom de la clé s'affiche pour <Clé et certificat>.

Exemple d'écran :

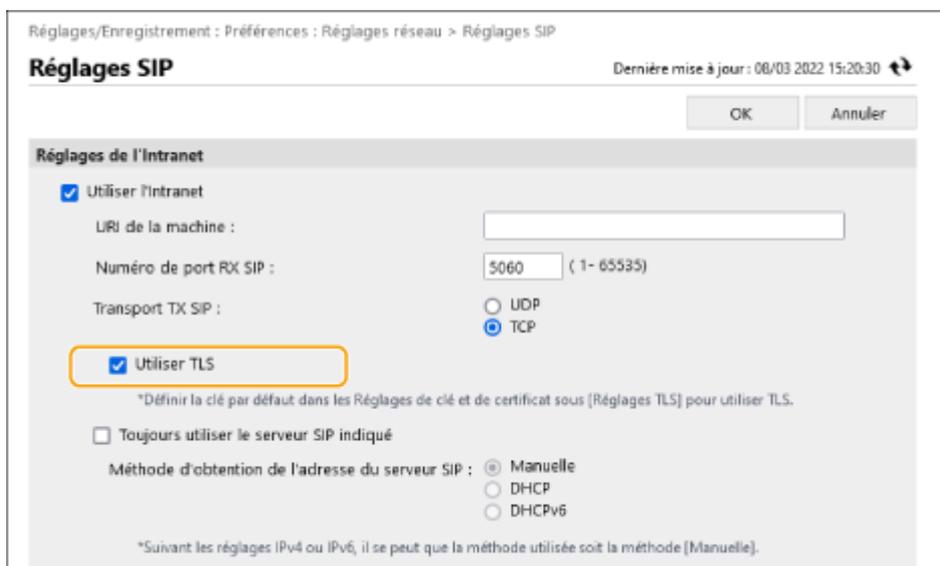


- Si un nom de clé s'affiche pour <Clé et certificat>, effectuez les procédures suivantes.
- Si le nom de la clé ne s'affiche pas pour <Clé et certificat>, vous n'avez pas besoin d'effectuer les procédures suivantes.

Utilisation de l'interface utilisateur distante

■ Vérification de [Utiliser TLS] et de [Clé et certificat]

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Réglages réseau] ► [Réglages SIP].
- 4 Vérifiez [Utiliser TLS] dans [Réglages de l'Intranet].



- Si [Utiliser TLS] est sélectionné, passez à la vérification de [Clé et certificat].
- Si [Utiliser TLS] est désélectionné, vous n'avez pas besoin d'effectuer les procédures suivantes.

5 Vérifiez [Nom de clé] dans [Réglages TLS].

réglages du support (1.36)

Transport TX T.38 :	UDPTL
Type de support T.38 :	image
Numéro de port RX T.38 :	49152 (1- 65535)
Numéro de port RX RTP :	5004 (1024- 65534)

Réglages TLS

Nom de clé	key1
------------	------

Clé et certificat...

Réglages RX

Demander l'authentification du client

Réglages TX

Vérifier le certificat du serveur

Ajouter CN à la liste des éléments à vérifier

Copyright CANON INC. 2020

- Si un nom de clé s'affiche, effectuez les procédures suivantes.
- Si le nom de la clé ne s'affiche pas, vous n'avez pas besoin d'effectuer les procédures suivantes.

Étape 2 : Régénération de la clé et du certificat (pour SIP)

Vous pouvez générer deux types de certificats pour une clé générée avec l'appareil : un certificat auto-signé et un certificat CSR. La procédure diffère selon le type de certificat.

Il se peut que vous ne puissiez pas effectuer les opérations à partir du panneau de contrôle, selon le modèle de votre appareil. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

► Pour un certificat auto-signé(P. 68)

► Pour un certificat CSR(P. 71)

Pour un certificat auto-signé

► Utilisation du panneau de commande(P. 68)

► Utilisation de l'interface utilisateur distante(P. 69)

■ Utilisation du panneau de commande

1 Appuyer sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Générer une clé> ► <Générer clé communication réseau>.

3 Configurez les paramètres requis et passez à l'écran suivant.

Exemple d'écran :



a <Nom de clé>

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b <Algorithme signature>

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512. Si vous sélectionnez <RSA> pour **c**, et que vous définissez <Longueur de la clé (bit)> à <1024> ou plus pour **d**, vous pouvez sélectionner les algorithmes de hachage SHA384 et SHA512.

