Informazioni sulle misure contro la vulnerabilità della generazione di chiavi RSA

USRM3-1248-02 2022-07 it

Sommario

Prefazione

Prefazione

Per aggiornare una chiave RSA creata con una libreria di crittografia vulnerabile, è necessario aggiornare il firmware ed eseguire le procedure aggiuntive descritte nel presente documento.

Per prima cosa, verificare il modello e la versione della macchina.
Se il modello e la versione della macchina sono presenti in questa pagina, aggiornare il firmware, quindi eseguire le procedure aggiuntive descritte nel presente documento. **Verifica della necessità delle procedure aggiuntive(P. 5)**
Per informazioni sull'aggiornamento del firmware, visitare il sito web da cui è stato ottenuto il presente documento.

Verifica della versione della macchina

Attenersi alla seguente procedura per verificare la versione della macchina.

1 Avviare la IU remota.

2 Fare clic su [Monitoraggio stato/Annulla] nella pagina del portale.

3 Fare clic su [Informazioni periferica] ▶ verificare [Controller] in [Informazioni versione].

Modelli e versioni che richiedono procedure aggiuntive

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

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

NOTA

- In base al modello della macchina in uso, le schermate utilizzate nel presente documento potrebbero essere diverse da quelle effettivamente visualizzate. Per ulteriori informazioni sulle schermate, consultare il manuale della propria macchina sul sito web dei manuali online.

  https://oip.manual.canon/

Verifica della necessità delle procedure aggiuntive

Verifica della necessità delle procedure aggiuntive

Eseguire le tre operazioni indicate di seguito per verificare le procedure aggiuntive da seguire.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire le operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Verifica della chiave RSA(P. 5)
Verifica delle impostazioni Bluetooth(P. 8)
Verifica delle impostazioni di Sistema di gestione degli accessi(P. 8)
La verifica di una chiave RSA non è necessaria se per una chiave registrata nella macchina compare "Chiave predefinita" o "AMS". Verificare le impostazioni di Bluetooth e Sistema di gestione degli accessi, quindi eseguire le eventuali procedure aggiuntive necessarie.

NOTA

- Le schermate utilizzate nel presente documento sono solo un esempio. In base al modello della macchina in uso, le schermate potrebbero essere diverse da quelle effettivamente visualizzate.

Verifica della chiave RSA

Verificare la presenza di una chiave RSA. In presenza di una chiave RSA generata con la macchina, verificare l'utilizzo della chiave.

Utilizzo del pannello comandi(P. 5)
Utilizzo della IU remota(P. 6)

■ Utilizzo del pannello comandi

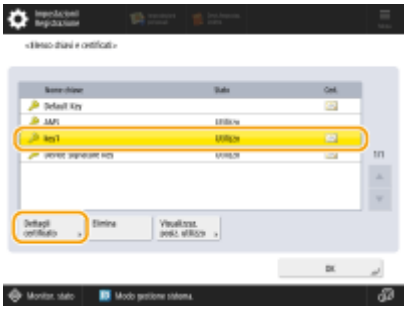
1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Elenco chiavi e certificati>.**

3 **Premere <Elenco chiavi e certificati per la periferica>.**

- <Elenco chiavi e certificati per la periferica> non viene visualizzato a meno che la funzione firma utente non sia abilitata sulla macchina. In questo caso, procedere al passaggio successivo.

4 **Selezionare una chiave diversa da <Default Key> e <AMS> con <Utilizzo> visualizzato per <Stato> ▶ premere <Dettagli certificato>.**
Schermata di esempio:



5 Verificare <Chiave pubblica>.

Schermata di esempio:

Per un certificato diverso da RSA

Le procedure aggiuntive non sono necessarie. Premere <OK> per chiudere la schermata.

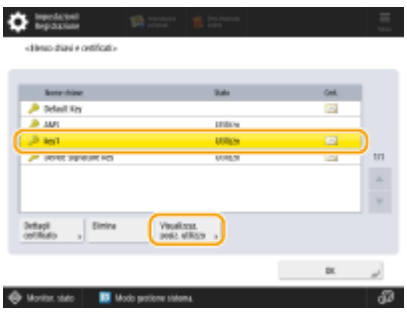
Per un certificato RSA

Passare alla Fase 6.

- Le procedure aggiuntive non sono necessarie per le seguenti chiavi. Premere <OK> per chiudere la schermata.
  - Una chiave RSA generata esternamente e registrata sulla macchina
- Nel caso in cui siano necessario le procedure aggiuntive, potrebbero servire le informazioni sul certificato per disabilitare il certificato. Annotare le informazioni necessarie prima di eliminare la chiave/certificato. Richiedere le informazioni necessarie all'autorità di certificazione.

6 Premere <Visualizzaz. posiz. utilizzo> ▶ verificare l'utilizzo della chiave.

Schermata di esempio:

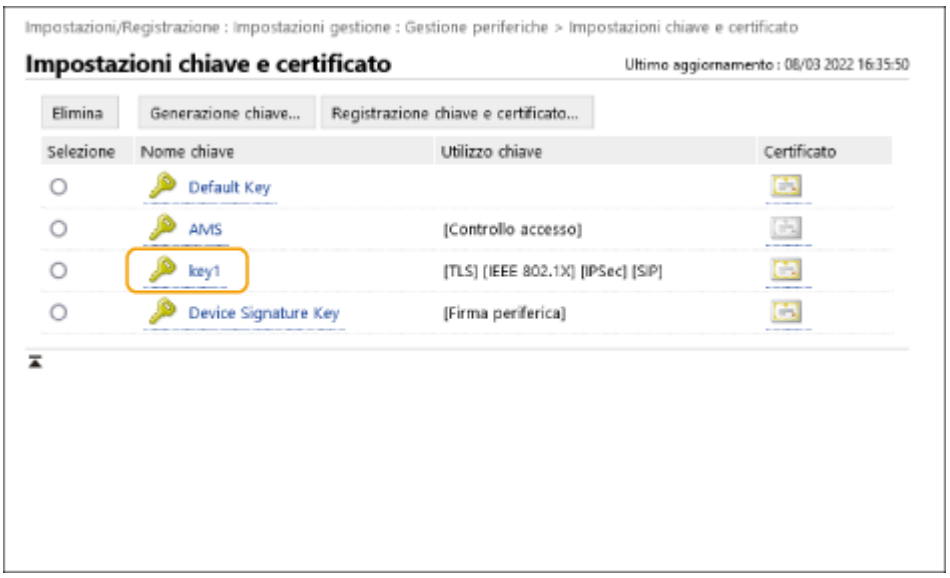


Eseguire le procedure aggiuntive in base a quanto visualizzato qui. **Utilizzo della chiave RSA e procedura aggiuntiva(P. 12)**

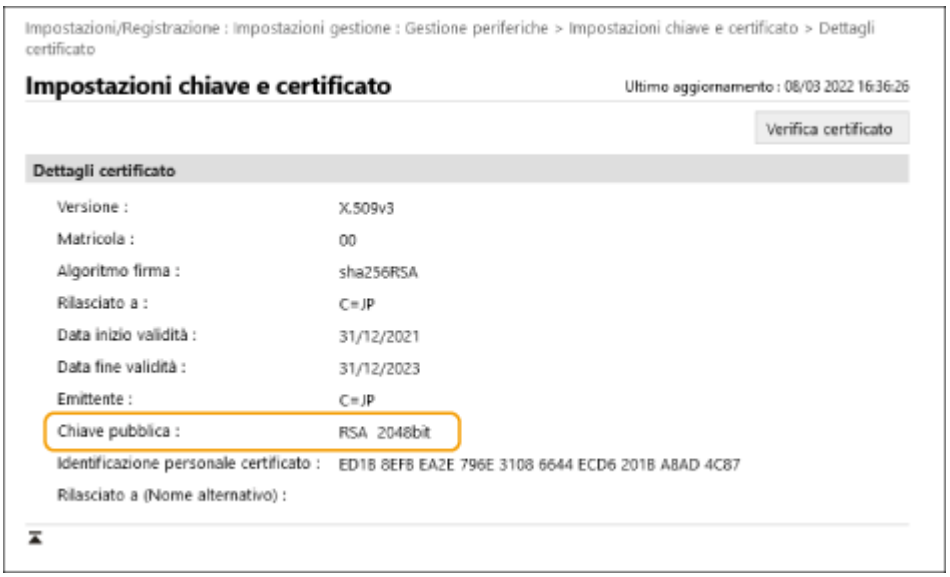
■Utilizzo della IU remota

1 Avviare la IU remota ▶ fare clic su [Impostazioni/Registrazione] ▶ [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

2 Fare clic su una chiave diversa da [Default Key] e [AMS].



3 Controllare [Chiave pubblica].



Per un certificato diverso da RSA

Le procedure aggiuntive non sono necessarie.

Per un certificato RSA

Fare clic su [Impostazioni chiave e certificato] nella parte superiore della schermata ▶ verificare l'utilizzo della chiave.

- Eseguire le procedure aggiuntive in base a quanto visualizzato qui. **Utilizzo della chiave RSA e procedura aggiuntiva(P. 12)**
- Le procedure aggiuntive non sono necessarie per le seguenti chiavi.
  - Una chiave RSA generata esternamente e registrata sulla macchina
- Nel caso in cui siano necessario le procedure aggiuntive, potrebbero servire le informazioni sul certificato per disabilitare il certificato. Annotare le informazioni necessarie prima di eliminare la chiave/certificato. Richiedere le informazioni necessarie all'autorità di certificazione.

Verifica delle impostazioni Bluetooth

Verificare se il Bluetooth è impostato su <On>. Se è impostato su <On>, le procedure aggiuntive sono necessarie.

Utilizzo del pannello comandi(P. 8)
Utilizzo della IU remota(P. 8)

■ Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni Bluetooth>.

3 Verificare <Utilizzo Bluetooth>.

- Se <Utilizzo Bluetooth> è impostato su <On>, eseguire le procedure successive. **Procedure aggiuntive per le impostazioni Bluetooth(P. 89)**
- Se <Utilizzo Bluetooth> è impostato su <Off>, le procedure successive non sono necessarie.

■ Utilizzo della IU remota

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Rete] ▶ [Impostazioni Bluetooth].

4 Controllare [Utilizzo Bluetooth].

- Se [Utilizzo Bluetooth] è selezionato, eseguire le procedure successive. **Procedure aggiuntive per le impostazioni Bluetooth(P. 89)**
- Se [Utilizzo Bluetooth] è deselezionato, le procedure successive non sono necessarie.

Verifica delle impostazioni di Sistema di gestione degli accessi

Verificare se Sistema di gestione degli accessi è impostato su <On>. Se è impostato su <On>, le procedure aggiuntive non sono necessarie.

In base alla macchina in uso, questa impostazione potrebbe non essere visualizzata. In tal caso, le procedure aggiuntive non sono necessarie.

Utilizzo del pannello comandi(P. 9)
Utilizzo della IU remota(P. 9)

■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Impostazioni gestione> ▶ <Licenza/Altro> ▶ <Utilizzo ACCESS MANAGEMENT SYSTEM>.

3 Verificare <Utilizzo ACCESS MANAGEMENT SYSTEM>.

- Se <Utilizzo ACCESS MANAGEMENT SYSTEM> è impostato su <On>, eseguire le procedure successive. **Procedure aggiuntive per le impostazioni di Sistema di gestione degli accessi(P. 94)**
- Se <Utilizzo ACCESS MANAGEMENT SYSTEM> è impostato su <Off>, le procedure successive non sono necessarie.

■Utilizzo della IU remota

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Licenza/Altro] ▶ [Impostazioni ACCESS MANAGEMENT SYSTEM].

4 Controllare [Utilizzo ACCESS MANAGEMENT SYSTEM].

- Se [Utilizzo ACCESS MANAGEMENT SYSTEM] è selezionato, eseguire le procedure successive. **Procedure aggiuntive per le impostazioni di Sistema di gestione degli accessi(P. 94)**
- Se [Utilizzo ACCESS MANAGEMENT SYSTEM] è deselezionato, le procedure successive non sono necessarie.

Utilizzo della chiave RSA e procedura aggiuntiva

Utilizzo della chiave RSA e procedura aggiuntiva

Consultare "Procedure aggiuntive" ed eseguirle in base all'utilizzo della chiave.

Utilizzo della chiave RSA	Condizioni	Procedure aggiuntive
TLS	Le procedure aggiuntive sono necessarie in qualsiasi condizione.	**Procedura per TLS(P. 13)**
IEEE 802.1X	Le procedure aggiuntive sono necessarie se il metodo di autenticazione IEEE 802.1X è impostato su EAP-TLS.	**Procedura per IEEE 802.1X(P. 28)**
IPSec	Le procedure aggiuntive sono necessarie se il metodo di autenticazione IKE è impostato sul metodo di firma digitale.	**Procedura per IPSec(P. 46)**
SIP	Le procedure aggiuntive sono necessarie se si utilizza TLS.	**Procedura per SIP(P. 64)**
Firma dispositivo	Le procedure aggiuntive sono necessarie nei seguenti casi: • Quando viene aggiunta una firma digitale ai file inviati utilizzando una chiave per firma periferica • Quando la crittografia è abilitata nelle impostazioni di crittografia S/MIME	**Procedura per firma periferica(P. 81)**

NOTA

- Le schermate utilizzate nel presente documento sono solo un esempio. In base al modello della macchina in uso, le schermate potrebbero essere diverse da quelle effettivamente visualizzate.

Procedura per TLS

Passaggio 1: Rigenerazione di chiave e certificato (per TLS)

È possibile generare tre tipi di certificati per una chiave generata con la macchina: un certificato autofirmato, un certificato CSR e un certificato SCEP. La procedura varia a seconda del tipo di certificato.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Per un certificato autofirmato(P. 14)
Per un certificato CSR(P. 17)
Per un certificato SCEP(P. 19)

Per un certificato autofirmato

Utilizzo del pannello comandi(P. 14)
Utilizzo della IU remota(P. 15)

■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Generazione chiave> ▶ <Generazione chiave comunicazione rete>.

