针对 RSA 密钥产生脆弱性的相关措施

USRM3-1251-02 2022-07 zh

目录

前言

前言

必须更新固件并执行本文档中描述的附加步骤，以升级使用易受攻击的加密库创建的 RSA 密钥。

首先，检查您的机器型号和版本。
如果在此页上找到您的机器型号和版本，请更新固件，然后执行本文档中描述的附加步骤。 **检查是否必须执行附加程序 (P. 5)**
有关更新固件的信息，请访问从中获得本文档的网站。

检查本机的版本

按照以下步骤检查本机的版本。

1 **启动远程用户界面。**

2 **单击门户页面上的[状态确认/取消]。**

3 **单击[设备信息] ▶ 检查[版本信息]中的[控制器]。**

需要执行附加步骤的型号和版本

型号	版本
- 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	版本 59.39 至版本 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	版本 29.39 至版本 37.30
- iR-ADV 4725 / 4735 / 4745 - iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B - iR-ADV C3730 / C3720	版本 17.44 至版本 27.30

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

注释

- 根据您的机器型号，本文档中使用的屏幕截图可能与您实际看到的有所不同。有关屏幕截图的详细信息，请参阅在线手册网站上的相关机器手册。

  https://oip.manual.canon/

检查是否必须执行附加程序

检查是否必须执行附加程序

执行以下三项操作，检查是否必须执行附加程序。
根据机器型号的不同，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面操作。

检查 RSA 密钥(P. 5)
检查蓝牙设置(P. 7)
检查 Access Management System 设置(P. 8)
如果已在本机中注册的密钥显示“Default Key”或“AMS”，则不需要检查 RSA 密钥。请检查蓝牙设置和 Access Management System 设置，然后根据需要执行附加程序。

注释

- 本文档中使用的屏幕截图仅为示例。根据您的机器型号，它们可能与您实际看到的有所不同。

检查 RSA 密钥

检查是否存在 RSA 密钥。如果存在本机生成的 RSA 密钥，请检查密钥用途。

使用控制面板(P. 5)
使用远程用户界面时(P. 6)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <密钥和证书列表>。**

3 **按下 <本设备的密钥和证书列表>。**

- 除非在本机上启用了用户签名功能，否则不会显示<本设备的密钥和证书列表>。在这种情况下，请继续执行下一步。

4 **选择<Default Key>和<AMS>以外的密钥（<状态>显示<使用>） ▶ 按<证书详细说明>。**

示例屏幕：

5 检查<公钥>。

示例屏幕：

对于 RSA 以外的证书

不需要执行附加步骤。按<确定>以关闭屏幕。

对于 RSA 证书

前进到步骤 6。

- 不需要对以下密钥执行附加步骤。按<确定>以关闭屏幕。
  - 已外部生成并注册到本机的 RSA 密钥
- 如果必须执行附加步骤，则可能需要证书信息来禁用证书。请在删除密钥/证书前记录所需的信息。向颁发证书的证书颁发机构询问所需的信息。

6 按<显示使用位置> ▶ 检查密钥用途。

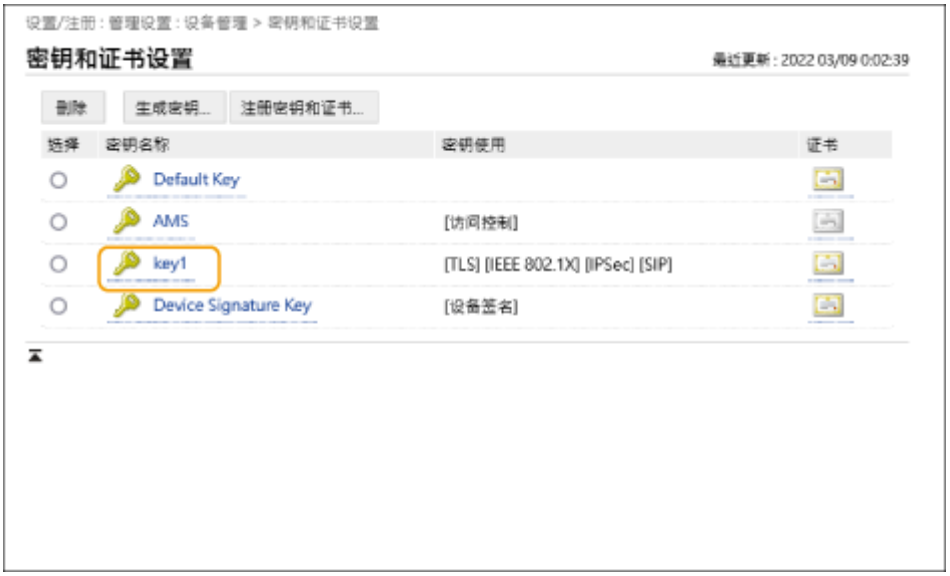
示例屏幕：

根据此处显示的内容执行附加步骤。 **RSA 密钥用途和附加步骤(P. 11)**

■使用远程用户界面时

1 启动远程用户界面 ▶ 单击[设置/注册] ▶ [设备管理] ▶ [密钥和证书设置]。

2 单击[Default Key]和[AMS]以外的密钥。



3 检查[公钥]。

对于 RSA 以外的证书

不需要执行附加步骤。

对于 RSA 证书

单击屏幕顶部的[密钥和证书设置] ▶ 检查密钥用途。

- 根据此处显示的内容执行附加步骤。 **RSA 密钥用途和附加步骤(P. 11)**
- 不需要对以下密钥执行附加步骤。
  - 已外部生成并注册到本机的 RSA 密钥
- 如果必须执行附加步骤，则可能需要证书信息来禁用证书。请在删除密钥/证书前记录所需的信息。向颁发证书的证书颁发机构询问所需的信息。

检查蓝牙设置

检查蓝牙是否设置为<打开>。如果其设置为<打开>，则必须执行附加步骤。

使用控制面板(P. 8)
使用远程用户界面时(P. 8)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <蓝牙设置>。**

3 **检查<使用蓝牙>。**

- 如果<使用蓝牙>设置为<打开>，则执行后续步骤。 **适用于蓝牙设置的附加步骤(P. 84)**
- 如果<使用蓝牙>设置为<关闭>，则不需要执行后续步骤。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络] ▶ [蓝牙设置]。**

4 **检查[使用蓝牙]。**

- 如果选择[使用蓝牙]设置，则执行后续步骤。 **适用于蓝牙设置的附加步骤(P. 84)**
- 如果取消选择[使用蓝牙]，则不需要执行后续步骤。

检查 Access Management System 设置

检查 Access Management System 是否设置为<打开>。如果其设置为<打开>，则必须执行附加步骤。

根据您的机器，可能不会显示此设置。在这种情况下，不需要执行附加步骤。

使用控制面板(P. 8)
使用远程用户界面时(P. 9)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <授权/其他> ▶ <使用 ACCESS MANAGEMENT SYSTEM>。**

3 检查<使用 ACCESS MANAGEMENT SYSTEM>。

- 如果<使用 ACCESS MANAGEMENT SYSTEM>设置为<打开>，则执行后续步骤。 **适用于 Access Management System 设置的附加步骤(P. 89)**
- 如果<使用 ACCESS MANAGEMENT SYSTEM>设置为<关闭>，则不需要执行后续步骤。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[授权/其他] ▶ [ACCESS MANAGEMENT SYSTEM 设置]。

4 检查[使用 ACCESS MANAGEMENT SYSTEM]。

- 如果选择[使用 ACCESS MANAGEMENT SYSTEM]设置，则执行后续步骤。 **适用于 Access Management System 设置的附加步骤(P. 89)**
- 如果取消选择[使用 ACCESS MANAGEMENT SYSTEM]，则不需要执行后续步骤。