c <Algorithme de clé>

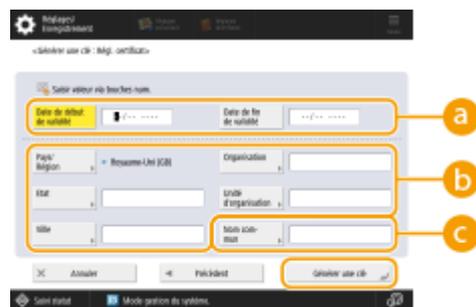
Sélectionnez l'algorithme de clé. Si vous sélectionnez <RSA>, <Longueur de la clé (bit)> s'affiche comme élément de réglage pour **d**. Si vous sélectionnez <ECDSA>, <Type de clé> s'affiche à la place.

d <Longueur de la clé (bit)>/<Type de clé>

Spécifiez la longueur de la clé si vous sélectionnez <RSA> pour **c**, ou spécifiez le type de clé si vous sélectionnez <ECDSA>. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement de la communication.

4 Configurez les éléments nécessaires pour le certificat ► appuyez sur <Générer une clé>.

Exemple d'écran :



a <Date de début de validité>/<Date de fin de validité>

Saisissez la date de début et les données de fin de la période de validité du certificat.

b <Pays/Région>/<Etat>/<Ville>/<Organisation>/<Unité org.>

Sélectionnez le code du pays dans la liste et saisissez l'emplacement et le nom de l'organisation.

c <Nom commun>

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

■ Utilisation de l'interface utilisateur distante

- 1** Lancez l'interface utilisateur distante.
- 2** Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3** Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4** Cliquez sur [Générer une clé].
- 5** Cliquez sur [Communication réseau].

6 Configurez les paramètres de la clé et du certificat.

a [Nom de clé]

Saisissez un nom pour la clé en utilisant des caractères alphanumériques. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature. Les algorithmes de hachage disponibles varient en fonction de la longueur de la clé. Une longueur de clé de 1024 bits ou plus peut prendre en charge les algorithmes de hachage SHA384 et SHA512.

c [Algorithme de clé]

Sélectionnez [RSA] ou [ECDSA] comme algorithme de génération de clé. Spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA]. Dans les deux cas, une valeur plus élevée offre une plus grande sécurité mais réduit la vitesse de traitement des communications.

REMARQUE :

- Si vous sélectionnez [SHA384] ou [SHA512] pour [Algorithme signature], vous ne pouvez pas définir la longueur de clé sur [512 bits] lorsque vous sélectionnez [RSA] pour [Algorithme de clé].

d [Date de début de validité (AAAA/MM/JJ)]/[Date de fin de validité (AAAA/MM/JJ)]

Saisissez la date de début et les données de fin de la période de validité du certificat. Vous ne pouvez pas définir [Date de fin de validité (AAAA/MM/JJ)] sur une date antérieure à celle de [Date de début de validité (AAAA/MM/JJ)].

e [Pays/Région]

Cliquez sur [Choisir un pays/une région] et sélectionnez le pays/la région dans la liste déroulante. Vous pouvez également cliquer sur [Saisir le code pays Internet] et saisir un code de pays, tel que « US » pour les États-Unis.

f [Etat]/[Ville]

Saisissez l'emplacement en utilisant les caractères alphanumériques nécessaires.

g [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation en utilisant les caractères alphanumériques nécessaires.

h [Nom commun]

Saisissez le nom commun du certificat en utilisant les caractères alphanumériques nécessaires. Le « nom commun » est souvent abrégé par « CN ».

7 Cliquez sur [OK].

- La génération d'une clé et d'un certificat peut prendre un certain temps.
- Les clés et les certificats générés sont automatiquement enregistrés sur l'appareil.

Pour un certificat CSR

Générez une clé et un CSR sur l'appareil. Utilisez les données CSR affichées à l'écran ou sorties dans un fichier pour demander à l'autorité de certification d'émettre un certificat. Ensuite, enregistrez le certificat émis pour la clé. Vous pouvez configurer ce paramètre uniquement à partir de l'interface utilisateur distante.

■ 1. Génération d'une clé et d'un CSR

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Cliquez sur [Générer une clé].
- 5 Cliquez sur [Clé et demande de signature de certificat (CSR)].
- 6 Configurez les paramètres de la clé et du certificat.