3 Configurare le impostazioni necessarie e procedere alla schermata successiva.

Schermata di esempio:

a <Nome chiave>

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b <Algoritmo firma>

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512. Se si seleziona <RSA> per c e si imposta <Lunghezza chiave (bit)> su <1024> o più per d, è possibile selezionare gli algoritmi hash SHA384 e SHA512.

c <Algoritmo chiave>

Selezionare l'algoritmo della chiave. Se si seleziona <RSA>, <Lunghezza chiave (bit)> compare come voce di impostazione per d. Se si seleziona <ECDSA>, compare invece <Tipo di chiave>.

d <Lunghezza chiave (bit)>/<Tipo di chiave>

Specificare la lunghezza della chiave se si seleziona <RSA> per c oppure specificare il tipo di chiave se si seleziona <ECDSA>. In entrambi i casi, un valore maggiore garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

4 Configurare le voci necessarie per il certificato ▶ premere <Generazione chiave>.

Schermata di esempio:

a <Data inizio validità>/<Data fine validità>

Inserire la data di inizio e la data di fine del periodo di validità del certificato.

b <Paese/Regione>/<Stato>/<Città>/<Organizzazione>/<Unità organizzativa>

Selezionare il codice paese dall'elenco e inserire il nome del luogo e dell'organizzazione.

c <Nome comune>

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

■ Utilizzo della IU remota

1 Avviare la IU remota.

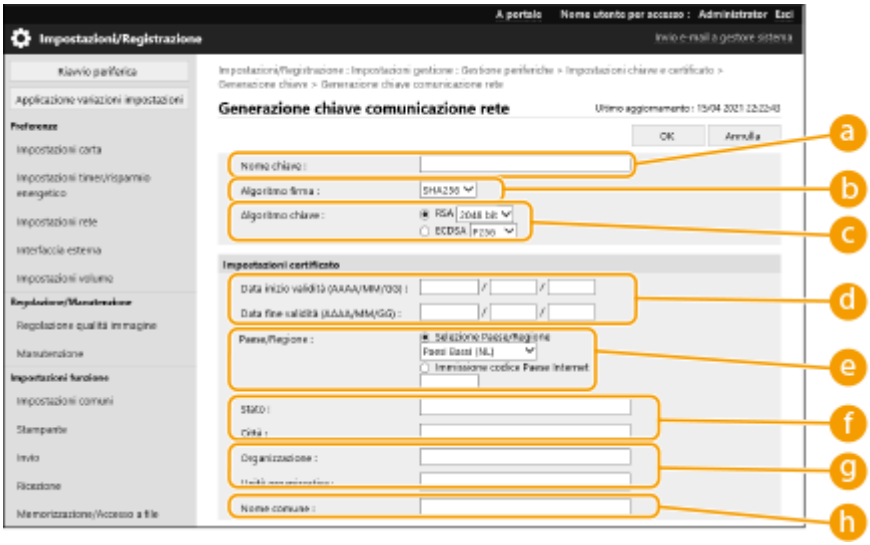
2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Fare clic su [Generazione chiave].

5 Fare clic su [Comunicazione rete].

6 Configurare le impostazioni di chiave e certificato.



a [Nome chiave]

Immettere un nome per la chiave utilizzando caratteri alfanumerici. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512.

c [Algoritmo chiave]

Selezionare [RSA] o [ECDSA] come algoritmo di generazione chiave. Specificare la lunghezza della chiave se si seleziona [RSA] o il tipo di chiave se si seleziona [ECDSA]. In entrambi i casi, un valore più alto garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

NOTA:

- Se si seleziona [SHA384] o [SHA512] per [Algoritmo firma], non è possibile impostare la lunghezza della chiave su [512 bit] quando si seleziona [RSA] per [Algoritmo chiave].

d [Data inizio validità (AAAA/MM/GG)]/[Data fine validità (AAAA/MM/GG)]

Immettere la data di inizio e la data di fine del periodo di validità del certificato. Il valore [Data fine validità (AAAA/MM/GG)] non può essere impostato su una data precedente alla data in [Data inizio validità (AAAA/MM/GG)].

e [Paese/Regione]

Fare clic su [Selezione Paese/Regione] e selezionare il paese/regione dall'elenco a discesa. In alternativa, fare clic su [Immissione codice Paese Internet] e inserire un codice paese, per esempio "US" per gli Stati Uniti.

f [Stato]/[Città]

Inserire il luogo utilizzando caratteri alfanumerici secondo necessità.

g [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione utilizzando caratteri alfanumerici secondo necessità.

h [Nome comune]

Inserire il nome comune del certificato utilizzando caratteri alfanumerici secondo necessità. "Nome comune" viene spesso abbreviato con "CN".

7 Fare clic su [OK].

- La generazione di una chiave e un certificato potrebbe richiedere del tempo.
- Le chiavi e i certificati generati vengono registrati automaticamente nella macchina.

Per un certificato CSR

Generare una chiave e una richiesta CSR sulla macchina. Utilizzare i dati della richiesta CSR visualizzati sullo schermo o esportarli in un file per richiedere l'emissione di un certificato all'autorità di certificazione. In seguito, registrare il certificato emesso per la chiave.
Questa impostazione può essere configurata solo dalla IU remota.

■1. Generazione di chiave e CSR

1 **Avviare la IU remota.**

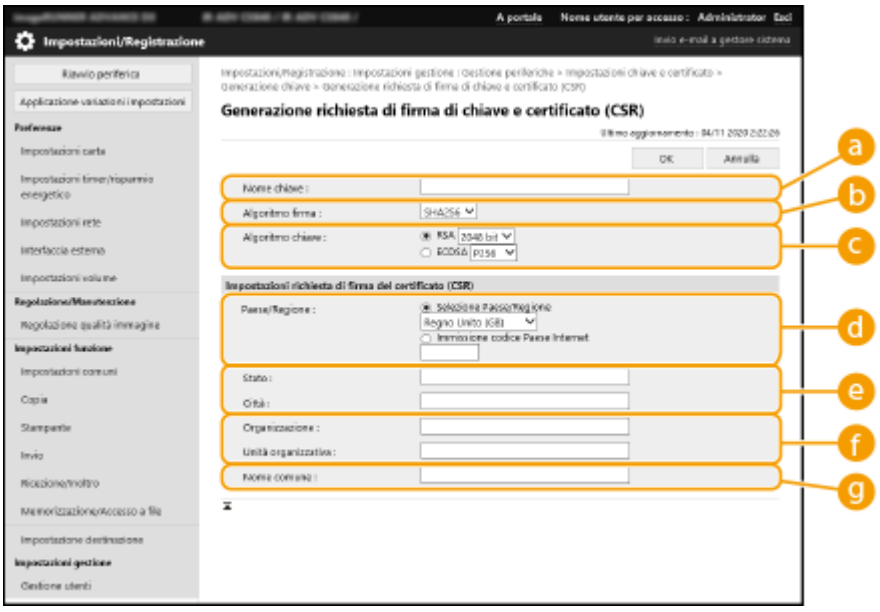
2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Fare clic su [Generazione chiave].**

5 **Fare clic su [Richiesta di firma di chiave e certificato (CSR)].**

6 **Configurare le impostazioni di chiave e certificato.**



a [Nome chiave]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Algoritmo chiave]

Selezionare l'algoritmo chiave e specificare la lunghezza della chiave se si seleziona [RSA], oppure specificare il tipo di chiave se si seleziona [ECDSA].

d [Paese/Regione]

Selezionare il codice paese dall'elenco oppure inserirlo direttamente.

e [Stato]/[Città]

Inserire il luogo.

f [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione.

g [Nome comune]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

7 Fare clic su [OK].

➠ Compaiono i dati della richiesta CSR.

- Se si desidera salvare i dati della richiesta CSR in un file, fare clic su [Memorizzazione in file] e specificare la posizione di salvataggio.

NOTA:

- La chiave che ha generato la richiesta CSR viene visualizzata nella schermata di elenco di chiave e certificato, ma non è possibile utilizzarla autonomamente. Per utilizzare questa chiave è necessario registrare il certificato che viene rilasciato successivamente in base alla richiesta CSR.

8 Richiedere l'emissione di un certificato in base ai dati della richiesta CSR all'autorità di certificazione.

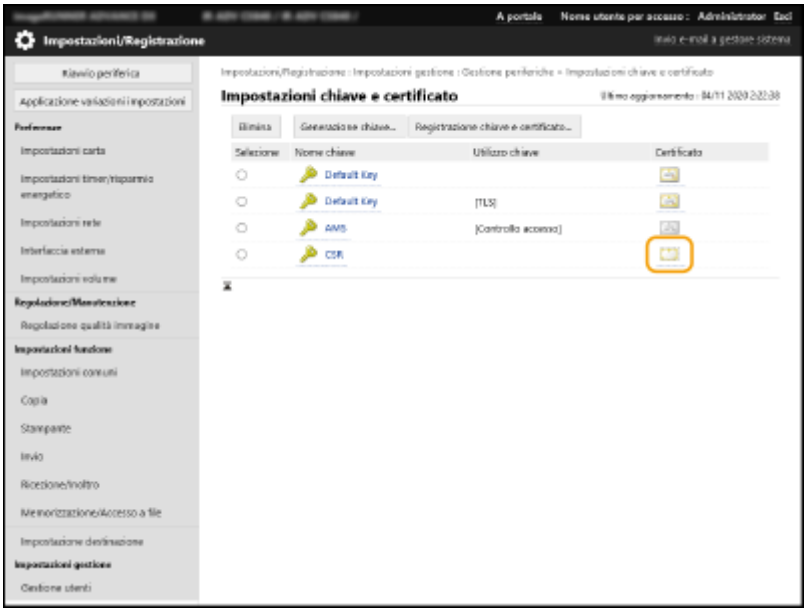
■2. Registrazione del certificato emesso con la chiave

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Nell'elenco [Certificato], fare clic su per il certificato che si desidera registrare.



5 **Fare clic su [Registrazione certificato...].**

6 **Registrare il certificato.**

- Fare clic su [Sfoglia...] ▶ specificare il file (certificato) da registrare ▶ fare clic su [Registra].

Per un certificato SCEP

Richiedere manualmente l'emissione di un certificato al server SCEP.
Questa impostazione può essere configurata solo dalla IU remota.

NOTA

- Se si seleziona [Abilitazione timer per richiesta automatica emissione certificato], non è possibile inviare una richiesta manuale per l'emissione di un certificato. Se questa opzione è selezionata, deselezionarla.

Avviare la IU remota ▶ fare clic su [Impostazioni/Registrazione] ▶ [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)] ▶ [Impostazioni per richiesta automatica emissione certificato] ▶ deselezionare [Abilitazione timer per richiesta automatica emissione certificato] ▶ fare clic su [Aggiornamento].

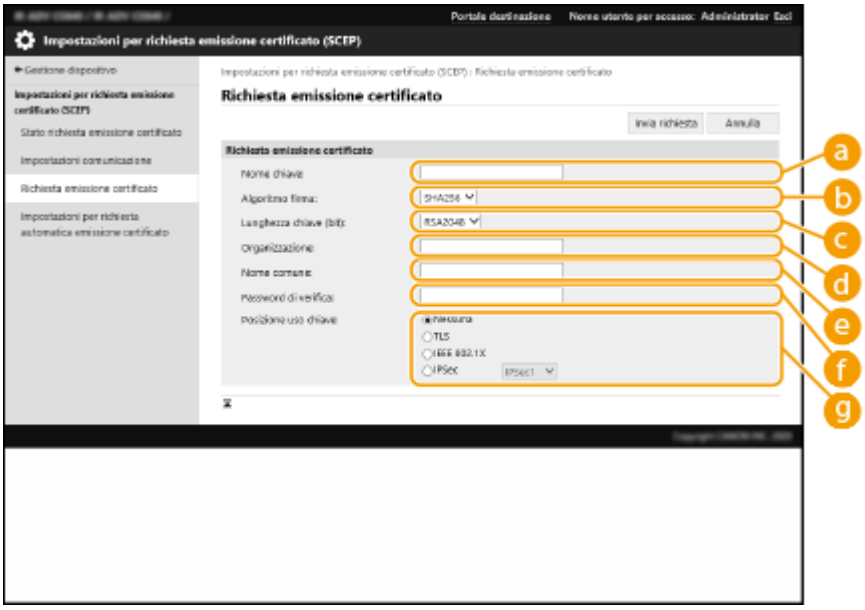
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)].**

4 **Fare clic su [Richiesta emissione certificato].**

5 Configurare le impostazioni necessarie per la richiesta di un certificato.



a [Nome chiave:]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma:]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Lunghezza chiave (bit):]

Selezionare la lunghezza della chiave.

d [Organizzazione:]

Inserire il nome dell'organizzazione.

e [Nome comune:]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

f [Password di verifica:]

Se è impostata una password sul lato del server SCEP, immettere la password di verifica inclusa nei dati della richiesta (PKCS#9) per richiedere l'emissione di un certificato.

g [Posizione uso chiave:]

Selezionare [TLS].

NOTA:

- Quando si seleziona un'opzione diversa da [Nessuna], abilitare ogni funzione in anticipo. Se si ottiene un certificato con tutte le funzioni disabilitate, il certificato viene assegnato alla posizione di utilizzo della chiave, ma le singole funzioni non vengono abilitate automaticamente.

6 Fare clic su [Invia richiesta].

7 **Fare clic su [Riavvio].**

Passaggio 2: Ripristino di chiave e certificato (per TLS)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.
Questa procedura non è necessaria per un certificato SCEP.

Per un certificato autofirmato/certificato CSR

Utilizzo del pannello comandi(P. 22)
Utilizzo della IU remota(P. 23)

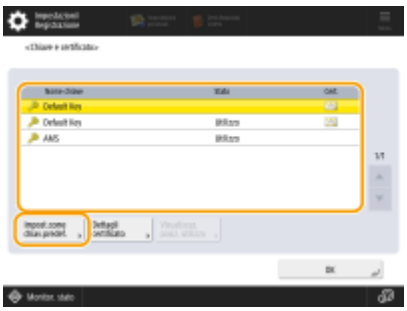
■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni TLS>.**

3 **Premere <Chiave e certificato>.**

4 **Selezionare la chiave e il certificato da utilizzare per la comunicazione crittografata TLS ▶ premere <Impost.come chiav.predef.> ▶ <Sì>.**
Schermata di esempio:



- Se si desidera utilizzare il codice e il certificato preinstallati, selezionare <Default Key>.

NOTA:

- La comunicazione crittografata TLS non può utilizzare <Device Signature Key>, che viene utilizzato per la firma periferica, né <AMS>, che viene utilizzato per le limitazioni di accesso.

5 **Premere <OK>.**

6 **Premere (Impostazioni/Registrazione) ▶ <Applicazione variazioni impostazioni> ▶ <Sì>.**

➠ La macchina si riavvia e le impostazioni vengono applicate.

■Utilizzo della IU remota

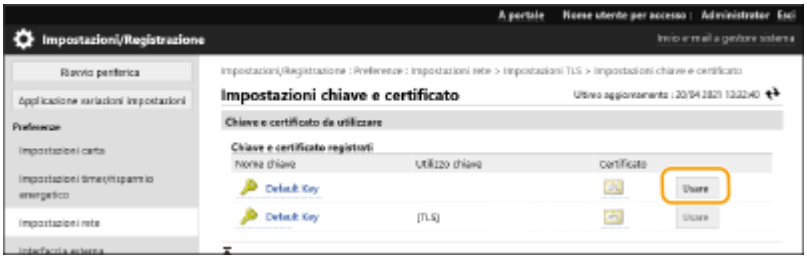
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Rete] ▶ [Impostazioni TLS].**

4 **Fare clic su [Chiave e certificato].**

5 **Fare clic su [Usare] per la chiave e il certificato da utilizzare per la comunicazione crittografata TLS.**



- Se si desidera utilizzare la chiave e il certificato preinstallati, selezionare [Default Key].

6 **Fare clic su [Applic.variaz.impost.] per riavviare la macchina.**

➠ La macchina si riavvia e le impostazioni vengono applicate.

Passaggio 3: Eliminazione di chiave/certificato generati in precedenza (per TLS)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

NOTA

- Potrebbe essere necessario fornire informazioni all'autorità di certificazione quando si disabilita il certificato. Consultare **Verifica della necessità delle procedure aggiuntive(P. 5)** e annotare le informazioni necessarie prima di eliminare chiave/certificato.