RSA 密钥用途和附加步骤

RSA 密钥用途和附加步骤

请参阅“附加步骤”并根据密钥用途执行相应的步骤。

RSA 密钥用途	条件	附加步骤
TLS	在任何情况下都必须执行附加步骤。	**适用于 TLS 的步骤(P. 12)**
IEEE 802.1X	如果 IEEE 802.1X 认证方法设置为 EAP-TLS，则必须执行附加步骤。	**适用于 IEEE 802.1X 步骤(P. 26)**
IPSec	如果 IKE 认证方法设置为数字签名方法，则必须执行附加步骤。	**适用于 IPSec 的步骤(P. 43)**
SIP	如果使用 TLS，则必须执行附加步骤。	**适用于 SIP 的步骤(P. 59)**
设备签名	在下列情况下必须执行附加步骤： • 当使用设备签名的密钥将数字签名添加到已发送文件时 • 当在 S/MIME 加密设置中启用加密时	**适用于设备签名的步骤(P. 76)**

注释

- 本文档中使用的屏幕截图仅为示例。根据您的机器型号，它们可能与您实际看到的有所不同。

适用于 TLS 的步骤

步骤 1：重新生成密钥和证书(TLS)

可以为使用本机生成的密钥生成三种类型的证书：自签名证书、CSR 证书和 SCEP 证书。根据证书类型的不同，相关步骤也不同。
根据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

对于自签名证书(P. 13)
对于 CSR 证书(P. 16)
对于 SCEP 证书(P. 18)

对于自签名证书

使用控制面板(P. 13)
使用远程用户界面时(P. 14)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <生成密钥> ▶ <生成网络通信密钥>。**

3 **配置所需的设置，然后转到下一个屏幕。**

示例屏幕：

a <密钥名称>

输入密钥名称。输入易于在列表中找到的名称。

b <签名算法>

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。等于或大于 1024 位的密钥长度可以支持 SHA384 和 SHA512 哈希算法。如果 c 选择为<RSA>，且 d 中的<密钥长度(bit)>设置为<1024>或更大，则可以选择 SHA384 和 SHA512 哈希算法。

c <密钥算法>

选择密钥算法。如果选择<RSA>，则<密钥长度(bit)>会显示为 d 的设置项目。如果选择<ECDSA>，则会显示<密钥类型>。

d <密钥长度(bit)>/<密钥类型>

如果对于 c 选择<RSA>，则指定密钥长度，如果选择<ECDSA>，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

4 为证书配置必要的项目 ▶ 按<生成密钥>。

示例屏幕：

a <有效期开始日期>/<有效期结束日期>

输入证书有效期的开始日期和结束日期。

b <国家名称/地区名称>/<省区>/<城市>/<组织>/<组织单位>

从列表中选择国家代码，然后输入位置和组织名称。

c <通用名称>

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 单击[生成密钥]。

5 单击[网络通信]。

6 配置密钥和证书设置。

a [密钥名称]

使用字母数字字符输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。1024 位或更长的密钥长度可以支持 SHA384 和 SHA512 哈希算法。

c [密钥算法]

选择[RSA]或[ECDSA]作为密钥生成算法。如果选择[RSA]，请指定密钥长度；或者如果选择[ECDSA]，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

注释:

- 如果选择[SHA384]或[SHA512]作为[签名算法]，则在选择[RSA]作为[密钥算法]时无法将密钥长度设置为[512 bit]。

d [有效期开始日期(YYYY/MM/DD)]/[有效期结束日期(YYYY/MM/DD)]

输入证书有效期的开始日期和结束日期。[有效期结束日期(YYYY/MM/DD)]无法设为[有效期开始日期(YYYY/MM/DD)]中的日期之前的日期。

e [国家名称/地区名称]

单击[选择国家名称/地区名称]，然后从下拉列表中选择国家/地区。还可单击[输入互联网国家代码]并输入国家/地区代码，如将美国输入为“US”。

f [省区]/[城市]

根据需要使用字母数字字符输入位置。

g [组织]/[组织单位]

根据需要使用字母数字字符输入组织名称。

h [通用名称]

根据需要使用字母数字字符输入证书的通用名称。“通用名称”通常简写为“CN”。

7 单击[确定]。

- 生成密钥和证书需要一些时间。
- 生成的密钥和证书会自动注册到本机。

对于 CSR 证书

在本机上生成密钥和证书。使用屏幕上显示的 CSR 数据或输出到文件来请求证书颁发机构颁发证书。然后为密钥注册所颁发的证书。
只能从远程用户界面配置此设置。

■1. 生成密钥和 CSR

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **单击[生成密钥]。**

5 **单击[密钥和证书签名请求(CSR)]。**

6 **配置密钥和证书设置。**

a [密钥名称]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。

c [密钥算法]

选择密钥算法，并在选择[RSA]时指定密钥长度，或在选择[ECDSA]时指定密钥类型。

d [国家名称/地区名称]

从列表中选择国家代码，或直接输入。

e [省区]/[城市]

输入位置。

f [组织]/[组织单位]

输入组织名称。

g [通用名称]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

7 单击[确定]。

➡ 随即显示 CSR 数据。

- 如果要将 CSR 数据保存到文件，单击[存储到文件中]并指定保存位置。

注释:

- 生成 CSR 的密钥会显示在密钥和证书列表屏幕上，但无法单独使用。要使用此密钥，需要注册之后根据 CSR 颁发的证书。

8 请求证书颁发机构根据 CSR 数据颁发证书。

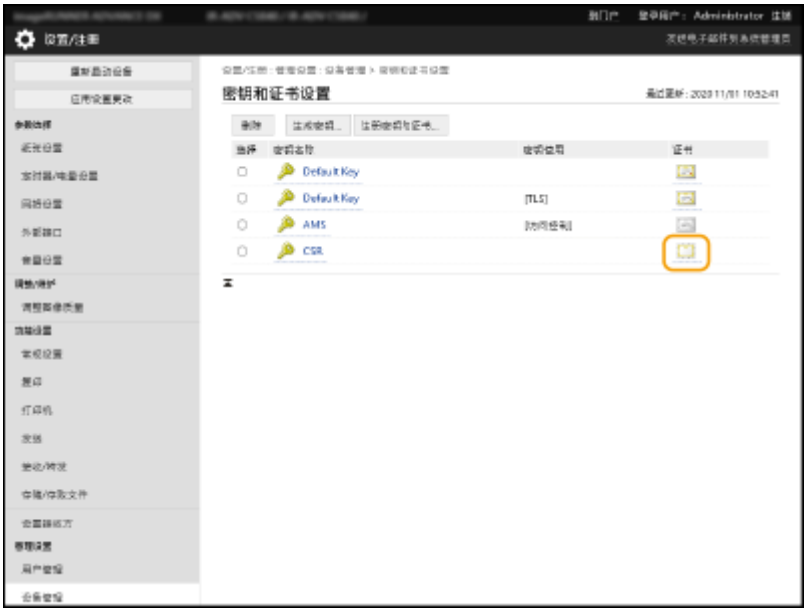
■2. 将颁发的证书注册的密钥

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 在[证书]列表中，针对要注册的证书单击 。



5 **单击[注册证书...]。**

6 **注册证书。**

- 单击[浏览...] ▶ 指定要注册的文件（证书） ▶ 单击[注册]。

对于 SCEP 证书

手动请求 SCEP 服务器颁发证书。
只能从远程用户界面配置此设置。

注释

- 如果选择[启用证书自动颁发请求定时器]，则无法发送颁发证书的手动请求。如果其被选中，请取消选择。

启动“远程用户界面” ▶ 单击[设置/注册] ▶ [设备管理] ▶ [证书颁发请求的设置(SCEP)] ▶ [证书自动颁发请求设置] ▶ 取消选择[启用证书自动颁发请求定时器] ▶ 单击[更新]。

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [证书颁发请求的设置(SCEP)]。**

4 **单击[证书颁发请求]。**

5 **设置请求证书所需的项目。**

a [密钥名称:]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法:]

选择用于签名的哈希算法。

c [密钥长度(bit):]

选择密钥长度。

d [组织:]

输入组织名称。

e [通用名称:]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

f [质询密码:]

在 SCEP 服务器端设置密码时，请输入请求数据 (PKCS#9) 中包含的质询密码，以请求颁发证书。

g [密钥使用位置:]

选择[TLS]。

注释:

- 如果选择[无]以外的选项，请事先启用每个功能。如果在禁用每个功能的情况下成功获得证书，证书将指定为密钥使用位置，但不会自动启用每个功能。

6 单击[发送请求]。

7 单击[重新启动]。

步骤 2：重置密钥和证书(TLS)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。
对于 SCEP 证书，不需要此步骤。

对于自签名证书/CSR 证书

使用控制面板(P. 20)
使用远程用户界面时(P. 21)

■使用控制面板

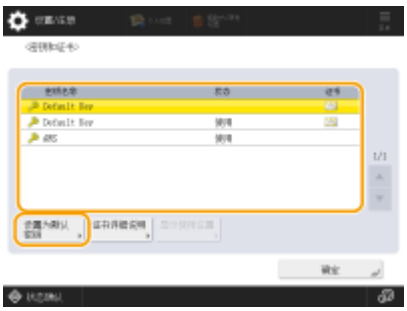
1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <TLS 设置>。**

3 **按下 <密钥和证书>。**

4 **选择要用于 TLS 加密通信的密钥和证书 ▶ 按<设置为默认密钥> ▶ <是>。**

示例屏幕：



- 如果要使用预装的密钥和证书，请选择<Default Key>。

注释:

- TLS 加密通信无法使用<Device Signature Key>（用于设备签名），也无法使用<AMS>（用于访问限制）。

5 **按下 <确定>。**

6 **按 (设置/注册) ▶ <应用设置更改> ▶ <是>。**

➠ 重新启动本机后设置才会应用。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络] ▶ [TLS 设置]。**

4 **单击[密钥和证书]。**

5 **为要用于 TLS 加密通信的密钥和证书点击[使用]。**

- 如果要使用预装的密钥和证书，请选择[Default Key]。

6 **单击[应用设置更改]重新启动本机。**

➠ 重新启动本机后设置才会应用。

步骤 3：删除过去生成的密钥/证书(TLS)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

注释

- 禁用证书时，可能需要向证书颁发机构传递信息。删除密钥/证书前，请参阅 **检查是否必须执行附加程序(P. 5)** ，并记下所需的信息。

使用控制面板(P. 22)
使用远程用户界面时(P. 22)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <密钥和证书列表> ▶ <本设备的密钥和证书列表>。**

- 除非在本机上启用了用户签名功能，否则不会显示<本设备的密钥和证书列表>。在这种情况下，请继续执行下一步。

3 **选择密钥和证书 ▶ 按下<删除> ▶ <是>。**

示例屏幕：

注释:

- 如果显示 ，则密钥损坏或无效。
- 如果没有显示 ，则密钥的证书不存在。
- 如果选择密钥和证书并按<证书详细说明>，则显示证书详细信息。也可以按此屏幕上的<验证证书>以检查证书是否有效。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **选择密钥和证书 ▶ 单击[删除] ▶ [确定]。**

注释

- 如果显示 ，则密钥损坏或无效。
- 如果显示 ，则表示密钥的证书不存在。
- 单击密钥名称可以显示证书详细信息。也可以在此屏幕上单击[校验证书]检查证书是否有效。

步骤 4：禁用证书(TLS)

禁用过去生成的证书。根据证书类型的不同，相关步骤也不同。

■对于自签名证书

如果在计算机或 Web 浏览器中将包含需要附加步骤的密钥的证书注册为可信证书，请删除已注册的证书。

■对于 CSR/SCEP 证书

请求已颁发证书的证书颁发机构吊销证书。对于要请求的证书颁发机构，请参阅证书中的[发行者]。

注释

- 如果在与本机通信的计算机或 Web 浏览器中使用 CRL 检查证书吊销情况，请在吊销证书后将更新的 CRL 注册到计算机或 Web 浏览器中。
- 如果使用 CRL 以外的方法（例如 OCSP）来检查证书吊销情况，请执行该方法的相关步骤。

步骤 5：启用新证书(TLS)

启用在本机上新生成的证书。

■对于自签名证书

将新证书作为可信证书注册到计算机或 Web 浏览器中。

■对于 CSR/SCEP 证书

不需要执行附加步骤。

适用于 IEEE 802.1X 步骤

步骤 1：检查认证方法(IEEE 802.1X)

如果 IEEE 802.1X 认证方法设置为 EAP-TLS，则必须执行后续步骤。
按照以下步骤检查认证方法。
据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

使用控制面板(P. 27)
使用远程用户界面时(P. 27)

■使用控制面板

1 按 (设置/注册)。

2 按<参数选择> ▶ <网络> ▶ <IEEE 802.1X 设置>。

3 按<下一步> ▶ 检查<使用 TLS>。

示例屏幕：

- 如果<使用 TLS>设置为<打开>且<密钥和证书>显示密钥名称，则执行后续步骤。
- 如果<使用 TLS>设置为<关闭>，则不需要执行后续步骤。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[网络] ▶ [IEEE 802.1X 设置]。

4 检查[使用 TLS]。

- 如果选择[使用 TLS]并显示密钥名称，则执行后续步骤。
- 如果取消选择[使用 TLS]，则不需要执行后续步骤。

步骤 2：重新生成密钥和证书(IEEE 802.1X)

可以为使用本机生成的密钥生成三种类型的证书：自签名证书、CSR 证书和 SCEP 证书。根据证书类型的不同，相关步骤也不同。
根据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

对于自签名证书(P. 29)
对于 CSR 证书(P. 32)
对于 SCEP 证书(P. 34)

对于自签名证书

使用控制面板(P. 29)
使用远程用户界面时(P. 30)

■使用控制面板

1 按 (设置/注册)。

2 按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <生成密钥> ▶ <生成网络通信密钥>。

3 配置所需的设置，然后转到下一个屏幕。

示例屏幕：

a <密钥名称>

输入密钥名称。输入易于在列表中找到的名称。

b <签名算法>

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。等于或大于 1024 位的密钥长度可以支持 SHA384 和 SHA512 哈希算法。如果 c 选择为<RSA>，且 d 中的<密钥长度(bit)>设置为<1024>或更大，则可以选择 SHA384 和 SHA512 哈希算法。

c <密钥算法>

选择密钥算法。如果选择<RSA>，则<密钥长度(bit)>会显示为 d 的设置项目。如果选择<ECDSA>，则会显示<密钥类型>。

d <密钥长度(bit)>/<密钥类型>

如果对于 c 选择<RSA>，则指定密钥长度，如果选择<ECDSA>，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

4 为证书配置必要的项目 ▶ 按<生成密钥>。

示例屏幕：

a <有效期开始日期>/<有效期结束日期>

输入证书有效期的开始日期和结束日期。

b <国家名称/地区名称>/<省区>/<城市>/<组织>/<组织单位>

从列表中选择国家代码，然后输入位置和组织名称。

c <通用名称>

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 单击[生成密钥]。

5 单击[网络通信]。

6 配置密钥和证书设置。

a [密钥名称]

使用字母数字字符输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。1024 位或更长的密钥长度可以支持 SHA384 和 SHA512 哈希算法。

c [密钥算法]

选择[RSA]或[ECDSA]作为密钥生成算法。如果选择[RSA]，请指定密钥长度；或者如果选择[ECDSA]，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

注释:

- 如果选择[SHA384]或[SHA512]作为[签名算法]，则在选择[RSA]作为[密钥算法]时无法将密钥长度设置为[512 bit]。

d [有效期开始日期(YYYY/MM/DD)]/[有效期结束日期(YYYY/MM/DD)]

输入证书有效期的开始日期和结束日期。[有效期结束日期(YYYY/MM/DD)]无法设为[有效期开始日期(YYYY/MM/DD)]中的日期之前的日期。

e [国家名称/地区名称]

单击[选择国家名称/地区名称]，然后从下拉列表中选择国家/地区。还可单击[输入互联网国家代码]并输入国家/地区代码，如将美国输入为“US”。

f [省区]/[城市]

根据需要使用字母数字字符输入位置。

g [组织]/[组织单位]

根据需要使用字母数字字符输入组织名称。

h [通用名称]