The screenshot shows the 'Générer clé et demande de signature de certificat (CSR)' interface. The interface is in French and shows various configuration options for generating a key and CSR. The options are grouped into sections: 'Générer clé et demande de signature de certificat (CSR)' and 'Réglages de demande de signature de certificat (CSR)'. The first section includes fields for 'Nom de clé', 'Algorithme signature', and 'Algorithme de clé'. The second section includes fields for 'Pays/Région', 'Etat', 'Ville', 'Organisation', 'Unité d'organisation', and 'Nom complet'. The interface also has a sidebar with navigation options and a top bar with user information and a 'Déconnexion' button.

a [Nom de clé]

Saisissez un nom pour la clé. Saisissez un nom qui sera facile à trouver dans une liste.

b [Algorithme signature]

Sélectionnez l'algorithme de hachage à utiliser pour la signature.

c [Algorithme de clé]

Sélectionnez l'algorithme de clé, et spécifiez la longueur de la clé si vous sélectionnez [RSA], ou spécifiez le type de clé si vous sélectionnez [ECDSA].

d [Pays/Région]

Sélectionnez le code du pays dans la liste ou bien saisissez-le directement.

e [Etat]/[Ville]

Saisissez le lieu.

f [Organisation]/[Unité d'organisation]

Saisissez le nom de l'organisation.

g [Nom commun]

Saisissez l'adresse IP ou le nom de domaine complet (FQDN).

- Pour l'impression IPPS dans un environnement Windows, n'oubliez pas de saisir l'adresse IP de l'appareil.
- Un serveur DNS est nécessaire pour entrer le FQDN de l'appareil. Entrez l'adresse IP de l'appareil si vous n'utilisez pas de serveur DNS.

7 Cliquez sur [OK].

▢ Les données CSR s'affichent.

- Si vous voulez sauvegarder les données CSR dans un fichier, cliquez sur [Memoriser dans un fichier] et spécifiez l'emplacement de sauvegarde.

REMARQUE :

- La clé qui a généré la CSR s'affiche sur l'écran de la liste des clés et des certificats, mais vous ne pouvez pas l'utiliser seule. Pour utiliser cette clé, vous devez enregistrer le certificat qui sera émis ultérieurement sur la base de la CSR.

8 Demandez à l'autorité de certification d'émettre un certificat basé sur les données CSR.

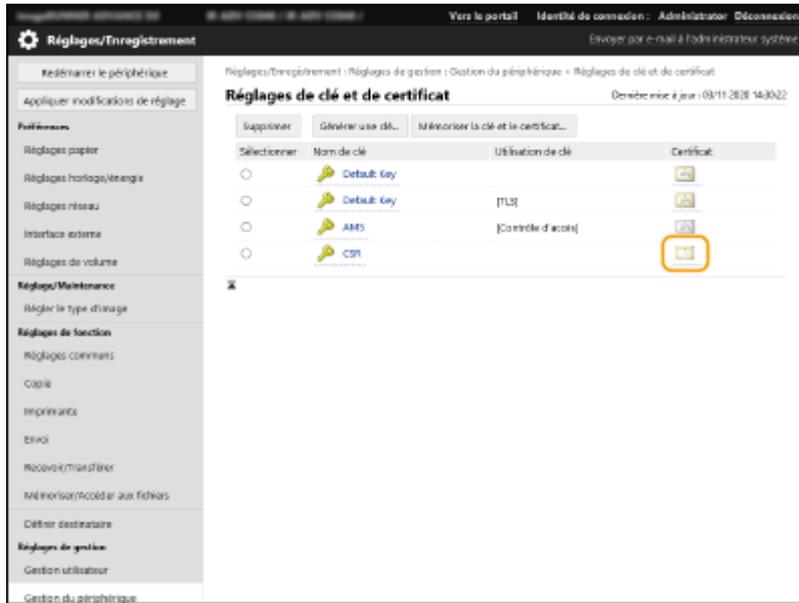
■ 2. Enregistrement du certificat délivré sur la clé

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].

4 Dans la liste [Certificat], cliquez sur  pour le certificat que vous voulez enregistrer.



5 Cliquez sur [Mémoriser certificat...].

6 Enregistrez le certificat.

- Cliquez sur [Parcourir...] ► spécifiez le fichier (certificat) à enregistrer ► cliquez sur [Mémoriser].

Étape 3 : Réinitialisation de la clé et du certificat (pour SIP)

Définissez la clé et le certificat générés comme la clé et le certificat à utiliser dans la communication cryptée TLS de SIP.

- ▶ Utilisation du panneau de commande (P. 74)
- ▶ Utilisation de l'interface utilisateur distante (P. 75)

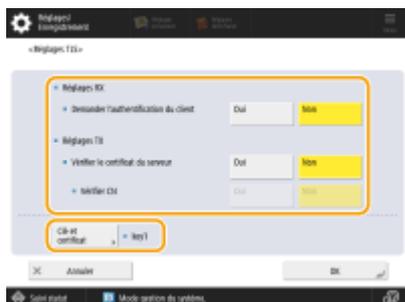
■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Préférences> ▶ <Réseau> ▶ <Réglages TCP/IP> ▶ <Réglages SIP> ▶ <Réglages TLS>.