Utilizzo del pannello comandi(P. 24)
Utilizzo della IU remota(P. 25)

■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Elenco chiavi e certificati> ▶ <Elenco chiavi e certificati per la periferica>.**

- <Elenco chiavi e certificati per la periferica> non viene visualizzato a meno che la funzione firma utente non sia abilitata sulla macchina. In questo caso, procedere al passaggio successivo.

3 **Selezionare la chiave e il certificato ▶ premere <Elimina> ▶ <Sì>.**

Schermata di esempio:

NOTA:

- Se compare , la chiave è corrotta o non valida.
- Se non compare , il certificato per la chiave non esiste.
- Se si seleziona una chiave e un certificato e si preme <Dettagli certificato>, saranno visualizzate le informazioni dettagliate sul certificato. Inoltre, per verificare che il certificato sia valido, è possibile premere <Verif. certif.> in questa schermata.

■Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Selezionare la chiave e il certificato ▶ fare clic su [Elimina] ▶ [OK].**

NOTA

- Se compare , la chiave è corrotta o non valida.
- Se compare , il certificato per la chiave non esiste.
- Fare clic su un nome di codice per visualizzare le informazioni dettagliate sul certificato. È anche possibile fare clic su [Verifica certificato] in questa schermata per controllare se il certificato è valido.

Passaggio 4: Disabilitazione del certificato (per TLS)

Disabilitare un certificato generato in precedenza. La procedura varia in base al tipo di certificato.

■ Per un certificato autofirmato

Se un certificato includente una chiave che richiede le procedure aggiuntive viene registrato in un computer o in un browser web come certificato attendibile, eliminare il certificato registrato.

■ Per un certificato CSR/SCEP

Richiedere all'autorità di certificazione che ha emesso il certificato di revocare il certificato. Fare riferimento alla voce [Emittente] nel certificato per sapere a quale autorità di certificazione presentare la richiesta.

NOTA

- In caso di verifica della revoca del certificato con un CRL in un computer o browser web che comunica con la macchina, registrare il CRL aggiornato sul computer o browser web dopo che il certificato è stato revocato.
- Se si utilizza un metodo diverso da CRL (per esempio, OCSP) per verificare la revoca del certificato, attenersi alla procedura relativa a quel metodo.

Passaggio 5: Abilitazione del nuovo certificato (per TLS)

Abilitare il nuovo certificato generato sulla macchina.

■ Per un certificato autofirmato

Registrare il nuovo certificato sul computer o browser web come certificato attendibile.

■ Per un certificato CSR/SCEP

Le procedure aggiuntive non sono necessarie.

Procedura per IEEE 802.1X

Passaggio 1: Verifica del metodo di autenticazione (per IEEE 802.1X)

Se il metodo di autenticazione IEEE 802.1X è impostato su EAP-TLS, le procedure successive sono necessarie.
Attenersi alla seguente procedura per verificare il metodo di autenticazione.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Utilizzo del pannello comandi(P. 29)
Utilizzo della IU remota(P. 29)

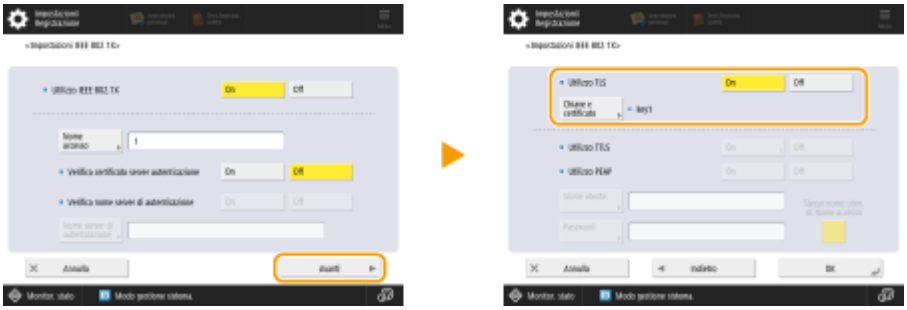
Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni IEEE 802.1X>.

3 Premere <Avanti> ▶ verificare <Utilizzo TLS>.

Schermata di esempio:



- Se <Utilizzo TLS> è impostato su <On> e viene visualizzato un nome chiave per <Chiave e certificato>, eseguire le procedure successive.
- Se <Utilizzo TLS> è impostato su <Off>, le procedure successive non sono necessarie.

Utilizzo della IU remota

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Rete] ▶ [Impostazioni IEEE 802.1X].

4 Controllare [Utilizzo TLS].

- Se [Utilizzo TLS] è selezionato e viene visualizzato un nome chiave, eseguire le procedure successive.
- Se [Utilizzo TLS] è deselezionato, le procedure successive non sono necessarie.

Passaggio 2: Rigenerazione di chiave e certificato (per IEEE 802.1X)

È possibile generare tre tipi di certificati per una chiave generata con la macchina: un certificato autofirmato, un certificato CSR e un certificato SCEP. La procedura varia a seconda del tipo di certificato.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Per un certificato autofirmato(P. 31)
Per un certificato CSR(P. 34)
Per un certificato SCEP(P. 36)

Per un certificato autofirmato

Utilizzo del pannello comandi(P. 31)
Utilizzo della IU remota(P. 32)

■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Generazione chiave> ▶ <Generazione chiave comunicazione rete>.**

3 **Configurare le impostazioni necessarie e procedere alla schermata successiva.**

Schermata di esempio:

a <Nome chiave>

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b <Algoritmo firma>

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512. Se si seleziona <RSA> per c e si imposta <Lunghezza chiave (bit)> su <1024> o più per d, è possibile selezionare gli algoritmi hash SHA384 e SHA512.

c <Algoritmo chiave>

Selezionare l'algoritmo della chiave. Se si seleziona <RSA>, <Lunghezza chiave (bit)> compare come voce di impostazione per d. Se si seleziona <ECDSA>, compare invece <Tipo di chiave>.

d <Lunghezza chiave (bit)>/<Tipo di chiave>

Specificare la lunghezza della chiave se si seleziona <RSA> per c oppure specificare il tipo di chiave se si seleziona <ECDSA>. In entrambi i casi, un valore maggiore garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

4 Configurare le voci necessarie per il certificato ▶ premere <Generazione chiave>.

Schermata di esempio:

a <Data inizio validità>/<Data fine validità>

Inserire la data di inizio e la data di fine del periodo di validità del certificato.

b <Paese/Regione>/<Stato>/<Città>/<Organizzazione>/<Unità organizzativa>

Selezionare il codice paese dall'elenco e inserire il nome del luogo e dell'organizzazione.

c <Nome comune>

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

■ Utilizzo della IU remota

1 Avviare la IU remota.

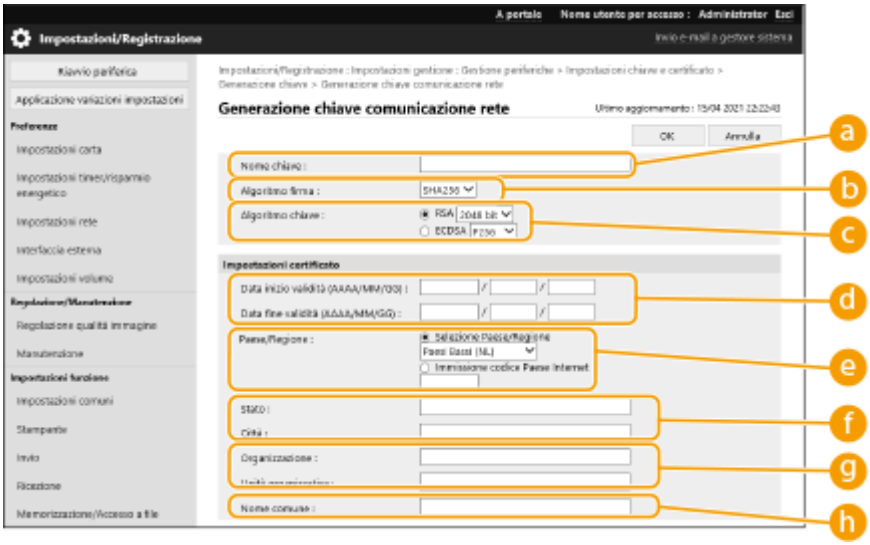
2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Fare clic su [Generazione chiave].

5 Fare clic su [Comunicazione rete].

6 Configurare le impostazioni di chiave e certificato.



a [Nome chiave]

Immettere un nome per la chiave utilizzando caratteri alfanumerici. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512.

c [Algoritmo chiave]

Selezionare [RSA] o [ECDSA] come algoritmo di generazione chiave. Specificare la lunghezza della chiave se si seleziona [RSA] o il tipo di chiave se si seleziona [ECDSA]. In entrambi i casi, un valore più alto garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

NOTA:

- Se si seleziona [SHA384] o [SHA512] per [Algoritmo firma], non è possibile impostare la lunghezza della chiave su [512 bit] quando si seleziona [RSA] per [Algoritmo chiave].

d [Data inizio validità (AAAA/MM/GG)]/[Data fine validità (AAAA/MM/GG)]

Immettere la data di inizio e la data di fine del periodo di validità del certificato. Il valore [Data fine validità (AAAA/MM/GG)] non può essere impostato su una data precedente alla data in [Data inizio validità (AAAA/MM/GG)].

e [Paese/Regione]

Fare clic su [Selezione Paese/Regione] e selezionare il paese/regione dall'elenco a discesa. In alternativa, fare clic su [Immissione codice Paese Internet] e inserire un codice paese, per esempio "US" per gli Stati Uniti.

f [Stato]/[Città]

Inserire il luogo utilizzando caratteri alfanumerici secondo necessità.

g [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione utilizzando caratteri alfanumerici secondo necessità.

h [Nome comune]

Inserire il nome comune del certificato utilizzando caratteri alfanumerici secondo necessità. "Nome comune" viene spesso abbreviato con "CN".

7 Fare clic su [OK].

- La generazione di una chiave e un certificato potrebbe richiedere del tempo.
- Le chiavi e i certificati generati vengono registrati automaticamente nella macchina.

Per un certificato CSR

Generare una chiave e una richiesta CSR sulla macchina. Utilizzare i dati della richiesta CSR visualizzati sullo schermo o esportarli in un file per richiedere l'emissione di un certificato all'autorità di certificazione. In seguito, registrare il certificato emesso per la chiave.
Questa impostazione può essere configurata solo dalla IU remota.

■1. Generazione di chiave e CSR

1 **Avviare la IU remota.**

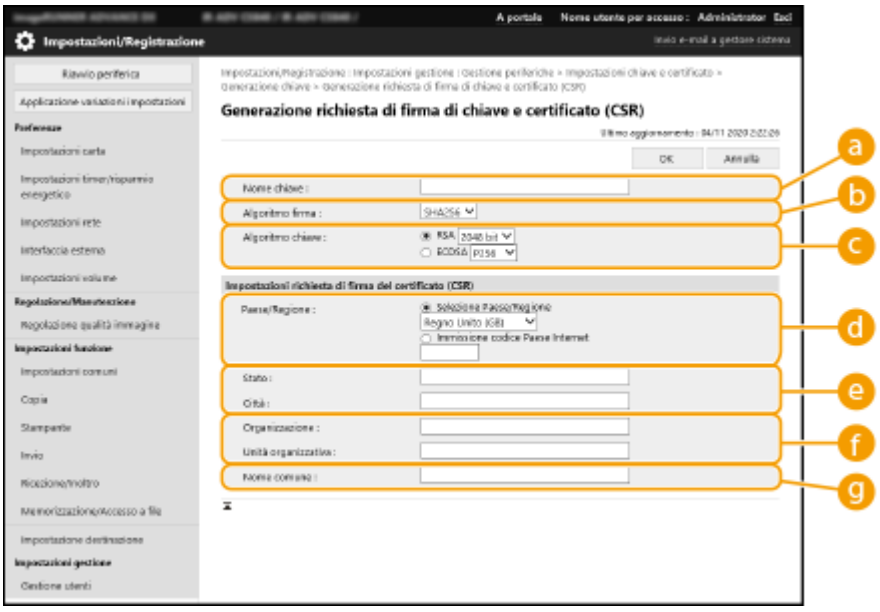
2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Fare clic su [Generazione chiave].**

5 **Fare clic su [Richiesta di firma di chiave e certificato (CSR)].**

6 **Configurare le impostazioni di chiave e certificato.**



a [Nome chiave]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Algoritmo chiave]

Selezionare l'algoritmo chiave e specificare la lunghezza della chiave se si seleziona [RSA], oppure specificare il tipo di chiave se si seleziona [ECDSA].

d [Paese/Regione]

Selezionare il codice paese dall'elenco oppure inserirlo direttamente.

e [Stato]/[Città]

Inserire il luogo.

f [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione.

g [Nome comune]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

7 Fare clic su [OK].

➠ Compaiono i dati della richiesta CSR.

- Se si desidera salvare i dati della richiesta CSR in un file, fare clic su [Memorizzazione in file] e specificare la posizione di salvataggio.

NOTA:

- La chiave che ha generato la richiesta CSR viene visualizzata nella schermata di elenco di chiave e certificato, ma non è possibile utilizzarla autonomamente. Per utilizzare questa chiave è necessario registrare il certificato che viene rilasciato successivamente in base alla richiesta CSR.

8 Richiedere l'emissione di un certificato in base ai dati della richiesta CSR all'autorità di certificazione.

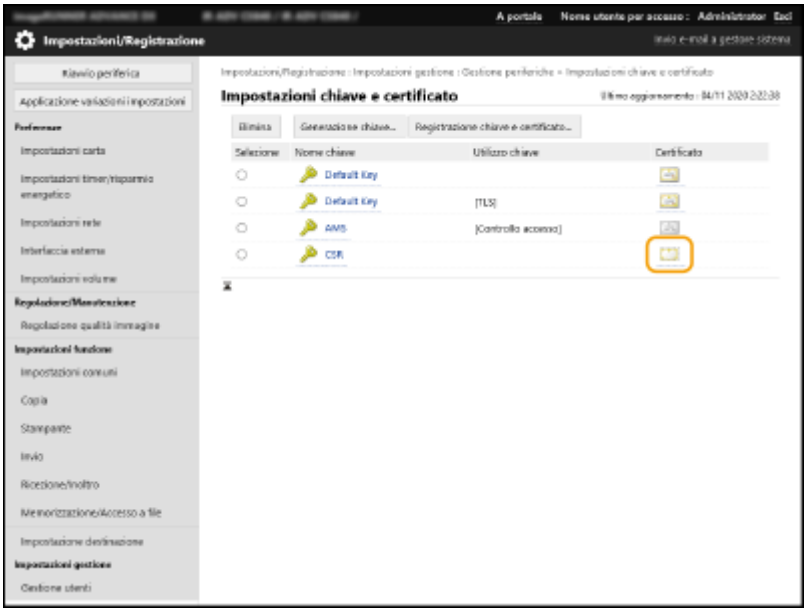
■2. Registrazione del certificato emesso con la chiave

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Nell'elenco [Certificato], fare clic su per il certificato che si desidera registrare.



5 **Fare clic su [Registrazione certificato...].**

6 **Registrare il certificato.**

- Fare clic su [Sfoglia...] ▶ specificare il file (certificato) da registrare ▶ fare clic su [Registra].