根据需要使用字母数字字符输入证书的通用名称。“通用名称”通常简写为“CN”。

7 单击[确定]。

- 生成密钥和证书需要一些时间。
- 生成的密钥和证书会自动注册到本机。

对于 CSR 证书

在本机上生成密钥和证书。使用屏幕上显示的 CSR 数据或输出到文件来请求证书颁发机构颁发证书。然后为密钥注册所颁发的证书。
只能从远程用户界面配置此设置。

■1. 生成密钥和 CSR

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **单击[生成密钥]。**

5 **单击[密钥和证书签名请求(CSR)]。**

6 **配置密钥和证书设置。**

a [密钥名称]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。

c [密钥算法]

选择密钥算法，并在选择[RSA]时指定密钥长度，或在选择[ECDSA]时指定密钥类型。

d [国家名称/地区名称]

从列表中选择国家代码，或直接输入。

e [省区]/[城市]

输入位置。

f [组织]/[组织单位]

输入组织名称。

g [通用名称]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

7 单击[确定]。

➡ 随即显示 CSR 数据。

- 如果要将 CSR 数据保存到文件，单击[存储到文件中]并指定保存位置。

注释:

- 生成 CSR 的密钥会显示在密钥和证书列表屏幕上，但无法单独使用。要使用此密钥，需要注册之后根据 CSR 颁发的证书。

8 请求证书颁发机构根据 CSR 数据颁发证书。

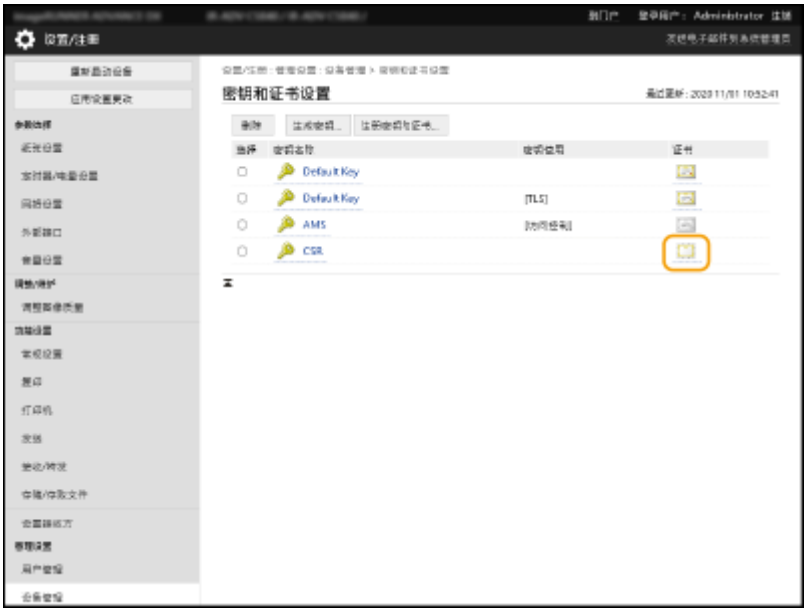
■2. 将颁发的证书注册的密钥

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 在[证书]列表中，针对要注册的证书单击 。



5 **单击[注册证书...]。**

6 **注册证书。**

- 单击[浏览...] ▶ 指定要注册的文件（证书） ▶ 单击[注册]。

对于 SCEP 证书

手动请求 SCEP 服务器颁发证书。
只能从远程用户界面配置此设置。

注释

- 如果选择[启用证书自动颁发请求定时器]，则无法发送颁发证书的手动请求。如果其被选中，请取消选择。

启动“远程用户界面” ▶ 单击[设置/注册] ▶ [设备管理] ▶ [证书颁发请求的设置(SCEP)] ▶ [证书自动颁发请求设置] ▶ 取消选择[启用证书自动颁发请求定时器] ▶ 单击[更新]。

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [证书颁发请求的设置(SCEP)]。**

4 **单击[证书颁发请求]。**

5 **设置请求证书所需的项目。**

a [密钥名称:]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法:]

选择用于签名的哈希算法。

c [密钥长度(bit):]

选择密钥长度。

d [组织:]

输入组织名称。

e [通用名称:]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

f [质询密码:]

在 SCEP 服务器端设置密码时，请输入请求数据 (PKCS#9) 中包含的质询密码，以请求颁发证书。

g [密钥使用位置:]

选择[IEEE 802.1X]。

注释:

- 如果选择[无]以外的选项，请事先启用每个功能。如果在禁用每个功能的情况下成功获得证书，证书将指定为密钥使用位置，但不会自动启用每个功能。

6 单击[发送请求]。

7 单击[重新启动]。

步骤 3：重置密钥和证书(IEEE 802.1X)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。
对于 SCEP 证书，不需要此步骤。

对于自签名证书/CSR 证书

使用控制面板(P. 36)
使用远程用户界面时(P. 37)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <IEEE 802.1X 设置>。**

3 **对于<使用 IEEE 802.1X>按<打开> ▶ 配置所需的设置 ▶ 按<下一步>。**

示例屏幕：

a <登录名称>

输入登录用户的名称(EAP 登录名)以接收 IEEE 802.1X 认证。

b <验证认证服务器证书>

验证认证服务器发送的服务器证书时，将此设置设为<打开>。

c <验证认证服务器名>

要验证服务器证书中的通用名称，请选择<打开>。然后在<认证服务器名>中输入登录用户所注册的认证服务器的名称。

4 **按<使用 TLS>的<打开> ▶ 按<密钥和证书>。**

5 **在列表中选择要使用的密钥和证书 ▶ 按<设置为默认密钥> ▶ <是>。**

6 **按下 <确定>。**

7 **按 (设置/注册) ▶ (设置/注册) ▶ <应用设置更改> ▶ <是>。**

➠ 重新启动本机后设置才会应用。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络设置] ▶ [IEEE 802.1X 设置]。**

4 **选择[使用 IEEE 802.1X] ▶ 配置所需的设置。**

a [登录名称]

输入登录用户的名称(EAP 登录名)以接收 IEEE 802.1X 认证。

b [验证认证服务器证书]

验证认证服务器发送的服务器证书时，需选中此复选框。

c [验证认证服务器名]

要验证服务器证书中的通用名称，请选中此复选框。然后在[认证服务器名]中输入登录用户所注册的认证服务器的名称。

5 **选择[使用 TLS] ▶ 单击[密钥和证书]。**

6 **在列表中将为使用的密钥点击[使用]。**

7 **单击[确定]。**

8 **单击[应用设置更改]重新启动本机。**

➠ 重新启动本机后设置才会应用。

步骤 4：删除过去生成的密钥/证书(IEEE 802.1X)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

注释

- 禁用证书时，可能需要向证书颁发机构传递信息。删除密钥/证书前，请参阅 **检查是否必须执行附加程序(P. 5)** ，并记下所需的信息。

使用控制面板(P. 39)
使用远程用户界面时(P. 39)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <密钥和证书列表> ▶ <本设备的密钥和证书列表>。**

- 除非在本机上启用了用户签名功能，否则不会显示<本设备的密钥和证书列表>。在这种情况下，请继续执行下一步。

3 **选择密钥和证书 ▶ 按下<删除> ▶ <是>。**

示例屏幕：

注释:

- 如果显示 ，则密钥损坏或无效。
- 如果没有显示 ，则密钥的证书不存在。
- 如果选择密钥和证书并按<证书详细说明>，则显示证书详细信息。也可以按此屏幕上的<验证证书>以检查证书是否有效。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **选择密钥和证书 ▶ 单击[删除] ▶ [确定]。**

注释

- 如果显示 ，则密钥损坏或无效。
- 如果显示 ，则表示密钥的证书不存在。
- 单击密钥名称可以显示证书详细信息。也可以在此屏幕上单击[校验证书]检查证书是否有效。

步骤 5：禁用证书(IEEE 802.1X)

禁用过去生成的证书。根据证书类型的不同，相关步骤也不同。

■对于自签名证书

如果将包含需要附加步骤的密钥的证书作为可信证书注册到 IEEE 802.1X 认证服务器，请删除已注册的证书。

■对于 CSR/SCEP 证书

请求已颁发证书的证书颁发机构吊销证书。对于要请求的证书颁发机构，请参阅证书中的[发行者]。

注释

- 如果在 IEEE 802.1X 认证服务器中使用 CRL 检查证书吊销情况，请在吊销证书后将更新的 CRL 注册到计算机或 Web 浏览器中。
- 如果使用 CRL 以外的方法（例如 OCSP）来检查证书吊销情况，请执行该方法的相关步骤。