3 Configurez les différents réglages dans <Réglages RX> et <Réglages TX> ▶ appuyez sur <Clé et certificat>.

Exemple d'écran :



<Réglages RX>	
<Demander l'authentification du client>	Sélectionnez <Oui> ou <Non>. Si vous sélectionnez <Oui>, l'appareil demande une authentification client lorsqu'il reçoit un fax IP.
<Réglages TX>	
<Vérifier le certificat du serveur>	Sélectionnez <Oui> ou <Non>. Si vous sélectionnez <Oui>, l'appareil vérifie si le certificat du serveur TLS est valide lorsque l'appareil reçoit un fax IP.
<Vérifier CN>	Sélectionnez <Oui> ou <Non>. Si vous sélectionnez <Oui>, l'appareil vérifie le CN (nom commun) lorsqu'il reçoit un fax IP.

4 Sélectionnez la clé et le certificat à utiliser pour la communication cryptée TLS de SIP ▶ appuyez sur <Définir en clé par déf.> ▶ <OK>.

Exemple d'écran :



REMARQUE

- Vous ne pouvez pas sélectionner la clé et le certificat si leur statut est « Utilisé ».
- Vous pouvez appuyer sur <Détails du certificat> pour vérifier les informations détaillées sur le certificat.
- Vous pouvez appuyer sur <Aff. emplac. d'utilisation> pour vérifier l'utilisation de la clé/certificat.

5 Appuyez sur <OK>.

6 Appuyez sur (Réglages/Enregistr.) ▶ (Réglages/Enregistr.) ▶ <Appliquer modifications réglages> ▶ <Oui>.

⇒ L'appareil redémarre, et les réglages sont appliqués.

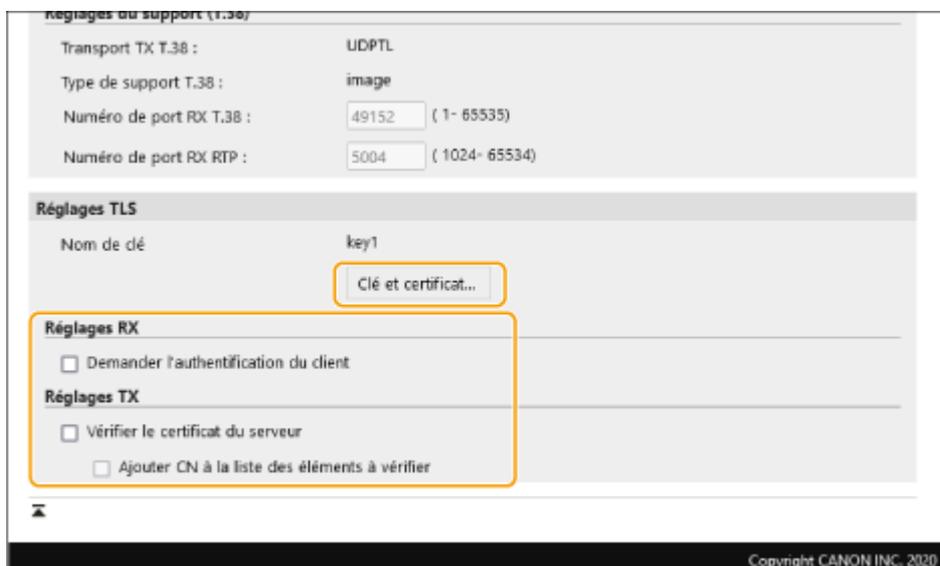
■ Utilisation de l'interface utilisateur distante

1 Lancez l'interface utilisateur distante.

2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.

3 Cliquez sur [Réglages réseau] ▶ [Réglages SIP].

4 Configurez les différents réglages dans [Réglages TLS] ▶ cliquez sur [Clé et certificat].



[Réglages RX]	
[Demander l'authentification du client]	Si vous cochez cette case, l'appareil demande une authentification client lorsqu'il reçoit un fax IP.
[Réglages TX]	
[Vérifier le certificat du serveur]	Si vous cochez cette case, l'appareil vérifie si le certificat du serveur TLS est valide lorsqu'il reçoit un fax IP.
[Ajouter CN à la liste des éléments à vérifier]	Sélectionnez [Oui] ou [Non]. Si vous cochez cette case, l'appareil vérifie le CN (nom commun) lorsqu'il reçoit un fax IP.

5 Cliquez sur [Utiliser] pour la clé à utiliser dans la liste.



6 Cliquez sur [OK].

7 Cliquez sur [Appliquer modifications de réglage] pour redémarrer l'appareil.

⇒ L'appareil redémarre, et les réglages sont appliqués.