Per un certificato SCEP

Richiedere manualmente l'emissione di un certificato al server SCEP.
Questa impostazione può essere configurata solo dalla IU remota.

NOTA

- Se si seleziona [Abilitazione timer per richiesta automatica emissione certificato], non è possibile inviare una richiesta manuale per l'emissione di un certificato. Se questa opzione è selezionata, deselezionarla.

Avviare la IU remota ▶ fare clic su [Impostazioni/Registrazione] ▶ [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)] ▶ [Impostazioni per richiesta automatica emissione certificato] ▶ deselezionare [Abilitazione timer per richiesta automatica emissione certificato] ▶ fare clic su [Aggiornamento].

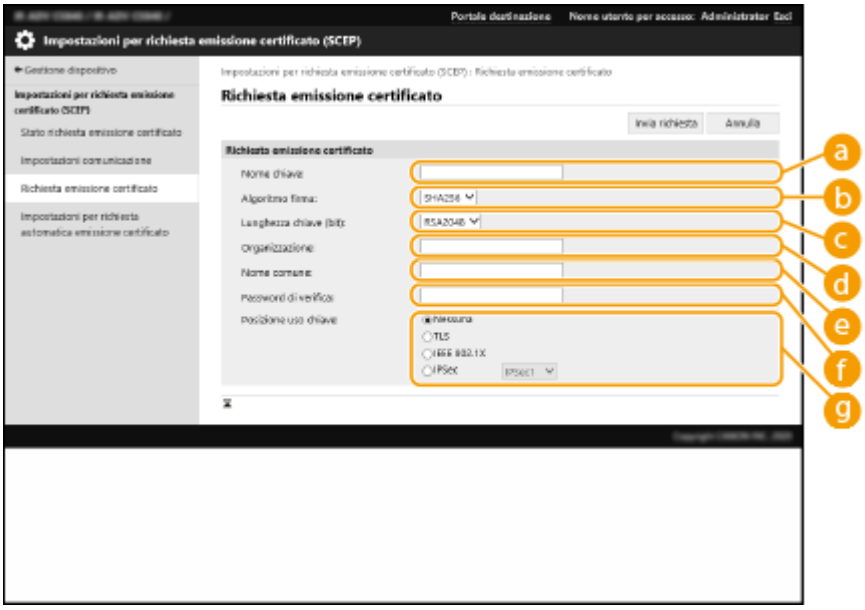
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)].**

4 **Fare clic su [Richiesta emissione certificato].**

5 Configurare le impostazioni necessarie per la richiesta di un certificato.



a [Nome chiave:]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma:]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Lunghezza chiave (bit):]

Selezionare la lunghezza della chiave.

d [Organizzazione:]

Inserire il nome dell'organizzazione.

e [Nome comune:]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

f [Password di verifica:]

Se è impostata una password sul lato del server SCEP, immettere la password di verifica inclusa nei dati della richiesta (PKCS#9) per richiedere l'emissione di un certificato.

g [Posizione uso chiave:]

Selezionare [IEEE 802.1X].

NOTA:

- Quando si seleziona un'opzione diversa da [Nessuna], abilitare ogni funzione in anticipo. Se si ottiene un certificato con tutte le funzioni disabilitate, il certificato viene assegnato alla posizione di utilizzo della chiave, ma le singole funzioni non vengono abilitate automaticamente.

6 Fare clic su [Invia richiesta].

7 **Fare clic su [Riavvio].**

Passaggio 3: Ripristino di chiave e certificato (per IEEE 802.1X)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.
Questa procedura non è necessaria per un certificato SCEP.

Per un certificato autofirmato/certificato CSR

Utilizzo del pannello comandi(P. 39)
Utilizzo della IU remota(P. 40)

■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni IEEE 802.1X>.

3 Premere <On> per <Utilizzo IEEE 802.1X> ▶ configurare le impostazioni necessarie ▶ premere <Avanti>.

Schermata di esempio:

a <Nome accesso>

Immettere il nome (identità EAP) dell'utente di accesso per ricevere l'autenticazione IEEE 802.1X.

b <Verifica certificato server autenticazione>

Configurare questa impostazione su <On> quando si verificano i certificati del server inviati da un server di autenticazione.

c <Verifica nome server di autenticazione>

Per verificare un nome comune nel certificato del server, selezionare <On>. Immettere il nome del server di autenticazione in cui l'utente di accesso è registrato in <Nome server di autenticazione>.

4 Premere <On> per <Utilizzo TLS> ▶ premere <Chiave e certificato>.

5 **Selezionare la chiave e il certificato da utilizzare nell'elenco ▶ premere <Impost.come chiav.predef.> ▶ <Sì>.**

6 **Premere <OK>.**

7 **Premere (Impostazioni/Registrazione) ▶ (Impostazioni/Registrazione) ▶ <Applic.variaz.impost.> ▶ <Sì>.**

➠ La macchina si riavvia e le impostazioni vengono applicate.

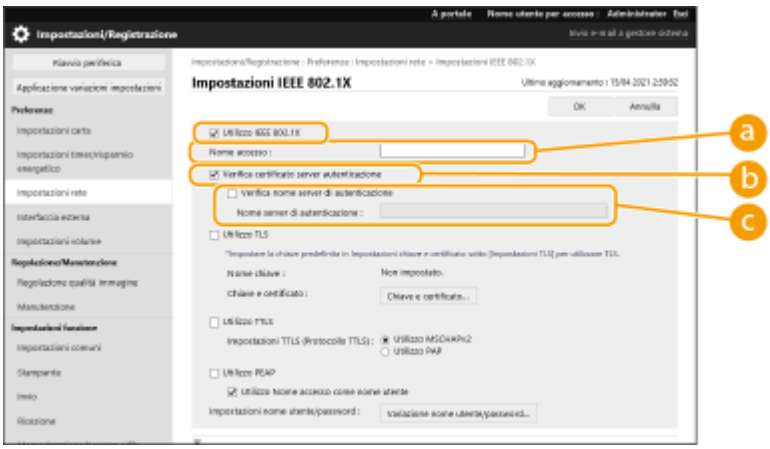
■ Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Impostazioni rete] ▶ [Impostazioni IEEE 802.1X].**

4 **Selezionare [Utilizzo IEEE 802.1X] ▶ configurare le impostazioni necessarie.**



a [Nome accesso]

Immettere il nome (identità EAP) dell'utente di accesso per ricevere l'autenticazione IEEE 802.1X.

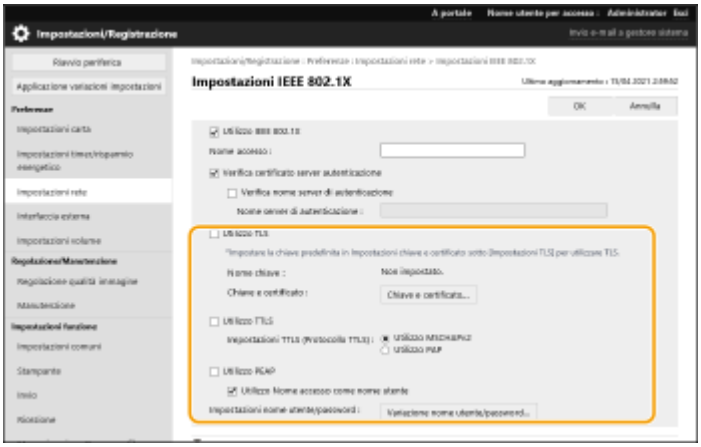
b [Verifica certificato server autenticazione]

Selezionare questa casella di controllo quando si verificano i certificati del server inviati da un server di autenticazione.

c [Verifica nome server di autenticazione]

Per verificare il nome comune nel certificato del server, selezionare questa casella di controllo. Immettere il nome del server di autenticazione in cui l'utente di accesso è registrato in [Nome server di autenticazione].

5 Selezionare [Utilizzo TLS] ▶ fare clic su [Chiave e certificato].



6 Fare clic su [Usare] per la chiave da utilizzare nell'elenco.

7 Fare clic su [OK].

8 Fare clic su [Applicazione variazioni impostazioni] per riavviare la macchina.

➠ La macchina si riavvia e le impostazioni vengono applicate.

Passaggio 4: Eliminazione di chiave/certificato generati in precedenza (per IEEE 802.1X)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

NOTA

- Potrebbe essere necessario fornire informazioni all'autorità di certificazione quando si disabilita il certificato. Consultare **Verifica della necessità delle procedure aggiuntive(P. 5)** e annotare le informazioni necessarie prima di eliminare chiave/certificato.

Utilizzo del pannello comandi(P. 42)
Utilizzo della IU remota(P. 43)

■ Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Elenco chiavi e certificati> ▶ <Elenco chiavi e certificati per la periferica>.**

- <Elenco chiavi e certificati per la periferica> non viene visualizzato a meno che la funzione firma utente non sia abilitata sulla macchina. In questo caso, procedere al passaggio successivo.

3 **Selezionare la chiave e il certificato ▶ premere <Elimina> ▶ <Sì>.**

Schermata di esempio:

NOTA:

- Se compare , la chiave è corrotta o non valida.
- Se non compare , il certificato per la chiave non esiste.
- Se si seleziona una chiave e un certificato e si preme <Dettagli certificato>, saranno visualizzate le informazioni dettagliate sul certificato. Inoltre, per verificare che il certificato sia valido, è possibile premere <Verif. certif.> in questa schermata.

■Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Selezionare la chiave e il certificato ▶ fare clic su [Elimina] ▶ [OK].**

NOTA

- Se compare , la chiave è corrotta o non valida.
- Se compare , il certificato per la chiave non esiste.
- Fare clic su un nome di codice per visualizzare le informazioni dettagliate sul certificato. È anche possibile fare clic su [Verifica certificato] in questa schermata per controllare se il certificato è valido.

Passaggio 5: Disabilitazione del certificato (per IEEE 802.1X)

Disabilitare un certificato generato in precedenza. La procedura varia in base al tipo di certificato.

■ Per un certificato autofirmato

Se un certificato includente una chiave che richiede le procedure aggiuntive viene registrato sul server di autenticazione IEEE 802.1X come certificato attendibile, eliminare il certificato registrato.

■ Per un certificato CSR/SCEP

Richiedere all'autorità di certificazione che ha emesso il certificato di revocare il certificato. Fare riferimento alla voce [Emittente] nel certificato per sapere a quale autorità di certificazione presentare la richiesta.

NOTA

- In caso di verifica della revoca del certificato con un CRL in un server di autenticazione IEEE 802.1X, registrare il CRL aggiornato sul computer o browser web dopo che il certificato è stato revocato.
- Se si utilizza un metodo diverso da CRL (per esempio, OCSP) per verificare la revoca del certificato, attenersi alla procedura relativa a quel metodo.

Passaggio 6: Abilitazione del nuovo certificato (per IEEE 802.1X)

Abilitare il certificato.

■ Per un certificato autofirmato

Registrare il nuovo certificato sul server di autenticazione IEEE 802.1X come certificato attendibile.

■ Per un certificato CSR/SCEP

Le procedure aggiuntive non sono necessarie.

Procedura per IPSec

Passaggio 1: Verifica del metodo di autenticazione (per IPSec)

Se il metodo di autenticazione per l'impostazione IKE in IPSec è impostato su <Metodo firma digitale>, le procedure successive sono necessarie.
Attenersi alla seguente procedura per verificare il metodo di autenticazione.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Utilizzo del pannello comandi(P. 47)
Utilizzo della IU remota(P. 48)

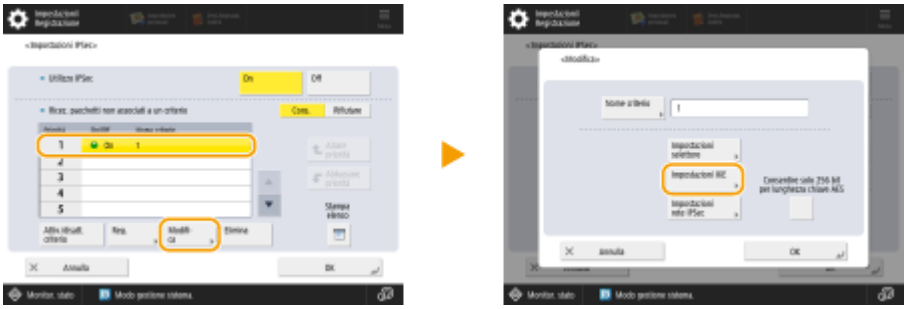
■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni IPSec>.

3 Selezionare il criterio registrato ▶ premere <Modifica> ▶ <Impostazioni IKE>.

Schermata di esempio:



4 Premere <Avanti> ▶ verificare <Metodo di autenticazione>.

Schermata di esempio:

- Se <Metodo di autenticazione> è impostato su <Metodo firma digitale> e viene visualizzato un nome chiave per <Chiave e certificato>, eseguire le procedure successive.
- Se <Metodo di autenticazione> è impostato su <Met. chiave già condivisa>, le procedure successive non sono necessarie.

■Utilizzo della IU remota

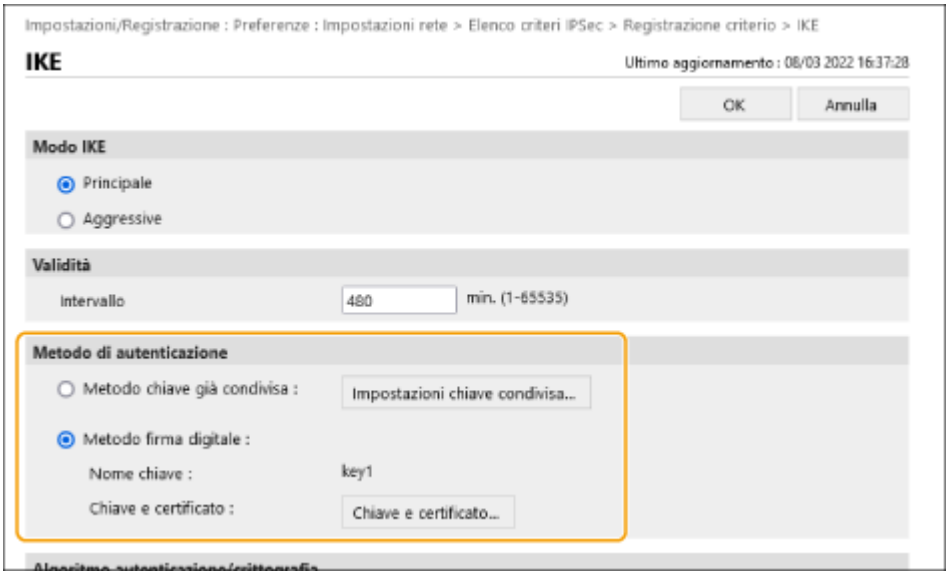
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Impostazioni rete] ▶ [Elenco criteri IPSec].**

4 **Fare clic sul criterio nell'elenco ▶ fare clic su [Impostazioni IKE].**

5 **Controllare [Metodo di autenticazione].**



- Se [Metodo di autenticazione] è impostato su [Metodo firma digitale] e viene visualizzato un nome chiave, eseguire le procedure successive.
- Se <Metodo di autenticazione> è impostato su <Metodo chiave già condivisa>, le procedure successive non sono necessarie.