步骤 6：启用新证书(IEEE 802.1X)

启用证书。

■对于自签名证书

将新证书作为可信证书注册到 IEEE 802.1X 认证服务器中。

■对于 CSR/SCEP 证书

不需要执行附加步骤。

适用于 IPSec 的步骤

步骤 1：检查认证方法(IPSec)

如果 IPSec 中 IKE 设置的认证方法设置为<数字签名方法>，则必须执行后续步骤。
按照以下步骤检查认证方法。
据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

使用控制面板(P. 44)
使用远程用户界面时(P. 45)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <IPSec 设置>。**

3 **选择已注册的策略 ▶ 按<编辑> ▶ <IKE 设置>。**

示例屏幕：

4 **按<下一步> ▶ 检查<认证方法>。**

示例屏幕：

- 如果<认证方法>设置为<数字签名方法>且<密钥和证书>显示密钥名称，则执行后续步骤。
- 如果<认证方法>设置为<预共享密钥方法>，则不需要执行后续步骤。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络设置] ▶ [IPSec 策略列表]。**

4 **单击列表中的策略 ▶ 单击[IKE 设置]。**

5 **检查[认证方法]。**

- 如果[认证方法]设置为[数字签名方法]且显示密钥名称，则执行后续步骤。
- 如果<认证方法>设置为<预共享密钥方法>，则不需要执行后续步骤。

步骤 2：重新生成密钥和证书(IPSec)

可以为使用本机生成的密钥生成三种类型的证书：自签名证书、CSR 证书和 SCEP 证书。根据证书类型的不同，相关步骤也不同。
根据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

对于自签名证书(P. 46)
对于 CSR 证书(P. 49)
对于 SCEP 证书(P. 51)

对于自签名证书

使用控制面板(P. 46)
使用远程用户界面时(P. 47)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <生成密钥> ▶ <生成网络通信密钥>。**

3 **配置所需的设置，然后转到下一个屏幕。**

示例屏幕：

a <密钥名称>

输入密钥名称。输入易于在列表中找到的名称。

b <签名算法>

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。等于或大于 1024 位的密钥长度可以支持 SHA384 和 SHA512 哈希算法。如果 c 选择为<RSA>，且 d 中的<密钥长度(bit)>设置为<1024>或更大，则可以选择 SHA384 和 SHA512 哈希算法。

c <密钥算法>

选择密钥算法。如果选择<RSA>，则<密钥长度(bit)>会显示为 d 的设置项目。如果选择<ECDSA>，则会显示<密钥类型>。

d <密钥长度(bit)>/<密钥类型>

如果对于 c 选择<RSA>，则指定密钥长度，如果选择<ECDSA>，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

4 为证书配置必要的项目 ▶ 按<生成密钥>。

示例屏幕：

a <有效期开始日期>/<有效期结束日期>

输入证书有效期的开始日期和结束日期。

b <国家名称/地区名称>/<省区>/<城市>/<组织>/<组织单位>

从列表中选择国家代码，然后输入位置和组织名称。

c <通用名称>

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 单击[生成密钥]。

5 单击[网络通信]。

6 配置密钥和证书设置。

a [密钥名称]

使用字母数字字符输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。1024 位或更长的密钥长度可以支持 SHA384 和 SHA512 哈希算法。

c [密钥算法]

选择[RSA]或[ECDSA]作为密钥生成算法。如果选择[RSA]，请指定密钥长度；或者如果选择[ECDSA]，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

注释:

- 如果选择[SHA384]或[SHA512]作为[签名算法]，则在选择[RSA]作为[密钥算法]时无法将密钥长度设置为[512 bit]。

d [有效期开始日期(YYYY/MM/DD)]/[有效期结束日期(YYYY/MM/DD)]

输入证书有效期的开始日期和结束日期。[有效期结束日期(YYYY/MM/DD)]无法设为[有效期开始日期(YYYY/MM/DD)]中的日期之前的日期。

e [国家名称/地区名称]

单击[选择国家名称/地区名称]，然后从下拉列表中选择国家/地区。还可单击[输入互联网国家代码]并输入国家/地区代码，如将美国输入为“US”。

f [省区]/[城市]

根据需要使用字母数字字符输入位置。

g [组织]/[组织单位]

根据需要使用字母数字字符输入组织名称。

h [通用名称]

根据需要使用字母数字字符输入证书的通用名称。“通用名称”通常简写为“CN”。

7 单击[确定]。

- 生成密钥和证书需要一些时间。
- 生成的密钥和证书会自动注册到本机。

对于 CSR 证书

在本机上生成密钥和证书。使用屏幕上显示的 CSR 数据或输出到文件来请求证书颁发机构颁发证书。然后为密钥注册所颁发的证书。
只能从远程用户界面配置此设置。

■1. 生成密钥和 CSR

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **单击[生成密钥]。**

5 **单击[密钥和证书签名请求(CSR)]。**

6 **配置密钥和证书设置。**

a [密钥名称]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。

[密钥算法]

选择密钥算法，并在选择[RSA]时指定密钥长度，或在选择[ECDSA]时指定密钥类型。

[国家名称/地区名称]

从列表中选择国家代码，或直接输入。

[省区]/[城市]

输入位置。

[组织]/[组织单位]

输入组织名称。

[通用名称]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

7 单击[确定]。

➡ 随即显示 CSR 数据。

- 如果要将 CSR 数据保存到文件，单击[存储到文件中]并指定保存位置。

注释:

- 生成 CSR 的密钥会显示在密钥和证书列表屏幕上，但无法单独使用。要使用此密钥，需要注册之后根据 CSR 颁发的证书。

8 请求证书颁发机构根据 CSR 数据颁发证书。

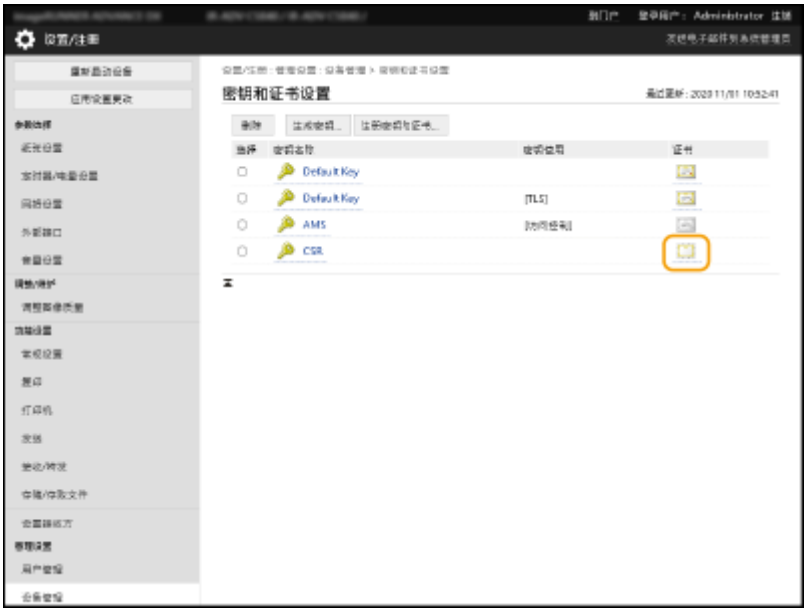
■2. 将颁发的证书注册的密钥

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 在[证书]列表中，针对要注册的证书单击 。



5 **单击[注册证书...]。**

6 **注册证书。**

- 单击[浏览...] ▶ 指定要注册的文件（证书） ▶ 单击[注册]。

对于 SCEP 证书

手动请求 SCEP 服务器颁发证书。
只能从远程用户界面配置此设置。

注释

- 如果选择[启用证书自动颁发请求定时器]，则无法发送颁发证书的手动请求。如果其被选中，请取消选择。

启动“远程用户界面” ▶ 单击[设置/注册] ▶ [设备管理] ▶ [证书颁发请求的设置(SCEP)] ▶ [证书自动颁发请求设置] ▶ 取消选择[启用证书自动颁发请求定时器] ▶ 单击[更新]。