Étape 4 : Suppression d'une clé/un certificat généré(e) dans le passé (pour SIP)

Selon le modèle de votre appareil, il se peut que vous ne puissiez pas effectuer d'opérations à partir du panneau de contrôle. Dans ce cas, effectuez les opérations à partir de l'interface utilisateur distante.

REMARQUE

- Vous devrez peut-être transmettre des informations à l'autorité de certification lors de la désactivation du certificat. Consultez **►Vérifier si vous devez effectuer les procédures supplémentaires(P. 5)** et notez les informations requises avant de supprimer la clé/le certificat.

►Utilisation du panneau de commande(P. 77)

►Utilisation de l'interface utilisateur distante(P. 78)

■ Utilisation du panneau de commande

1 Appuyez sur  (Réglages/Enregistr.).

2 Appuyez sur <Réglages de gestion> ► <Gestion du périphérique> ► <Réglages de certificat> ► <Liste de clés et de certificats> ► <Liste clés et certif. pour ce périphérique>.

- <Liste clés et certif. pour ce périphérique> ne s'affiche pas, sauf si la fonction de signature utilisateur est activée sur l'appareil. Dans ce cas, passez à l'étape suivante.

3 Sélectionnez la clé et le certificat ► appuyez sur <Supprimer> ► <Oui>.

Exemple d'écran :



REMARQUE :

- Si  s'affiche, la clé est corrompue ou non valide.
- Si  ne s'affiche pas, le certificat pour la clé n'existe pas.
- Si vous sélectionnez une clé et un certificat et appuyez sur <Détails du certificat>, des informations détaillées sur le certificat s'affichent. Vous pouvez également appuyer sur <Vérifier cert.> sur cet écran pour vérifier si le certificat est valide.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de clé et de certificat].
- 4 Sélectionnez la clé et le certificat ► cliquez sur [Supprimer] ► [OK].



REMARQUE

- Si s'affiche, la clé est corrompue ou non valide.
- Si s'affiche, le certificat pour la clé n'existe pas.
- Cliquez sur un nom de clé pour afficher des informations détaillées sur le certificat. Vous pouvez aussi appuyer sur [Vérifier le certificat] sur cet écran pour vérifier si le certificat est valide.

Étape 5 : Désactiver le certificat (pour SIP)

Désactivez un certificat généré dans le passé. La procédure diffère selon le type de certificat.

■ Pour un certificat auto-signé

Si un certificat comprenant une clé qui nécessite les procédures supplémentaires est enregistré sur un autre télécopieur IP en tant que certificat de confiance, supprimez le certificat enregistré. Après avoir supprimé le certificat enregistré, enregistrez le certificat de la clé régénérée.

■ Pour un certificat CSR

Demandez à l'autorité de certification qui a émis le certificat de le révoquer. Reportez-vous à [Créateur] dans le certificat pour connaître l'autorité de certification à demander.

REMARQUE

- Si vous vérifiez la révocation du certificat en utilisant l'autre télécopieur IP, enregistrez la CRL mise à jour sur l'ordinateur ou le navigateur web après la révocation du certificat.
- Si vous utilisez une méthode autre qu'une CRL (par exemple, OCSP) pour vérifier la révocation des certificats, effectuez la procédure correspondant à cette méthode.

Étape 6 : Activation du nouveau certificat (pour SIP)

Activez le certificat.

■ Pour un certificat auto-signé

Enregistrez le nouveau certificat auprès de l'autre télécopieur IP en tant que certificat de confiance.

■ Pour un certificat CSR

Vous n'avez pas besoin d'effectuer les procédures supplémentaires.

Procédure pour la signature des appareils

- ▶ **Étape 1 : Vérification des paramètres S/MIME (pour les signatures de l'appareil)(P. 82)**
- ▶ **Étape 2 : Régénération de la clé et du certificat (pour les signatures d'appareils)(P. 84)**
- ▶ **Étape 3 : Désactiver le certificat (pour les signatures d'appareils)(P. 85)**
- ▶ **Étape 4 : Activation du nouveau certificat (pour les signatures d'appareils)(P. 86)**

Étape 1 : Vérification des paramètres S/MIME (pour les signatures de l'appareil)

Vérifiez si vous devez effectuer les procédures supplémentaires pour S/MIME et les signatures de l'appareil.

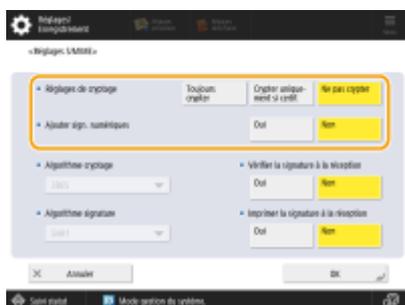
Suivez la procédure ci-dessous pour vérifier les paramètres S/MIME.