Passaggio 2: Rigenerazione di chiave e certificato (per IPSec)

È possibile generare tre tipi di certificati per una chiave generata con la macchina: un certificato autofirmato, un certificato CSR e un certificato SCEP. La procedura varia a seconda del tipo di certificato.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Per un certificato autofirmato(P. 49)
Per un certificato CSR(P. 52)
Per un certificato SCEP(P. 54)

Per un certificato autofirmato

Utilizzo del pannello comandi(P. 49)
Utilizzo della IU remota(P. 50)

■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Generazione chiave> ▶ <Generazione chiave comunicazione rete>.

3 Configurare le impostazioni necessarie e procedere alla schermata successiva.

Schermata di esempio:

a <Nome chiave>

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b <Algoritmo firma>

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512. Se si seleziona <RSA> per c e si imposta <Lunghezza chiave (bit)> su <1024> o più per d, è possibile selezionare gli algoritmi hash SHA384 e SHA512.

c <Algoritmo chiave>

Selezionare l'algoritmo della chiave. Se si seleziona <RSA>, <Lunghezza chiave (bit)> compare come voce di impostazione per d. Se si seleziona <ECDSA>, compare invece <Tipo di chiave>.

d <Lunghezza chiave (bit)>/<Tipo di chiave>

Specificare la lunghezza della chiave se si seleziona <RSA> per c oppure specificare il tipo di chiave se si seleziona <ECDSA>. In entrambi i casi, un valore maggiore garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

4 Configurare le voci necessarie per il certificato ▶ premere <Generazione chiave>.

Schermata di esempio:

a <Data inizio validità>/<Data fine validità>

Inserire la data di inizio e la data di fine del periodo di validità del certificato.

b <Paese/Regione>/<Stato>/<Città>/<Organizzazione>/<Unità organizzativa>

Selezionare il codice paese dall'elenco e inserire il nome del luogo e dell'organizzazione.

c <Nome comune>

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

■ Utilizzo della IU remota

1 Avviare la IU remota.

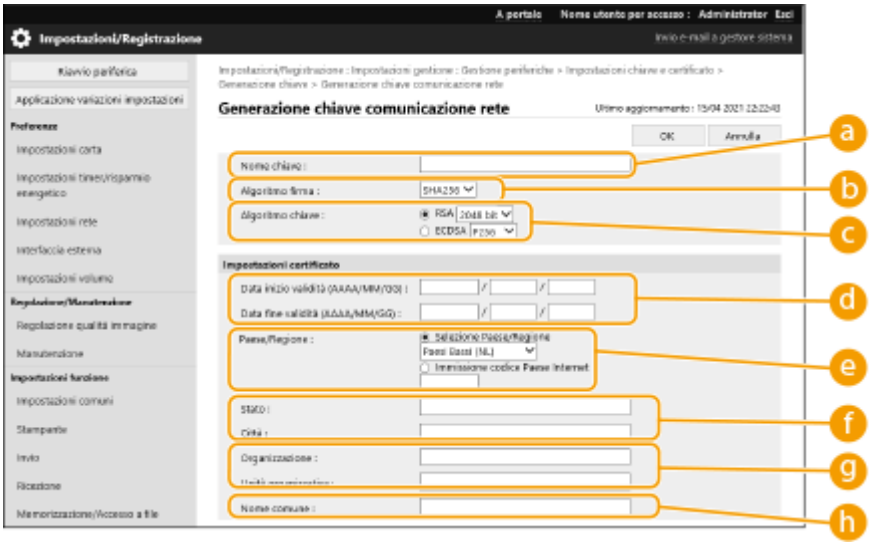
2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Fare clic su [Generazione chiave].

5 Fare clic su [Comunicazione rete].

6 Configurare le impostazioni di chiave e certificato.



a [Nome chiave]

Immettere un nome per la chiave utilizzando caratteri alfanumerici. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512.

c [Algoritmo chiave]

Selezionare [RSA] o [ECDSA] come algoritmo di generazione chiave. Specificare la lunghezza della chiave se si seleziona [RSA] o il tipo di chiave se si seleziona [ECDSA]. In entrambi i casi, un valore più alto garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

NOTA:

- Se si seleziona [SHA384] o [SHA512] per [Algoritmo firma], non è possibile impostare la lunghezza della chiave su [512 bit] quando si seleziona [RSA] per [Algoritmo chiave].

d [Data inizio validità (AAAA/MM/GG)]/[Data fine validità (AAAA/MM/GG)]

Immettere la data di inizio e la data di fine del periodo di validità del certificato. Il valore [Data fine validità (AAAA/MM/GG)] non può essere impostato su una data precedente alla data in [Data inizio validità (AAAA/MM/GG)].

e [Paese/Regione]

Fare clic su [Selezione Paese/Regione] e selezionare il paese/regione dall'elenco a discesa. In alternativa, fare clic su [Immissione codice Paese Internet] e inserire un codice paese, per esempio "US" per gli Stati Uniti.

f [Stato]/[Città]

Inserire il luogo utilizzando caratteri alfanumerici secondo necessità.

g [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione utilizzando caratteri alfanumerici secondo necessità.

h [Nome comune]

Inserire il nome comune del certificato utilizzando caratteri alfanumerici secondo necessità. "Nome comune" viene spesso abbreviato con "CN".

7 Fare clic su [OK].

- La generazione di una chiave e un certificato potrebbe richiedere del tempo.
- Le chiavi e i certificati generati vengono registrati automaticamente nella macchina.

Per un certificato CSR

Generare una chiave e una richiesta CSR sulla macchina. Utilizzare i dati della richiesta CSR visualizzati sullo schermo o esportarli in un file per richiedere l'emissione di un certificato all'autorità di certificazione. In seguito, registrare il certificato emesso per la chiave.
Questa impostazione può essere configurata solo dalla IU remota.

■1. Generazione di chiave e CSR

1 **Avviare la IU remota.**

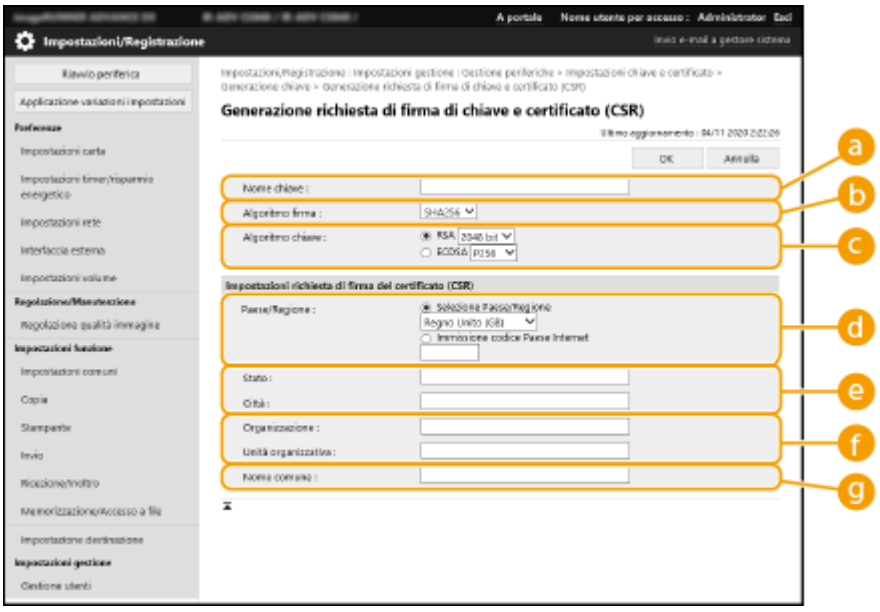
2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Fare clic su [Generazione chiave].**

5 **Fare clic su [Richiesta di firma di chiave e certificato (CSR)].**

6 **Configurare le impostazioni di chiave e certificato.**



a [Nome chiave]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Algoritmo chiave]

Selezionare l'algoritmo chiave e specificare la lunghezza della chiave se si seleziona [RSA], oppure specificare il tipo di chiave se si seleziona [ECDSA].

d [Paese/Regione]

Selezionare il codice paese dall'elenco oppure inserirlo direttamente.

e [Stato]/[Città]

Inserire il luogo.

f [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione.

g [Nome comune]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

7 Fare clic su [OK].

➡ Compaiono i dati della richiesta CSR.

- Se si desidera salvare i dati della richiesta CSR in un file, fare clic su [Memorizzazione in file] e specificare la posizione di salvataggio.

NOTA:

- La chiave che ha generato la richiesta CSR viene visualizzata nella schermata di elenco di chiave e certificato, ma non è possibile utilizzarla autonomamente. Per utilizzare questa chiave è necessario registrare il certificato che viene rilasciato successivamente in base alla richiesta CSR.

8 Richiedere l'emissione di un certificato in base ai dati della richiesta CSR all'autorità di certificazione.

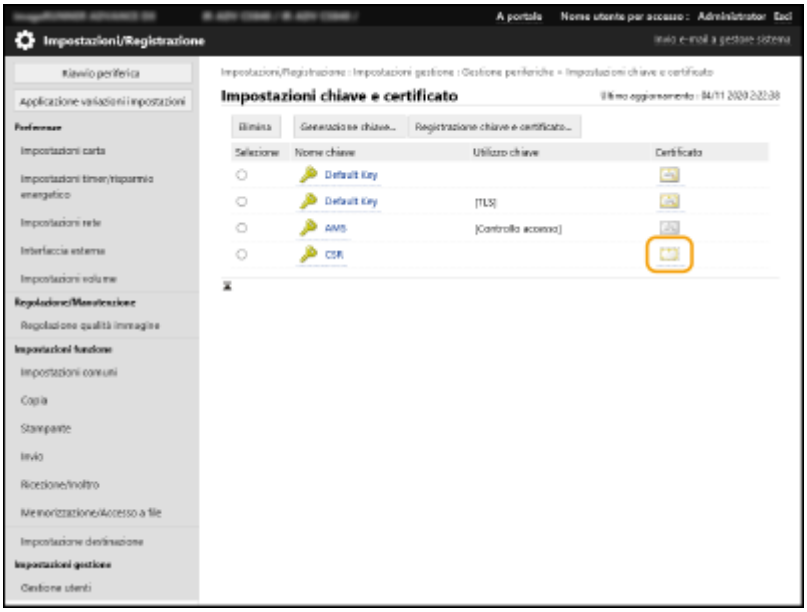
■2. Registrazione del certificato emesso con la chiave

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Nell'elenco [Certificato], fare clic su per il certificato che si desidera registrare.



5 **Fare clic su [Registrazione certificato...].**

6 **Registrare il certificato.**

- Fare clic su [Sfoglia...] ▶ specificare il file (certificato) da registrare ▶ fare clic su [Registra].

Per un certificato SCEP

Richiedere manualmente l'emissione di un certificato al server SCEP.
Questa impostazione può essere configurata solo dalla IU remota.

NOTA

- Se si seleziona [Abilitazione timer per richiesta automatica emissione certificato], non è possibile inviare una richiesta manuale per l'emissione di un certificato. Se questa opzione è selezionata, deselezionarla.

Avviare la IU remota ▶ fare clic su [Impostazioni/Registrazione] ▶ [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)] ▶ [Impostazioni per richiesta automatica emissione certificato] ▶ deselezionare [Abilitazione timer per richiesta automatica emissione certificato] ▶ fare clic su [Aggiornamento].

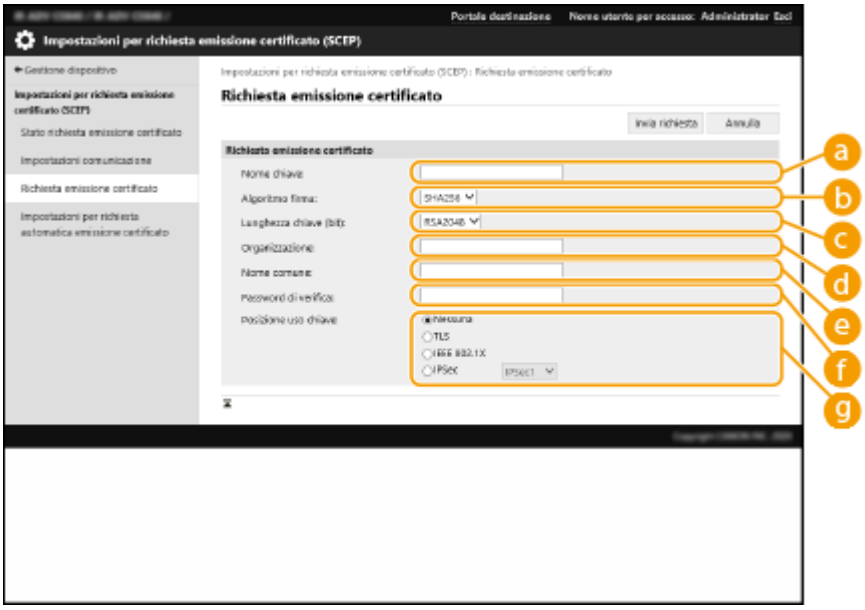
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni per richiesta rilascio certificato (SCEP)].**

4 **Fare clic su [Richiesta emissione certificato].**

5 Configurare le impostazioni necessarie per la richiesta di un certificato.



a [Nome chiave:]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma:]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Lunghezza chiave (bit):]

Selezionare la lunghezza della chiave.

d [Organizzazione:]

Inserire il nome dell'organizzazione.

e [Nome comune:]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

f [Password di verifica:]

Se è impostata una password sul lato del server SCEP, immettere la password di verifica inclusa nei dati della richiesta (PKCS#9) per richiedere l'emissione di un certificato.

g [Posizione uso chiave:]

Selezionare [IPSec].

NOTA:

- Quando si seleziona un'opzione diversa da [Nessuna], abilitare ogni funzione in anticipo. Se si ottiene un certificato con tutte le funzioni disabilitate, il certificato viene assegnato alla posizione di utilizzo della chiave, ma le singole funzioni non vengono abilitate automaticamente.

6 Fare clic su [Invia richiesta].

7 **Fare clic su [Riavvio].**

Passaggio 3: Ripristino di chiave e certificato (per IPSec)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.
Questa procedura non è necessaria per un certificato SCEP.

Per un certificato autofirmato/certificato CSR

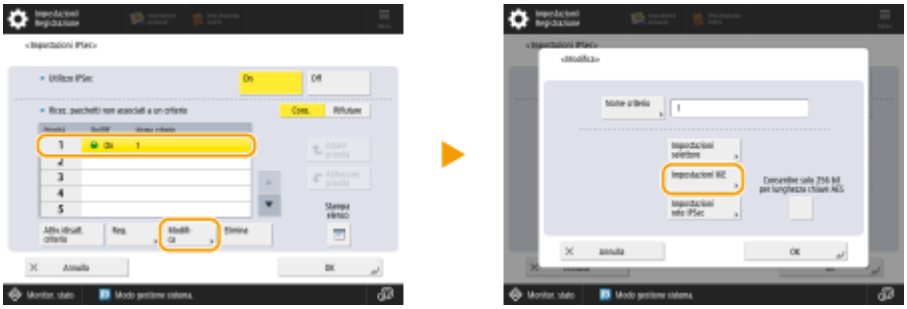
Utilizzo del pannello comandi(P. 57)
Utilizzo della IU remota(P. 58)

■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni IPSec>.**

3 **Selezionare il criterio per il ripristino di chiave e certificato ▶ premere <Modifica> ▶ <Impostazioni IKE>.**
Schermata di esempio:



4 **Premere <Avanti> ▶ selezionare <Metodo firma digitale> in <Metodo di autenticazione> ▶ premere <Chiave e certificato>.**
Schermata di esempio:

5 **Selezionare la chiave e il certificato da utilizzare nell'elenco ▶ premere <Impost.come chiav.predef.> ▶ <Sì>.**

6 **Premere <OK>.**

7 **Premere (Impostazioni/Registrazione) ▶ (Impostazioni/Registrazione) ▶ <Applic.variaz.impost.> ▶ <Sì>.**

➠ La macchina si riavvia e le impostazioni vengono applicate.