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [证书颁发请求的设置(SCEP)]。**

4 **单击[证书颁发请求]。**

5 **设置请求证书所需的项目。**

a [密钥名称:]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法:]

选择用于签名的哈希算法。

c [密钥长度(bit):]

选择密钥长度。

d [组织:]

输入组织名称。

e [通用名称:]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

f [质询密码:]

在 SCEP 服务器端设置密码时，请输入请求数据 (PKCS#9) 中包含的质询密码，以请求颁发证书。

g [密钥使用位置:]

选择[IPSec]。

注释:

- 如果选择[无]以外的选项，请事先启用每个功能。如果在禁用每个功能的情况下成功获得证书，证书将指定为密钥使用位置，但不会自动启用每个功能。

6 单击[发送请求]。

7 单击[重新启动]。

步骤 3：重置密钥和证书(IPSec)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。
对于 SCEP 证书，不需要此步骤。

对于自签名证书/CSR 证书

使用控制面板(P. 53)
使用远程用户界面时(P. 54)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <IPSec 设置>。**

3 **选择要重置密钥和证书的策略 ▶ 按<编辑> ▶ <IKE 设置>。**

示例屏幕：

4 **按<下一步> ▶ 在<认证方法>中选择<数字签名方法> ▶ 按<密钥和证书>。**

示例屏幕：

5 **在列表中选择要使用的密钥和证书 ▶ 按<设置为默认密钥> ▶ <是>。**

6 **按下 <确定>。**

7 **按 (设置/注册) ▶ (设置/注册) ▶ <应用设置更改> ▶ <是>。**

➠ 重新启动本机后设置才会应用。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络设置] ▶ [IPSec 策略列表]。**

4 **在列表中单击要重置密钥和证书的策略 ▶ 单击[IKE 设置]。**

5 **在[认证方法]中选择[数字签名方法] ▶ 单击[密钥和证书]。**

6 **在列表中将为使用的密钥点击[使用]。**

7 **单击[确定]。**

8 **单击[应用设置更改]重新启动本机。**

➠ 重新启动本机后设置才会应用。

步骤 4：删除过去生成的密钥/证书(IPSec)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

注释

- 禁用证书时，可能需要向证书颁发机构传递信息。删除密钥/证书前，请参阅 **检查是否必须执行附加程序(P. 5)** ，并记下所需的信息。

使用控制面板(P. 55)
使用远程用户界面时(P. 55)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <密钥和证书列表> ▶ <本设备的密钥和证书列表>。**

- 除非在本机上启用了用户签名功能，否则不会显示<本设备的密钥和证书列表>。在这种情况下，请继续执行下一步。

3 **选择密钥和证书 ▶ 按下<删除> ▶ <是>。**

示例屏幕：

注释:

- 如果显示 ，则密钥损坏或无效。
- 如果没有显示 ，则密钥的证书不存在。
- 如果选择密钥和证书并按<证书详细说明>，则显示证书详细信息。也可以按此屏幕上的<验证证书>以检查证书是否有效。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **选择密钥和证书 ▶ 单击[删除] ▶ [确定]。**

注释

- 如果显示 ，则密钥损坏或无效。
- 如果显示 ，则表示密钥的证书不存在。
- 单击密钥名称可以显示证书详细信息。也可以在此屏幕上单击[校验证书]检查证书是否有效。

步骤 5：禁用证书(IPSec)

禁用过去生成的证书。根据证书类型的不同，相关步骤也不同。

■对于自签名证书

如果将包含需要附加步骤的密钥的证书作为可信证书注册到使用 IPSec 通信的设备，请删除已注册的证书。删除已注册的证书后，注册重新生成的密钥的证书。

■对于 CSR/SCEP 证书

请求已颁发证书的证书颁发机构吊销证书。对于要请求的证书颁发机构，请参阅证书中的[发行者]。

注释

- 如果在使用 IPSec 通信的设备中使用 CRL 检查证书吊销情况，请在吊销证书后将更新的 CRL 注册到计算机或 Web 浏览器中。
- 如果使用 CRL 以外的方法（例如 OCSP）来检查证书吊销情况，请执行该方法的相关步骤。

步骤 6：启用新证书(IPSec)

启用证书。

■对于自签名证书

将新证书作为可信证书注册到使用 IPSec 通信的设备中。

■对于 CSR/SCEP 证书

不需要执行附加步骤。

适用于 SIP 的步骤

步骤 1：检查设置(SIP)

满足以下两个条件时，必须执行附加步骤：

- 在<SIP 设置>的<内联网设置>中启用了<使用 TLS>
- 在<SIP 设置>的<TLS 设置>中，<密钥和证书>显示密钥名称

按照以下步骤检查设置。

使用控制面板(P. 60)
使用远程用户界面时(P. 61)

使用控制面板

■检查<使用 TLS>

1 按 (设置/注册)。

2 按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <SIP 设置> ▶ <内联网设置>。

3 检查<使用 TLS>。

示例屏幕：

- 如果<使用 TLS>设置为<打开>，请继续检查<密钥和证书>。
- 如果<使用 TLS>设置为<关闭>，则不需要执行后续步骤。

■检查<密钥和证书>

1 按 (设置/注册)。

2 按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <SIP 设置> ▶ <TLS 设置>。

3 检查<密钥和证书>是否显示密钥名称。

示例屏幕：

- 如果<密钥和证书>显示密钥名称，则执行后续步骤。
- 如果<密钥和证书>没有显示密钥名称，则不需要执行后续步骤。

使用远程用户界面时

■检查[使用 TLS]和[密钥和证书]

1 启动远程用户界面。

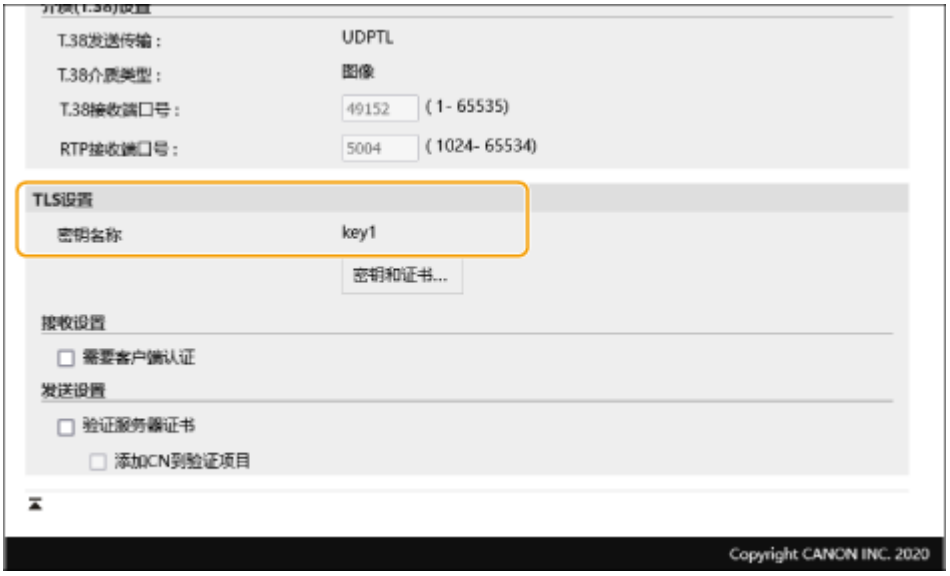
2 单击门户页面上的[设置/注册]。

3 单击[网络设置] ▶ [SIP 设置]。

4 检查[内联网设置]中的[使用 TLS]。

- 如果选择[使用 TLS]，请继续检查[密钥和证书]。
- 如果取消选择[使用 TLS]，则不需要执行后续步骤。

5 检查[TLS 设置]中的[密钥名称]。



- 如果显示密钥名称，则执行后续步骤。
- 如果没有显示密钥名称，则不需要执行后续步骤。

步骤 2：重新生成密钥和证书(SIP)