- Utilisation du panneau de commande (P. 82)
- Utilisation de l'interface utilisateur distante (P. 82)

■ Utilisation du panneau de commande

- 1 Appuyez sur  (Réglages/Enregistr.).
- 2 Appuyez sur <Réglages de fonction> ► <Envoi> ► <Réglages E-mail/I-Fax> ► <Réglages S/MIME>.
- 3 Vérifiez <Réglages de cryptage> et <Ajouter sign. numériques>.

Exemple d'écran :

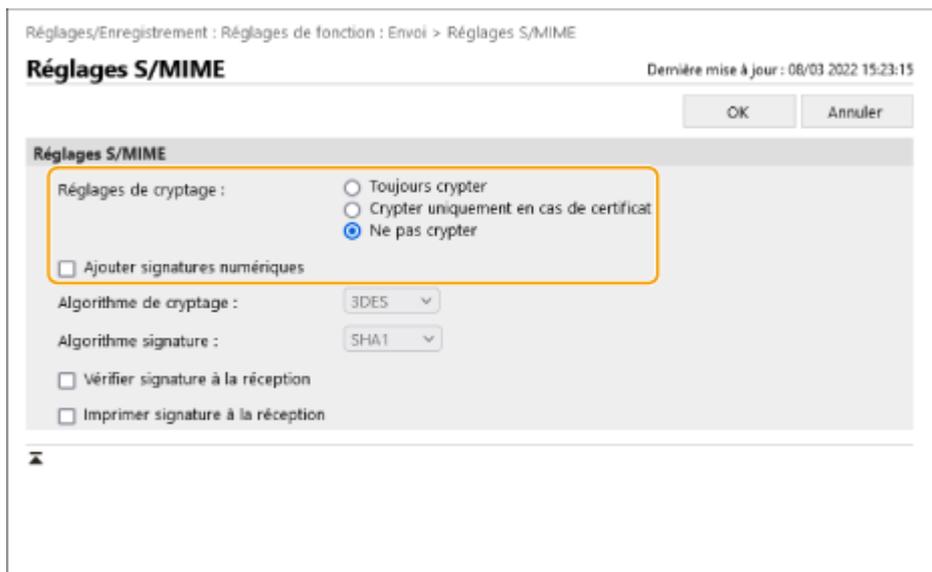


- Si <Réglages de cryptage> est réglé sur <Ne pas crypter> et que <Ajouter sign. numériques> est réglé sur <Non>, effectuez les procédures suivantes pour les signatures de l'appareil uniquement.
- Si d'autres réglages sont spécifiés, effectuez les procédures suivantes pour les signatures S/MIME et celles de l'appareil.

■ Utilisation de l'interface utilisateur distante

- 1 Lancez l'interface utilisateur distante.
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3 Cliquez sur [Envoi] ► [Réglages S/MIME].

4 Vérifiez [Réglages de cryptage] et [Ajouter signatures numériques].



- Si [Ne pas crypter] est sélectionné pour [Réglages de cryptage] et que [Ajouter signatures numériques] est désélectionné, effectuez les procédures suivantes pour les signatures de l'appareil uniquement.
- Si d'autres réglages sont spécifiés, effectuez les procédures suivantes pour les signatures S/MIME et celles de l'appareil.

Étape 2 : Régénération de la clé et du certificat (pour les signatures d'appareils)

- 🔍 Utilisation du panneau de commande (P. 84)
- 🔍 Utilisation de l'interface utilisateur distante (P. 84)

■ Utilisation du panneau de commande

- 1** Appuyer sur  (Réglages/Enregistr.).
- 2** Appuyez sur <Réglages de gestion> ▶ <Gestion du périphérique> ▶ <Réglages de certificat> ▶ <Générer une clé>.
- 3** Appuyez sur <Générer/Mettre à jour clé signature périph.> ▶ <Oui> ▶ <OK>.

■ Utilisation de l'interface utilisateur distante

- 1** Lancez l'interface utilisateur distante.
- 2** Cliquez sur [Réglages/Enregistrement] sur la page du portail.
- 3** Cliquez sur [Gestion du périphérique] ▶ [Réglages de clé et de certificat].
- 4** Cliquez sur [Générer une clé] ▶ [Signature de périphérique].
- 5** Cliquez sur [Générer/Mettre à jour] ▶ [OK].

Étape 3 : Désactiver le certificat (pour les signatures d'appareils)

Désactiver un certificat généré dans le passé.