■ Utilizzo della IU remota

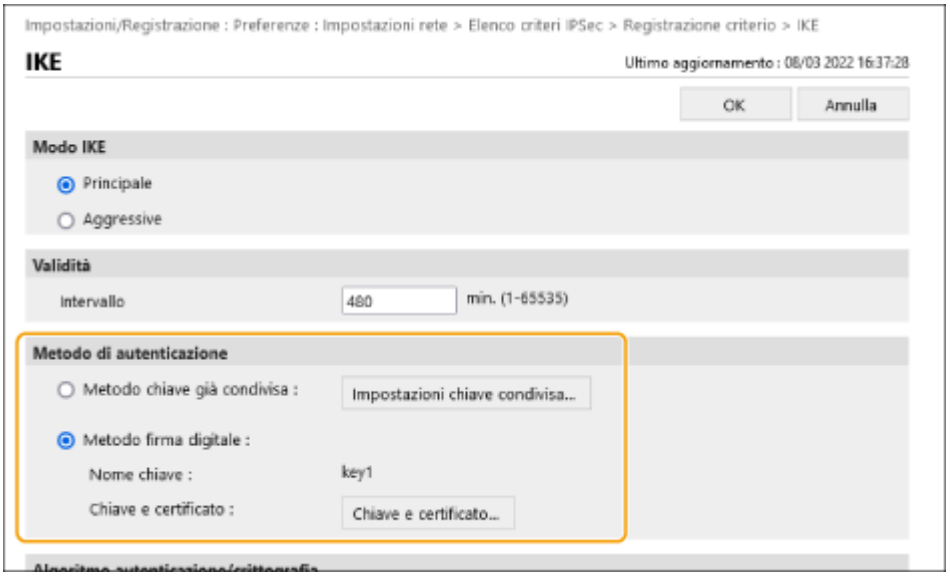
1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Impostazioni rete] ▶ [Elenco criteri IPSec].**

4 **Fare clic sul criterio per il ripristino di chiave e certificato nell'elenco ▶ fare clic su [Impostazioni IKE].**

5 **Selezionare [Metodo firma digitale] in [Metodo di autenticazione] ▶ fare clic su [Chiave e certificato].**



6 **Fare clic su [Usare] per la chiave da utilizzare nell'elenco.**

7 **Fare clic su [OK].**

8 Fare clic su [Applicazione variazioni impostazioni] per riavviare la macchina.

➠ La macchina si riavvia e le impostazioni vengono applicate.

Passaggio 4: Eliminazione di chiave/certificato generati in precedenza (per IPSec)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

NOTA

- Potrebbe essere necessario fornire informazioni all'autorità di certificazione quando si disabilita il certificato. Consultare **Verifica della necessità delle procedure aggiuntive(P. 5)** e annotare le informazioni necessarie prima di eliminare chiave/certificato.

Utilizzo del pannello comandi(P. 60)
Utilizzo della IU remota(P. 61)

■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Elenco chiavi e certificati> ▶ <Elenco chiavi e certificati per la periferica>.**

- <Elenco chiavi e certificati per la periferica> non viene visualizzato a meno che la funzione firma utente non sia abilitata sulla macchina. In questo caso, procedere al passaggio successivo.

3 **Selezionare la chiave e il certificato ▶ premere <Elimina> ▶ <Sì>.**

Schermata di esempio:

NOTA:

- Se compare , la chiave è corrotta o non valida.
- Se non compare , il certificato per la chiave non esiste.
- Se si seleziona una chiave e un certificato e si preme <Dettagli certificato>, saranno visualizzate le informazioni dettagliate sul certificato. Inoltre, per verificare che il certificato sia valido, è possibile premere <Verif. certif.> in questa schermata.

■Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Selezionare la chiave e il certificato ▶ fare clic su [Elimina] ▶ [OK].**

NOTA

- Se compare , la chiave è corrotta o non valida.
- Se compare , il certificato per la chiave non esiste.
- Fare clic su un nome di codice per visualizzare le informazioni dettagliate sul certificato. È anche possibile fare clic su [Verifica certificato] in questa schermata per controllare se il certificato è valido.

Passaggio 5: Disabilitazione del certificato (per IPSec)

Disabilitare un certificato generato in precedenza. La procedura varia in base al tipo di certificato.

■ Per un certificato autofirmato

Se un certificato includente una chiave che richiede le procedure aggiuntive viene registrato nella periferica che comunica con IPSec come certificato attendibile, eliminare il certificato registrato. Dopo aver eliminato il certificato registrato, registrare il certificato della chiave rigenerata.

■ Per un certificato CSR/SCEP

Richiedere all'autorità di certificazione che ha emesso il certificato di revocare il certificato. Fare riferimento alla voce [Emittente] nel certificato per sapere a quale autorità di certificazione presentare la richiesta.

NOTA

- In caso di verifica della revoca del certificato con un CRL nella periferica che comunica con IPSec, registrare il CRL aggiornato sul computer o browser web dopo che il certificato è stato revocato.
- Se si utilizza un metodo diverso da CRL (per esempio, OCSP) per verificare la revoca del certificato, attenersi alla procedura relativa a quel metodo.

Passaggio 6: Abilitazione del nuovo certificato (per IPSec)

Abilitare il certificato.

■ Per un certificato autofirmato

Registrare il nuovo certificato sulla periferica che comunica con IPSec come certificato attendibile.

■ Per un certificato CSR/SCEP

Le procedure aggiuntive non sono necessarie.

Procedura per SIP

Passaggio 1: Verifica delle impostazioni (per SIP)

Se le seguenti condizioni sono entrambe soddisfatte, è necessario attenersi alle procedure aggiuntive:

- <Utilizzo TLS> è abilitato in <Impostazioni intranet> in <Impostazioni SIP>
- Il nome chiave viene visualizzato per <Chiave e certificato> in <Impostazioni TLS> in <Impostazioni SIP>

Attenersi alla seguente procedura per verificare le impostazioni.

Utilizzo del pannello comandi(P. 65)
Utilizzo della IU remota(P. 66)

Utilizzo del pannello comandi

■Verifica di <Utilizzo TLS>

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni SIP> ▶ <Impostazioni intranet>.**

3 **Verificare <Utilizzo TLS>.**

Schermata di esempio:

- Se <Utilizzo TLS> è impostato su <On>, procedere alla verifica di <Chiave e certificato>.
- Se <Utilizzo TLS> è impostato su <Off>, le procedure successive non sono necessarie.

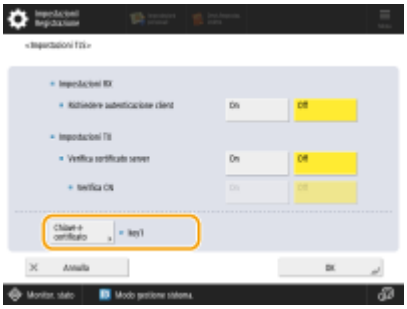
■Verifica di <Chiave e certificato>

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni SIP> ▶ <Impostazioni TLS>.**

3 Verificare se il nome chiave viene visualizzato per <Chiave e certificato>.

Schermata di esempio:



- Se viene visualizzato un nome chiave per <Chiave e certificato>, eseguire le procedure successive.
- Se il nome chiave non viene visualizzato per <Chiave e certificato>, non è necessario seguire le procedure successive.

Utilizzo della IU remota

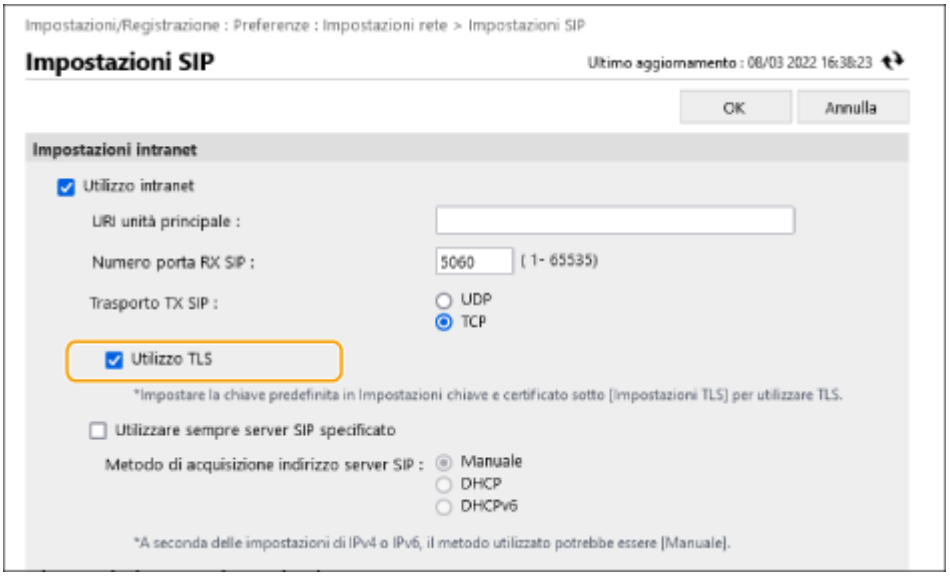
■Verifica di [Utilizzo TLS] e [Chiave e certificato]

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

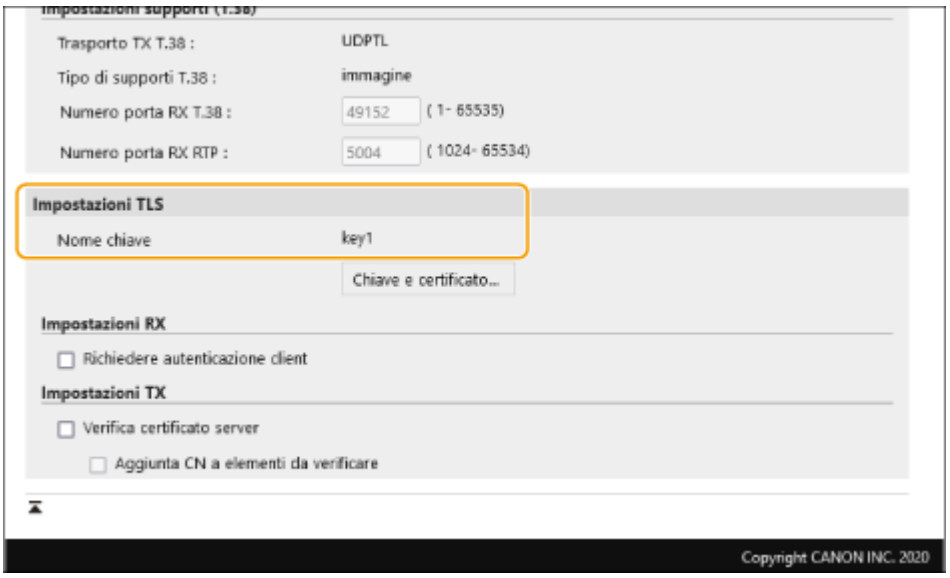
3 Fare clic su [Impostazioni rete] ▶ [Impostazioni SIP].

4 Verificare [Utilizzo TLS] in [Impostazioni intranet].



- Se [Utilizzo TLS] è selezionato, verificare [Chiave e certificato].
- Se [Utilizzo TLS] è deselezionato, le procedure successive non sono necessarie.

5 Verificare [Nome chiave] in [Impostazioni TLS].



- Se viene visualizzato un nome chiave, eseguire le procedure successive.
- Se il nome chiave non viene visualizzato, le procedure successive non sono necessarie.

Passaggio 2: Rigenerazione di chiave e certificato (per SIP)

È possibile generare due tipi di certificati per una chiave generata con la macchina: un certificato autofirmato e un certificato CSR. La procedura varia a seconda del tipo di certificato.
In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

Per un certificato autofirmato(P. 68)
Per un certificato CSR(P. 71)

Per un certificato autofirmato

Utilizzo del pannello comandi(P. 68)
Utilizzo della IU remota(P. 69)

■ Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Generazione chiave> ▶ <Generazione chiave comunicazione rete>.**

3 **Configurare le impostazioni necessarie e procedere alla schermata successiva.**

Schermata di esempio:

a <Nome chiave>

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b <Algoritmo firma>

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512. Se si seleziona <RSA> per c e si imposta <Lunghezza chiave (bit)> su <1024> o più per d, è possibile selezionare gli algoritmi hash SHA384 e SHA512.

c <Algoritmo chiave>

Selezionare l'algoritmo della chiave. Se si seleziona <RSA>, <Lunghezza chiave (bit)> compare come voce di impostazione per d. Se si seleziona <ECDSA>, compare invece <Tipo di chiave>.

d <Lunghezza chiave (bit)>/<Tipo di chiave>

Specificare la lunghezza della chiave se si seleziona <RSA> per c oppure specificare il tipo di chiave se si seleziona <ECDSA>. In entrambi i casi, un valore maggiore garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

4 Configurare le voci necessarie per il certificato ▶ premere <Generazione chiave>.

Schermata di esempio:

a <Data inizio validità>/<Data fine validità>

Inserire la data di inizio e la data di fine del periodo di validità del certificato.

b <Paese/Regione>/<Stato>/<Città>/<Organizzazione>/<Unità organizzativa>

Selezionare il codice paese dall'elenco e inserire il nome del luogo e dell'organizzazione.

c <Nome comune>

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

■ Utilizzo della IU remota

1 Avviare la IU remota.

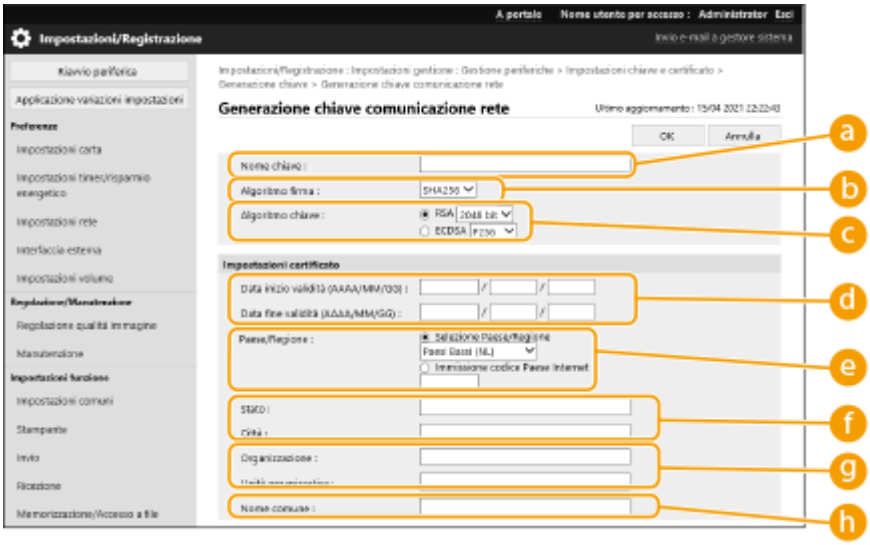
2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Fare clic su [Generazione chiave].