可以为使用本机生成的密钥生成两类型的证书：自签名证书和 CSR 证书。根据证书类型的不同，相关步骤也不同。
根据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

对于自签名证书(P. 63)
对于 CSR 证书(P. 66)

对于自签名证书

使用控制面板(P. 63)
使用远程用户界面时(P. 64)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <生成密钥> ▶ <生成网络通信密钥>。**

3 **配置所需的设置，然后转到下一个屏幕。**

示例屏幕：

a <密钥名称>

输入密钥名称。输入易于在列表中找到的名称。

b <签名算法>

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。等于或大于 1024 位的密钥长度可以支持 SHA384 和 SHA512 哈希算法。如果 c 选择为<RSA>，且 d 中的<密钥长度(bit)>设置为<1024>或更大，则可以选择 SHA384 和 SHA512 哈希算法。

c <密钥算法>

选择密钥算法。如果选择<RSA>，则<密钥长度(bit)>会显示为 d 的设置项目。如果选择<ECDSA>，则会显示<密钥类型>。

d <密钥长度(bit)>/<密钥类型>

如果对于 c 选择<RSA>，则指定密钥长度，如果选择<ECDSA>，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

4 为证书配置必要的项目 ▶ 按<生成密钥>。

示例屏幕：

a <有效期开始日期>/<有效期结束日期>

输入证书有效期的开始日期和结束日期。

b <国家名称/地区名称>/<省区>/<城市>/<组织>/<组织单位>

从列表中选择国家代码，然后输入位置和组织名称。

c <通用名称>

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 单击[生成密钥]。

5 单击[网络通信]。

6 配置密钥和证书设置。

a [密钥名称]

使用字母数字字符输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。根据密钥长度，可用的哈希算法可能有所不同。1024 位或更长的密钥长度可以支持 SHA384 和 SHA512 哈希算法。

c [密钥算法]

选择[RSA]或[ECDSA]作为密钥生成算法。如果选择[RSA]，请指定密钥长度；或者如果选择[ECDSA]，则指定密钥类型。在这两种情况下，值越高安全性越强，但同时会降低通信处理速度。

注释:

- 如果选择[SHA384]或[SHA512]作为[签名算法]，则在选择[RSA]作为[密钥算法]时无法将密钥长度设置为[512 bit]。

d [有效期开始日期(YYYY/MM/DD)]/[有效期结束日期(YYYY/MM/DD)]

输入证书有效期的开始日期和结束日期。[有效期结束日期(YYYY/MM/DD)]无法设为[有效期开始日期(YYYY/MM/DD)]中的日期之前的日期。

e [国家名称/地区名称]

单击[选择国家名称/地区名称]，然后从下拉列表中选择国家/地区。还可单击[输入互联网国家代码]并输入国家/地区代码，如将美国输入为“US”。

f [省区]/[城市]

根据需要使用字母数字字符输入位置。

g [组织]/[组织单位]

根据需要使用字母数字字符输入组织名称。

h [通用名称]

根据需要使用字母数字字符输入证书的通用名称。“通用名称”通常简写为“CN”。

7 单击[确定]。

- 生成密钥和证书需要一些时间。
- 生成的密钥和证书会自动注册到本机。

对于 CSR 证书

在本机上生成密钥和证书。使用屏幕上显示的 CSR 数据或输出到文件来请求证书颁发机构颁发证书。然后为密钥注册所颁发的证书。
只能从远程用户界面配置此设置。

■1. 生成密钥和 CSR

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **单击[生成密钥]。**

5 **单击[密钥和证书签名请求(CSR)]。**

6 **配置密钥和证书设置。**

a [密钥名称]

输入密钥名称。输入易于在列表中找到的名称。

b [签名算法]

选择用于签名的哈希算法。

c [密钥算法]

选择密钥算法，并在选择[RSA]时指定密钥长度，或在选择[ECDSA]时指定密钥类型。

d [国家名称/地区名称]

从列表中选择国家代码，或直接输入。

e [省区]/[城市]

输入位置。

f [组织]/[组织单位]

输入组织名称。

g [通用名称]

输入 IP 地址或 FQDN。

- 在 Windows 环境下执行 IPPS 打印时，请确保输入本机的 IP 地址。
- 输入本机的 FQDN 时需要 DNS 服务器。如果未使用 DNS 服务器，请输入本机的 IP 地址。

7 单击[确定]。

➠ 随即显示 CSR 数据。

- 如果要将 CSR 数据保存到文件，单击[存储到文件中]并指定保存位置。

注释:

- 生成 CSR 的密钥会显示在密钥和证书列表屏幕上，但无法单独使用。要使用此密钥，需要注册之后根据 CSR 颁发的证书。

8 请求证书颁发机构根据 CSR 数据颁发证书。

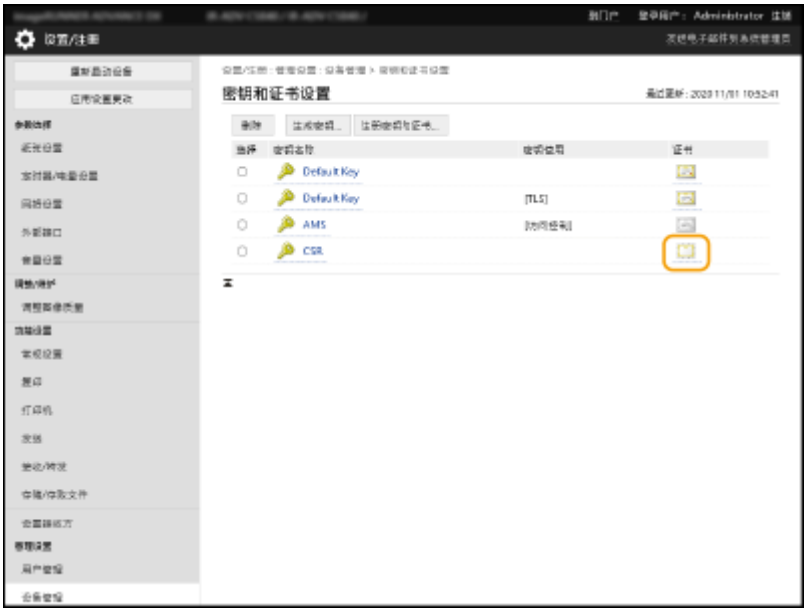
■2. 将颁发的证书注册的密钥

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 在[证书]列表中，针对要注册的证书单击 。



5 单击[注册证书...]。

6 注册证书。

- 单击[浏览...] ▶ 指定要注册的文件（证书） ▶ 单击[注册]。

步骤 3：重置密钥和证书(SIP)

将生成的密钥和证书设置为在 SIP 的 TLS 加密通信中使用的密钥和证书。

使用控制面板(P. 69)
使用远程用户界面时(P. 70)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<参数选择> ▶ <网络> ▶ <TCP/IP 设置> ▶ <SIP 设置> ▶ <TLS 设置>。**

3 **在<接收设置>和<发送设置>中配置相关设置 ▶ 按<密钥和证书>。**

示例屏幕：

<接收设置>	
<需要客户端认证>	选择<打开>或<关闭>。 如果选择<打开>，本机将在本机接收 IP 传真时请求客户端认证。
<发送设置>	
<验证服务器证书>	选择<打开>或<关闭>。 如果选择<打开>，本机将在本机接收 IP 传真时检查 TLS 服务器证书是否有效。
<验证 CN>	选择<打开>或<关闭>。 如果选择<打开>，本机将在本机接收 IP 传真时检查 CN（通用名称）。