■ Si un certificat pour les signatures d'appareils est enregistré dans Acrobat

Si un certificat pour les signatures d'appareils est enregistré dans Acrobat, supprimez le certificat enregistré.

■ Si un certificat S/MIME exporté de cet appareil a été importé sur un autre appareil

Si vous avez exporté le certificat de clé publique (certificat S/MIME) utilisé pour le cryptage des e-mails/télécopies via S/MIME à partir de cet appareil et importé le certificat sur un autre appareil, suivez la procédure ci-dessous pour supprimer le certificat de l'appareil où le certificat a été importé.

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Gestion du périphérique] ► [Réglages de certificat S/MIME].**
- 4 Sélectionnez le certificat correspondant ► cliquez sur [Supprimer] ► [OK].**

Étape 4 : Activation du nouveau certificat (pour les signatures d'appareils)

Activez le certificat.

■ Si un certificat pour les signatures d'appareils est enregistré dans Acrobat

Si un certificat pour les signatures d'appareils est enregistré dans Acrobat, exportez le certificat régénéré pour les signatures d'appareils et enregistrez le nouveau certificat dans Acrobat.

► Exportation du certificat de l'appareil(P. 86)

■ Si un certificat S/MIME exporté de cet appareil a été importé sur un autre appareil

Si vous avez exporté le certificat de clé publique (certificat S/MIME) utilisé pour le cryptage des e-mails/télécopies via S/MIME depuis cet appareil et importé le certificat sur un autre appareil, exportez le certificat régénéré et enregistrez-le sur l'autre appareil.

► Exportation du certificat de l'appareil(P. 86)

► Enregistrement du certificat sur l'autre appareil(P. 86)

■ Exportation du certificat de l'appareil

Effectuez la procédure suivante pour exporter le certificat.

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**
- 3 Cliquez sur [Gestion du périphérique] ► [Exporter signature de périphérique].**
- 4 Cliquez sur [Lancer l'exportation] ► pour enregistrer le fichier à l'endroit de votre choix.**

■ Enregistrement du certificat sur l'autre appareil

Effectuez la procédure suivante pour enregistrer le certificat sur l'autre appareil.

- 1 Lancez l'interface utilisateur distante.**
- 2 Cliquez sur [Réglages/Enregistrement] sur la page du portail.**

3 Cliquez sur [Gestion du périphérique] ► [Réglages de certificat S/MIME].

4 Cliquez sur [Mémoriser le certificat S/MIME].

5 Enregistrez le certificat S/MIME.

- Cliquez sur [Parcourir...] ► sélectionnez le fichier (certificat S/MIME) à enregistrer et cliquez sur ► cliquez sur [Mémoriser].

Procédures supplémentaires pour les réglages Bluetooth

Procédures supplémentaires pour les réglages Bluetooth	89
Procédure pour Bluetooth	90
Étape 1 : Suppression de l'appareil enregistré dans Canon PRINT Business (pour Bluetooth)	91
Étape 2 : Réenregistrer l'appareil sur Canon PRINT Business (pour Bluetooth)	92

Procédures supplémentaires pour les réglages Bluetooth

La clé pour Bluetooth est automatiquement mise à jour après la mise à jour du micrologiciel de l'appareil. Si vous utilisez l'application Canon PRINT Business pour les appareils mobiles, vous devez enregistrer à nouveau l'appareil.

▶ **Procédure pour Bluetooth(P. 90)**

Procédure pour Bluetooth

- **Étape 1 : Suppression de l'appareil enregistré dans Canon PRINT Business (pour Bluetooth)(P. 91)**
- **Étape 2 : Réenregistrer l'appareil sur Canon PRINT Business (pour Bluetooth)(P. 92)**

Étape 1 : Suppression de l'appareil enregistré dans Canon PRINT Business (pour Bluetooth)

Si le Bluetooth est réglé sur <Oui>, suivez la procédure ci-dessous.

▶ **Fonctionnement pour iOS(P. 91)**

▶ **Fonctionnement pour Android(P. 91)**

■ Fonctionnement pour iOS

1 Appuyez sur  en haut à gauche de l'écran d'accueil de Canon PRINT Business.

L'écran [Sél. une impr.] s'affiche.

2 Supprimez un appareil de la liste en appuyant sur  ► [Supprimer].

■ Fonctionnement pour Android

1 Appuyez sur  en haut à gauche de l'écran d'accueil de Canon PRINT Business.

L'écran [Sél. une impr.] s'affiche.

2 Appuyez et maintenez le nom de l'appareil ► appuyez sur [Supprimer] dans la boîte de dialogue affichée.

Étape 2 : Réenregistrer l'appareil sur Canon PRINT Business (pour Bluetooth)

Si le Bluetooth est réglé sur <Oui>, suivez la procédure ci-dessous.