5 Fare clic su [Comunicazione rete].

6 Configurare le impostazioni di chiave e certificato.



a [Nome chiave]

Immettere un nome per la chiave utilizzando caratteri alfanumerici. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash da utilizzare per la firma. Gli algoritmi hash disponibili variano in base alla lunghezza della chiave. Una lunghezza chiave di 1024 bit o più può supportare gli algoritmi hash SHA384 e SHA512.

c [Algoritmo chiave]

Selezionare [RSA] o [ECDSA] come algoritmo di generazione chiave. Specificare la lunghezza della chiave se si seleziona [RSA] o il tipo di chiave se si seleziona [ECDSA]. In entrambi i casi, un valore più alto garantisce una maggiore sicurezza, ma riduce la velocità di elaborazione della comunicazione.

NOTA:

- Se si seleziona [SHA384] o [SHA512] per [Algoritmo firma], non è possibile impostare la lunghezza della chiave su [512 bit] quando si seleziona [RSA] per [Algoritmo chiave].

d [Data inizio validità (AAAA/MM/GG)]/[Data fine validità (AAAA/MM/GG)]

Immettere la data di inizio e la data di fine del periodo di validità del certificato. Il valore [Data fine validità (AAAA/MM/GG)] non può essere impostato su una data precedente alla data in [Data inizio validità (AAAA/MM/GG)].

e [Paese/Regione]

Fare clic su [Selezione Paese/Regione] e selezionare il paese/regione dall'elenco a discesa. In alternativa, fare clic su [Immissione codice Paese Internet] e inserire un codice paese, per esempio "US" per gli Stati Uniti.

f [Stato]/[Città]

Inserire il luogo utilizzando caratteri alfanumerici secondo necessità.

g [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione utilizzando caratteri alfanumerici secondo necessità.

h [Nome comune]

Inserire il nome comune del certificato utilizzando caratteri alfanumerici secondo necessità. "Nome comune" viene spesso abbreviato con "CN".

7 Fare clic su [OK].

- La generazione di una chiave e un certificato potrebbe richiedere del tempo.
- Le chiavi e i certificati generati vengono registrati automaticamente nella macchina.

Per un certificato CSR

Generare una chiave e una richiesta CSR sulla macchina. Utilizzare i dati della richiesta CSR visualizzati sullo schermo o esportarli in un file per richiedere l'emissione di un certificato all'autorità di certificazione. In seguito, registrare il certificato emesso per la chiave.
Questa impostazione può essere configurata solo dalla IU remota.

■1. Generazione di chiave e CSR

1 **Avviare la IU remota.**

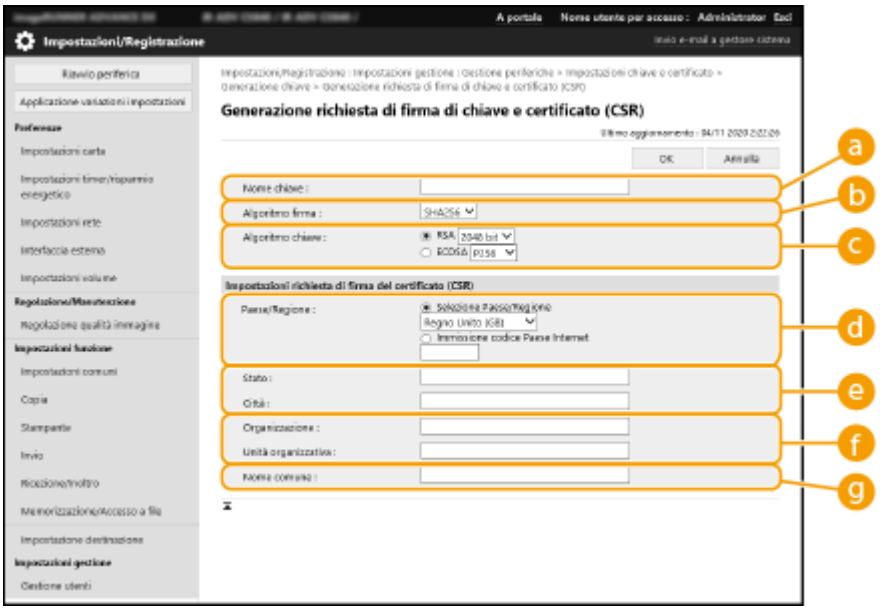
2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Fare clic su [Generazione chiave].**

5 **Fare clic su [Richiesta di firma di chiave e certificato (CSR)].**

6 **Configurare le impostazioni di chiave e certificato.**



a [Nome chiave]

Immettere un nome per la chiave. Sceglierne uno facile da trovare in un elenco.

b [Algoritmo firma]

Selezionare l'algoritmo hash per utilizzare la firma.

c [Algoritmo chiave]

Selezionare l'algoritmo chiave e specificare la lunghezza della chiave se si seleziona [RSA], oppure specificare il tipo di chiave se si seleziona [ECDSA].

d [Paese/Regione]

Selezionare il codice paese dall'elenco oppure inserirlo direttamente.

e [Stato]/[Città]

Inserire il luogo.

f [Organizzazione]/[Unità organizzativa]

Inserire il nome dell'organizzazione.

g [Nome comune]

Inserire l'indirizzo IP o l'FQDN.

- Quando si esegue la stampa IPPS in un ambiente Windows, inserire l'indirizzo IP della macchina.
- Per immettere l'FQDN della macchina è necessario un server DNS. Inserire l'indirizzo IP della macchina se non si utilizza un server DNS.

7 Fare clic su [OK].

➠ Compaiono i dati della richiesta CSR.

- Se si desidera salvare i dati della richiesta CSR in un file, fare clic su [Memorizzazione in file] e specificare la posizione di salvataggio.

NOTA:

- La chiave che ha generato la richiesta CSR viene visualizzata nella schermata di elenco di chiave e certificato, ma non è possibile utilizzarla autonomamente. Per utilizzare questa chiave è necessario registrare il certificato che viene rilasciato successivamente in base alla richiesta CSR.

8 Richiedere l'emissione di un certificato in base ai dati della richiesta CSR all'autorità di certificazione.

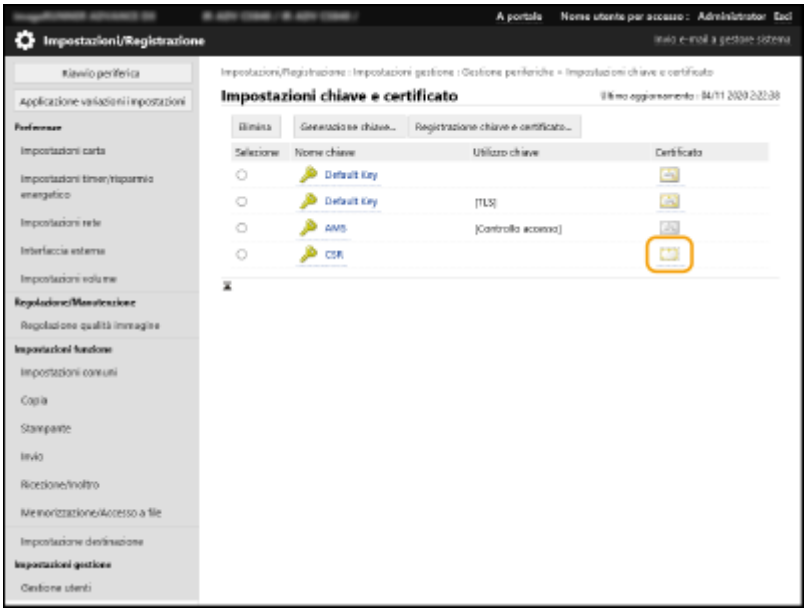
■2. Registrazione del certificato emesso con la chiave

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].

4 Nell'elenco [Certificato], fare clic su per il certificato che si desidera registrare.



5 Fare clic su [Registrazione certificato...].

6 Registrare il certificato.

- Fare clic su [Sfoglia...] ▶ specificare il file (certificato) da registrare ▶ fare clic su [Registra].

Passaggio 3: Ripristino di chiave e certificato (per SIP)

Impostare la chiave e il certificato generati come la chiave e il certificato da utilizzare nella comunicazione crittografata TLS di SIP.

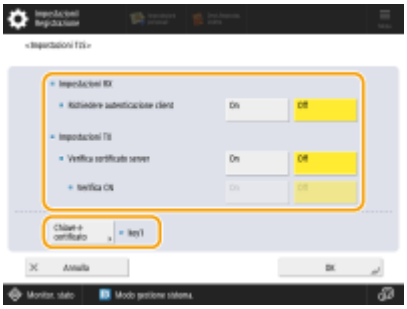
Utilizzo del pannello comandi(P. 74)
Utilizzo della IU remota(P. 75)

Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Preferenze> ▶ <Rete> ▶ <Impostazioni TCP/IP> ▶ <Impostazioni SIP> ▶ <Impostazioni TLS>.**

3 **Configurare le varie impostazioni in <Impostazioni RX> e <Impostazioni TX> ▶ premere <Chiave e certificato>.**
Schermata di esempio:



<Impostazioni RX>	
<Richiedere autenticazione client>	Selezionare <On> o <Off>. Se si seleziona <On>, la macchina richiede l'autenticazione client quando riceve un fax IP.
<Impostazioni TX>	
<Verifica certificato server>	Selezionare <On> o <Off>. Se si seleziona <On>, la macchina verifica la validità del certificato del server TLS quando riceve un fax IP.
<Verifica CN>	Selezionare <On> o <Off>. Se si seleziona <On>, la macchina verifica il CN (Nome comune) quando riceve un fax IP.

4 **Selezionare la chiave e il certificato da utilizzare per la comunicazione crittografata TLS di SIP ▶ premere <Impost.come chiav.predef.> ▶ <OK>.**
Schermata di esempio:

NOTA

- Non è possibile selezionare la chiave e il certificato se il loro stato è "Utilizzo".
- È possibile premere <Dettagli certificato> per accedere a informazioni dettagliate sul certificato.
- È possibile premere <Visualizzaz. posiz. utilizzo> per verificare l'utilizzo di chiave/certificato.

5 **Premere <OK>.**

6 **Premere (Impostazioni/Registrazione) ▶ (Impostazioni/Registrazione) ▶ <Applicazione variazioni impostazioni> ▶ <Sì>.**

➠ La macchina si riavvia e le impostazioni vengono applicate.

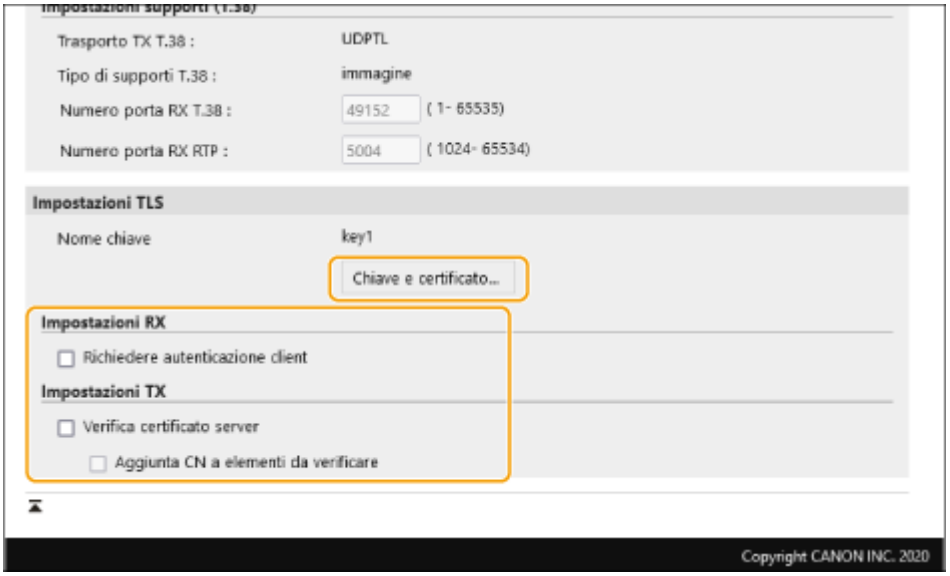
■ Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

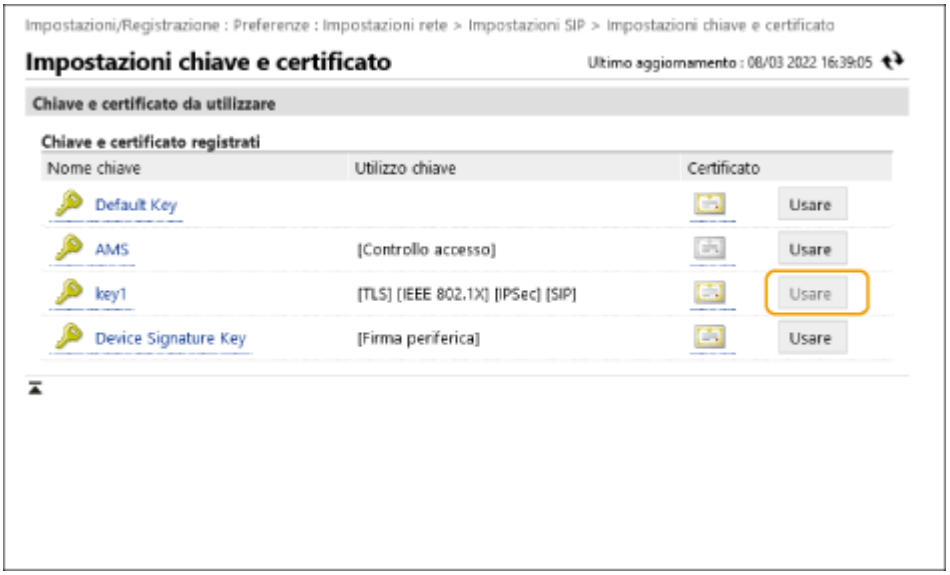
3 **Fare clic su [Impostazioni rete] ▶ [Impostazioni SIP].**

4 **Configurare le varie impostazioni in [Impostazioni TLS] ▶ fare clic su [Chiave e certificato].**



[Impostazioni RX]	
[Richiedere autenticazione client]	Se si seleziona questa casella di controllo, la macchina richiede l'autenticazione client quando riceve un fax IP.
[Impostazioni TX]	
[Verifica certificato server]	Se si seleziona questa casella di controllo, la macchina verifica la validità del certificato del server TLS quando riceve un fax IP.
[Aggiunta CN a elementi da verificare]	Selezionare [On] o [Off]. Se si seleziona questa casella di controllo, la macchina verifica il CN (Nome comune) quando riceve un fax IP.

5 Fare clic su [Usare] per la chiave da utilizzare nell'elenco.



6 Fare clic su [OK].

7 Fare clic su [Applicazione variazioni impostazioni] per riavviare la macchina.

➠ La macchina si riavvia e le impostazioni vengono applicate.

Passaggio 4: Eliminazione di chiave/certificato generati in precedenza (per SIP)

In base al modello della macchina in uso, potrebbe non essere possibile eseguire operazioni dal pannello comandi. In questo caso, eseguire le operazioni dalla IU remota.

NOTA

- Potrebbe essere necessario fornire informazioni all'autorità di certificazione quando si disabilita il certificato. Consultare **Verifica della necessità delle procedure aggiuntive(P. 5)** e annotare le informazioni necessarie prima di eliminare chiave/certificato.

Utilizzo del pannello comandi(P. 77)
Utilizzo della IU remota(P. 78)

■Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Elenco chiavi e certificati> ▶ <Elenco chiavi e certificati per la periferica>.**

- <Elenco chiavi e certificati per la periferica> non viene visualizzato a meno che la funzione firma utente non sia abilitata sulla macchina. In questo caso, procedere al passaggio successivo.

3 **Selezionare la chiave e il certificato ▶ premere <Elimina> ▶ <Sì>.**

Schermata di esempio:

NOTA:

- Se compare , la chiave è corrotta o non valida.
- Se non compare , il certificato per la chiave non esiste.
- Se si seleziona una chiave e un certificato e si preme <Dettagli certificato>, saranno visualizzate le informazioni dettagliate sul certificato. Inoltre, per verificare che il certificato sia valido, è possibile premere <Verif. certif.> in questa schermata.

■Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Selezionare la chiave e il certificato ▶ fare clic su [Elimina] ▶ [OK].**

NOTA

- Se compare , la chiave è corrotta o non valida.
- Se compare , il certificato per la chiave non esiste.
- Fare clic su un nome di codice per visualizzare le informazioni dettagliate sul certificato. È anche possibile fare clic su [Verifica certificato] in questa schermata per controllare se il certificato è valido.

Passaggio 5: Disabilitazione del certificato (per SIP)

Disabilitare un certificato generato in precedenza. La procedura varia in base al tipo di certificato.

■ Per un certificato autofirmato

Se un certificato includente una chiave che richiede le procedure aggiuntive viene registrato su un'altra macchina fax IP come certificato attendibile, eliminare il certificato registrato. Dopo aver eliminato il certificato registrato, registrare il certificato della chiave rigenerata.

■ Per un certificato CSR

Richiedere all'autorità di certificazione che ha emesso il certificato di revocare il certificato. Fare riferimento alla voce [Emittente] nel certificato per sapere a quale autorità di certificazione presentare la richiesta.

NOTA

- In caso di verifica della revoca del certificato con l'altra macchina IP fax, registrare il CRL aggiornato sul computer o browser web dopo che il certificato è stato revocato.
- Se si utilizza un metodo diverso da CRL (per esempio, OCSP) per verificare la revoca del certificato, attenersi alla procedura relativa a quel metodo.

Passaggio 6: Abilitazione del nuovo certificato (per SIP)

Abilitare il certificato.

■ Per un certificato autofirmato

Registrare il nuovo certificato sull'altra macchina fax IP come certificato attendibile.

■ Per un certificato CSR

Le procedure aggiuntive non sono necessarie.

Procedura per firma periferica

Passaggio 1: Verifica delle impostazioni S/MIME (per firma periferica)

Verificare la necessità delle procedure aggiuntive per S/MIME e la firma periferica.

Attenersi alla seguente procedura per verificare le impostazioni S/MIME.

Utilizzo del pannello comandi(P. 82)
Utilizzo della IU remota(P. 82)

■Utilizzo del pannello comandi

1 Premere (Impostazioni/Registrazione).

2 Premere <Impostazioni funzione> ▶ <Invio> ▶ <Impostazioni e-mail/I-Fax> ▶ <Impostazioni S/MIME>.

3 Verificare <Impostazioni crittografia> e <Aggiunta firme digitali>.

Schermata di esempio:

- Se <Impostazioni crittografia> è impostato su <Non crittografare> e <Aggiunta firme digitali> è impostato su <Off>, eseguire le procedure successive solo per la firma periferica.
- Se sono specificate altre impostazioni, eseguire le procedure successive sia per S/MIME che per la firma periferica.

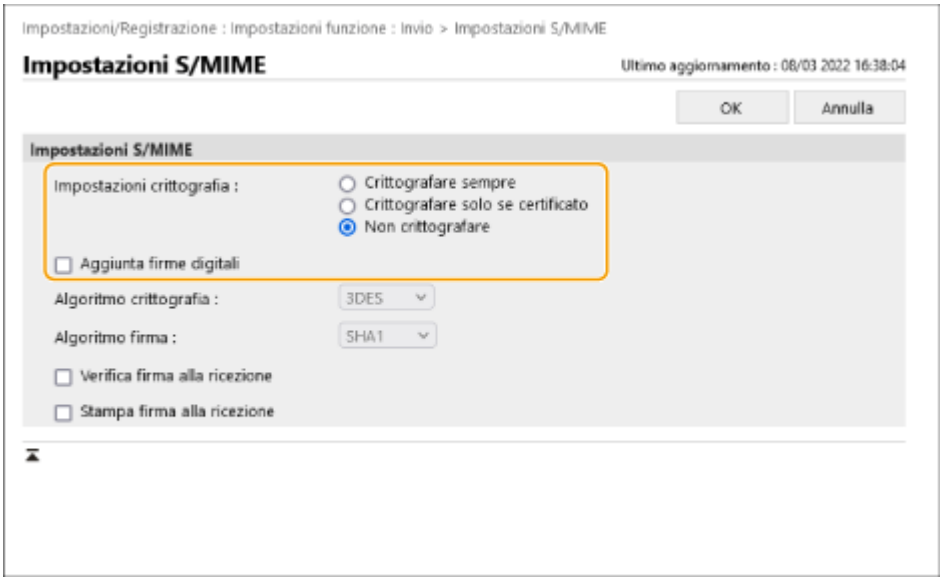
■Utilizzo della IU remota

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Invio] ▶ [Impostazioni S/MIME].

4 Verificare [Impostazioni crittografia] e [Aggiunta firme digitali].



- Se [Non crittografare] è selezionato per [Impostazioni crittografia] e [Aggiunta firme digitali] è deselezionato, eseguire le procedure successive solo per la firma periferica.
- Se sono specificate altre impostazioni, eseguire le procedure successive sia per S/MIME che per la firma periferica.

Passaggio 2: Rigenerazione di chiave e certificato (per firma periferica)

Utilizzo del pannello comandi(P. 84)
Utilizzo della IU remota(P. 84)

■ Utilizzo del pannello comandi

1 **Premere (Impostazioni/Registrazione).**

2 **Premere <Impostazioni gestione> ▶ <Gestione periferiche> ▶ <Impostazioni certificato> ▶ <Generazione chiave>.**

3 **Premere <Generazione/Aggiornam. chiave firma periferica> ▶ <Sì> ▶ <OK>.**

■ Utilizzo della IU remota

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni chiave e certificato].**

4 **Fare clic su [Generazione chiave] ▶ [Firma periferica].**

5 **Fare clic su [Generazione/Aggiornamento] ▶ [OK].**

Passaggio 3: Disabilitazione del certificato (per firma periferica)

Disabilitare un certificato generato in precedenza.

■Se un certificato per firma periferica è registrato su Acrobat

Se un certificato per firma periferica è registrato su Acrobat, eliminare il certificato registrato.

■Se un certificato S/MIME esportato da questa macchina è stato importato in un'altra macchina

Se il certificato della chiave pubblica (certificato S/MIME) utilizzato per crittografare e-mail/I-fax tramite S/MIME è stato esportato da questa macchina e importato in un'altra macchina, attenersi alla seguente procedura per eliminare il certificato dalla macchina in cui è stato importato.

1 **Avviare la IU remota.**

2 **Fare clic su [Impostazioni/Registrazione] nella pagina del portale.**

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni certificato S/MIME].**

4 **Selezionare il certificato corrispondente ▶ fare clic su [Elimina] ▶ [OK].**

Passaggio 4: Abilitazione del nuovo certificato (per firme periferica)

Abilitare il certificato.

■Se un certificato per firma periferica è registrato su Acrobat

Se un certificato per firma periferica è registrato in Acrobat, esportare il certificato rigenerato per firma periferica e registrare il nuovo certificato in Acrobat.

Esportazione del certificato dalla macchina(P. 86)

■Se un certificato S/MIME esportato da questa macchina è stato importato in un'altra macchina

Se il certificato della chiave pubblica (certificato S/MIME) utilizzato per crittografare e-mail/I-fax tramite S/MIME è stato esportato da questa macchina e importato in un'altra macchina, esportare il certificato rigenerato e registrarlo sull'altra macchina.

Esportazione del certificato dalla macchina(P. 86)
Registrazione del certificato sull'altra macchina(P. 86)

■Esportazione del certificato dalla macchina

Attenersi alla seguente procedura per esportare il certificato.

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 Fare clic su [Gestione periferiche] ▶ [Esportazione firma periferica].

4 Fare clic su [Avvio esportazione] ▶ salvare il file in una posizione a scelta.

■Registrazione del certificato sull'altra macchina

Attenersi alla seguente procedura per registrare il certificato sull'altra macchina.

1 Avviare la IU remota.

2 Fare clic su [Impostazioni/Registrazione] nella pagina del portale.

3 **Fare clic su [Gestione periferiche] ▶ [Impostazioni certificato S/MIME].**

4 **Fare clic su [Registrazione certificato S/MIME].**

5 **Registrare il certificato S/MIME.**

- Fare clic su [Sfoglia...] ▶ specificare il file (certificato S/MIME) da registrare ▶ fare clic su [Registra].

Procedure aggiuntive per le impostazioni Bluetooth

Procedure aggiuntive per le impostazioni Bluetooth

La chiave per il Bluetooth viene aggiornata automaticamente in seguito all'aggiornamento del firmware della macchina. Se si utilizza l'applicazione Canon PRINT Business per dispositivi mobili, occorre registrare nuovamente la periferica.

Procedura per Bluetooth(P. 90)

Procedura per Bluetooth

Passaggio 1: Eliminazione della periferica registrata in Canon PRINT Business (per Bluetooth)

Se il Bluetooth è impostato su <On>, attenersi alla seguente procedura.

Operazione per iOS(P. 91)
Operazione per Android(P. 91)

■ Operazione per iOS

1 Toccare [ ] in alto a sinistra della schermata principale di Canon PRINT Business.

Viene visualizzata la schermata [Selez. stamp.].

2 Eliminare una periferica dall'elenco toccando [ ] ▶ [Elimina].

■ Operazione per Android

1 Toccare [ ] in alto a sinistra della schermata principale di Canon PRINT Business.

Viene visualizzata la schermata [Selez. stamp.].

2 Tenere premuto il nome della periferica ▶ toccare [Elimina] nella finestra di dialogo visualizzata.

Passaggio 2: Nuova registrazione della periferica in Canon PRINT Business (per Bluetooth)

Se il Bluetooth è impostato su <On>, attenersi alla seguente procedura.

Operazione per iOS(P. 92)
Operazione per Android(P. 92)

Operazione per iOS

1 Toccare [ ] in alto a sinistra della schermata principale di Canon PRINT Business.

Viene visualizzata la schermata [Selez. stamp.].

2 Toccare [Stampanti vicine].

Vengono visualizzate le periferiche rilevate.

Se non vengono rilevate periferiche

Avvicinarsi alla macchina e toccare [Cerca]. Il Bluetooth può rilevare periferiche a una distanza massima di 2 metri o 80 pollici.

3 Selezionare la periferica ▶ toccare [Aggiungi].

Operazione per Android

1 Toccare [ ] in alto a sinistra della schermata principale di Canon PRINT Business.

Viene visualizzata la schermata [Selez. stamp.].

2 Toccare [Stampanti vicine].

Vengono visualizzate le periferiche rilevate.

Se non vengono rilevate periferiche

Avvicinarsi alla macchina e toccare [Cerca]. Il Bluetooth può rilevare periferiche a una distanza massima di 2 metri o 80 pollici.

3 Selezionare la periferica.

4 Leggere le informazioni periferica nella finestra di dialogo visualizzata ▶ toccare [Aggiungi].

Se viene visualizzata la schermata delle impostazioni della rete Wi-Fi, seguire le istruzioni visualizzate sullo schermo.

Procedure aggiuntive per le impostazioni di Sistema di gestione degli accessi

Procedure aggiuntive per le impostazioni di Sistema di gestione degli accessi

La chiave per Sistema di gestione degli accessi viene aggiornata automaticamente in seguito all'aggiornamento del firmware della macchina.

Le informazioni sulle restrizioni vengono automaticamente recuperate di nuovo circa 30 minuti dopo l'aggiornamento automatico della chiave. La stampa può quindi essere eseguita normalmente con la funzione Sistema di gestione degli accessi.

Se si desidera stampare con la funzione Sistema di gestione degli accessi del driver della stampante subito dopo l'aggiornamento del firmware, è necessario recuperare di nuovo manualmente le informazioni sulle restrizioni di Sistema di gestione degli accessi.

Procedura per Sistema di gestione degli accessi(P. 95)

Se si tenta di stampare senza recuperare nuovamente le informazioni sulle restrizioni, si verifica un errore.

Procedura per Sistema di gestione degli accessi

Se si desidera stampare con la funzione Sistema di gestione degli accessi del driver della stampante subito dopo l'aggiornamento del firmware, è necessario recuperare manualmente le informazioni sulle restrizioni di Sistema di gestione degli accessi.

Per farlo, attenersi alla seguente procedura.

Trascorsi circa 30 minuti dall'aggiornamento del firmware, la procedura riportata di seguito non sarà più necessaria poiché a quel punto le informazioni sulle restrizioni saranno state recuperate automaticamente.

1 Accedere al computer.

2 Visualizzare le proprietà della stampante da utilizzare con il driver della stampante che ha la funzione Sistema di gestione degli accessi abilitata.

■Per Windows Vista

- Fare clic su [Start] ▶ [Pannello di controllo] ▶ [Hardware e suoni] ▶ selezionare [Stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà].

■Per Windows Server 2008

- Fare clic su [Start] ▶ [Pannello di controllo] ▶ [Hardware e suoni] ▶ selezionare [Stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà].

■Per Windows Server 2008 R2

- Fare clic su [Start] ▶ [Pannello di controllo] ▶ [Hardware] ▶ selezionare [Dispositivi e stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà stampante].

■Per Windows 7

- Fare clic su [Start] ▶ [Pannello di controllo] ▶ [Hardware e suoni] ▶ selezionare [Dispositivi e stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà stampante].

■Per Windows 8.1/Windows Server 2012

- Passare al desktop e visualizzare la barra degli accessi sul lato destro dello schermo.
- Fare clic su [Impostazioni] ▶ [Pannello di controllo] ▶ selezionare [Visualizza dispositivi e stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà stampante].

■Per Windows 10/Windows Server 2016

- Fare clic con il pulsante destro del mouse su [Start] ▶ selezionare [Pannello di controllo] ▶ [Visualizza dispositivi e stampanti].
- Fare clic con il pulsante destro del mouse sull'icona della stampante ▶ selezionare [Proprietà stampante].

3 Fare clic sulla scheda [AMS].

4 Fare clic su [Recupera informazioni sulle limitazioni].

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.