► **Fonctionnement pour iOS**(P. 92)

► **Fonctionnement pour Android**(P. 92)

■ Fonctionnement pour iOS

1 Appuyez sur [] en haut à gauche de l'écran d'accueil de Canon PRINT Business.

L'écran [Sél. une impr.] s'affiche.

2 Onglet [Imprimantes à proximité].

Les appareils détectés s'affichent.

■ **Si les appareils ne sont pas détectés**

Rapprochez-vous de l'appareil, et tapez sur [Rechercher]. Le Bluetooth peut détecter des appareils à une distance allant jusqu'à 2 mètres ou 80 pouces.

3 Sélectionnez l'appareil ►, tapez sur [Ajouter].

■ Fonctionnement pour Android

1 Appuyez sur [] en haut à gauche de l'écran d'accueil de Canon PRINT Business.

L'écran [Sél. une impr.] s'affiche.

2 Onglet [Imprimantes à proximité].

Les appareils détectés s'affichent.

■ **Si les appareils ne sont pas détectés**

Rapprochez-vous de l'appareil, et tapez sur [Rechercher]. Le Bluetooth peut détecter des appareils à une distance allant jusqu'à 2 mètres ou 80 pouces.

3 Sélectionnez l'appareil.

4 Vérifiez les informations sur l'appareil dans la boîte de dialogue affichée ► tapez sur [Ajouter].

Si l'écran des paramètres du réseau Wi-Fi s'affiche, suivez les instructions à l'écran.

Procédures supplémentaires pour les paramètres du système de gestion des accès

Procédures supplémentaires pour les paramètres du système de gestion des accès ..

94

Procédure pour le système de gestion des accès 95

Procédures supplémentaires pour les paramètres du système de gestion des accès

La clé du système de gestion des accès est automatiquement mise à jour après la mise à jour du micrologiciel de l'appareil.

Les informations sur les restrictions sont automatiquement récupérées à nouveau environ 30 minutes après la mise à jour automatique de la clé. L'impression peut alors être effectuée normalement avec la fonction du système de gestion des accès.

Si vous souhaitez imprimer avec la fonction Système de gestion d'accès du pilote d'imprimante immédiatement après la mise à jour du micrologiciel, il est nécessaire de récupérer à nouveau manuellement les informations de restriction du Système de gestion d'accès.

► Procédure pour le système de gestion des accès(P. 95)

Une erreur se produit si vous essayez d'imprimer sans récupérer à nouveau les informations de restriction.

Procédure pour le système de gestion des accès

Si vous souhaitez imprimer avec la fonction Système de gestion d'accès du pilote d'imprimante immédiatement après la mise à jour du micrologiciel, vous devez récupérer manuellement les informations de restriction du Système de gestion d'accès.

Pour ce faire, suivez la procédure ci-dessous.

La procédure ci-dessous n'est pas nécessaire environ 30 minutes après la mise à jour du micrologiciel car les informations de restriction auront été automatiquement récupérées à ce moment-là.

1 Connectez-vous à l'ordinateur.

2 Affichez les propriétés de l'imprimante à utiliser avec le pilote d'imprimante dont la fonction de système de gestion des accès est activée.

■ Sous Windows Vista

- Cliquez sur [Démarrer] ► [Panneau de configuration] ► [Matériel et audio] ► sélectionnez [Imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés].

■ Sous Windows Server 2008

- Cliquez sur [Démarrer] ► [Panneau de configuration] ► [Matériel et audio] ► sélectionnez [Imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés].

■ Sous Windows Server 2008 R2

- Cliquez sur [Démarrer] ► [Panneau de configuration] ► [Matériel] ► sélectionnez [Périphériques et imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés de l'imprimante].

■ Sous Windows 7

- Cliquez sur [Démarrer] ► [Panneau de configuration] ► [Matériel et audio] ► sélectionnez [Périphériques et imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés de l'imprimante].

■ Sous Windows 8.1/Windows Server 2012

- Naviguez vers le bureau et affichez la barre symbole à droite de l'écran.
- Cliquez sur [Paramètres] ► [Panneau de configuration] ► sélectionnez [Afficher les périphériques et imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés de l'imprimante].

■ Sous Windows 10/Windows Server 2016

- Cliquez avec le bouton droit sur [Démarrer] ► sélectionnez [Panneau de configuration] ► [Afficher les périphériques et imprimantes].
- Cliquez avec le bouton droit sur l'icône de l'imprimante ► sélectionnez [Propriétés de l'imprimante].

3 Cliquer sur l'onglet [AMS].

4 Cliquez sur **[Obtenir des informations sur les restrictions]**.

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.