4 **选择要用于 SIP 的 TLS 加密通信的密钥和证书 ▶ 按<设置为默认密钥> ▶ <确定>。**

示例屏幕：

注释

- 无法选择状态为“使用”的密钥和证书。
- 可以按<证书详细说明>检查有关证书的详细信息。
- 可以按<显示使用位置>检查密钥/证书用途。

5 **按下 <确定>。**

6 **按 (设置/注册) ▶ (设置/注册) ▶ <应用设置更改> ▶ <是>。**

➠ 重新启动本机后设置才会应用。

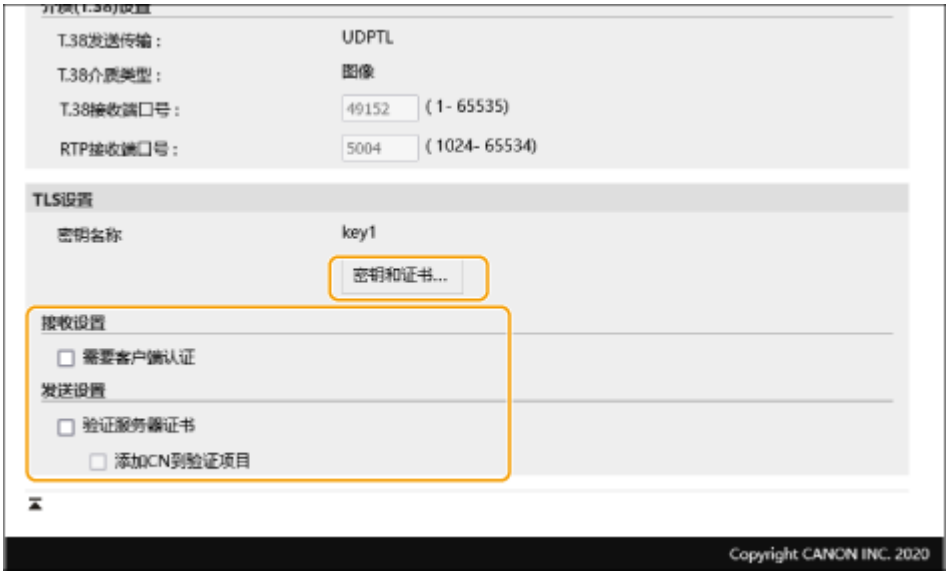
■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[网络设置] ▶ [SIP 设置]。**

4 **在[TLS 设置]中配置相关设置 ▶ 单击[密钥和证书]。**



[接收设置]	
[需要客户端认证]	如果选中此复选框，本机将在本机接收 IP 传真时请求客户端认证。
[发送设置]	
[验证服务器证书]	如果选中此复选框，本机将在本机接收 IP 传真时检查 TLS 服务器证书是否有效。
[添加 CN 到验证项目]	选择[打开] 或 [关闭]。 如果选中此复选框，本机将在本机接收 IP 传真时检查 CN（通用名称）。

5 在列表中将为使用的密钥点击[使用]。

6 单击[确定]。

7 单击[应用设置更改]重新启动本机。

➠ 重新启动本机后设置才会应用。

步骤 4：删除过去生成的密钥/证书(SIP)

据您的机器型号，可能无法从控制面板执行操作。在这种情况下，请从远程用户界面执行操作。

注释

- 禁用证书时，可能需要向证书颁发机构传递信息。删除密钥/证书前，请参阅 **检查是否必须执行附加程序(P. 5)** ，并记下所需的信息。

使用控制面板(P. 72)
使用远程用户界面时(P. 72)

■使用控制面板

1 **按 (设置/注册)。**

2 **按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <密钥和证书列表> ▶ <本设备的密钥和证书列表>。**

- 除非在本机上启用了用户签名功能，否则不会显示<本设备的密钥和证书列表>。在这种情况下，请继续执行下一步。

3 **选择密钥和证书 ▶ 按下<删除> ▶ <是>。**

示例屏幕：

注释:

- 如果显示 ，则密钥损坏或无效。
- 如果没有显示 ，则密钥的证书不存在。
- 如果选择密钥和证书并按<证书详细说明>，则显示证书详细信息。也可以按此屏幕上的<验证证书>以检查证书是否有效。

■使用远程用户界面时

1 **启动远程用户界面。**

2 **单击门户页面上的[设置/注册]。**

3 **单击[设备管理] ▶ [密钥和证书设置]。**

4 **选择密钥和证书 ▶ 单击[删除] ▶ [确定]。**

注释

- 如果显示 ，则密钥损坏或无效。
- 如果显示 ，则表示密钥的证书不存在。
- 单击密钥名称可以显示证书详细信息。也可以在此屏幕上单击[校验证书]检查证书是否有效。

步骤 5：禁用证书(SIP)

禁用过去生成的证书。根据证书类型的不同，相关步骤也不同。

■对于自签名证书

如果将包含需要附加步骤的密钥的证书作为可信证书注册到其他 IP 传真机器，请删除已注册的证书。删除已注册的证书后，注册重新生成的密钥的证书。

■对于 CSR 证书

请求已颁发证书的证书颁发机构吊销证书。对于要请求的证书颁发机构，请参阅证书中的[发行者]。

注释

- 如果使用其他 IP 传真机器检查证书吊销情况，请在吊销证书后将更新的 CRL 注册到计算机或 Web 浏览器中。
- 如果使用 CRL 以外的方法（例如 OCSP）来检查证书吊销情况，请执行该方法的相关步骤。

步骤 6：启用新证书(SIP)

启用证书。

■对于自签名证书

将新证书作为可信证书注册到其他 IP 传真机器中。

■对于 CSR 证书

不需要执行附加步骤。

适用于设备签名的步骤

步骤 1：检查 S/MIME 设置（设备签名）

检查是否需要执行适用于 S/MIME 和设备签名的附加步骤。

按照以下步骤检查 S/MIME 设置。

使用控制面板(P. 77)
使用远程用户界面时(P. 77)

■使用控制面板

1 按 (设置/注册)。

2 按<功能设置> ▶ <发送> ▶ <电子邮件/互联网传真设置> ▶ <S/MIME 设置>。

3 检查<加密设置>和<添加数字签名>。

示例屏幕：

- 如果<加密设置>设置为<不加密>且<添加数字签名>设置为<关闭>，则仅执行适用于设备签名的后续步骤。
- 如果指定了其他设置，请执行适用于 S/MIME 和设备签名的附加步骤。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[发送] ▶ [S/MIME 设置]。

4 检查[加密设置]和[添加数字签名]。

- 如果对于[加密设置]选择[不加密]且取消选择[添加数字签名]，则仅执行适用于设备签名的后续步骤。
- 如果指定了其他设置，请执行适用于 S/MIME 和设备签名的附加步骤。

步骤 2：重新生成密钥和证书（设备签名）

使用控制面板(P. 79)
使用远程用户界面时(P. 79)

■使用控制面板

1 按 (设置/注册)。

2 按<管理设置> ▶ <设备管理> ▶ <证书设置> ▶ <生成密钥>。

3 按<生成/更新设备签名密钥> ▶ <是> ▶ <确定>。

■使用远程用户界面时

1 启动远程用户界面。

2 单击门户页面上的[设置/注册]。

3 单击[设备管理] ▶ [密钥和证书设置]。

4 单击[生成密钥] ▶ [设备签名]。

5 单击[生成/更新] ▶ [确定]。

步骤 3：禁用证书（设备签名）

禁用过去生成的证书。

■如果用于设备签名的证书已注册到 Acrobat

如果用于设备签名的证书已在 Acrobat 中注册，请删除已注册的证书。

■如果从本机导出的 S/MIME 证书已导入其他机器

如果已从本机将用于通过 S/MIME 加密电子邮件/I-fax 的公钥证书（S/MIME 证书）导出并将其导入其他机器，请按照以下步骤，从已导入证书的机器中删除证书。

1. **启动远程用户界面。**
2. **单击门户页面上的[设置/注册]。**
3. **单击[设备管理] ▶ [S/MIME 证书设置]。**
4. **选择相应的证书 ▶ 单击[删除] ▶ [确定]。**

步骤 4：启用新证书（设备签名）

启用证书。

■如果用于设备签名的证书已注册到 Acrobat

如果已在 Acrobat 中注册用于设备签名的证书，请导出重新生成的用于设备签名的证书，然后将新证书注册到 Acrobat。

从本机导出证书(P. 81)

■如果从本机导出的 S/MIME 证书已导入其他机器

如果已从本机将用于通过 S/MIME 加密电子邮件/I-fax 的公钥证书（S/MIME 证书）导出并将其导入其他机器，请导出重新生成的证书，然后将其注册到其他机器。

从本机导出证书(P. 81)
将证书注册到其他机器(P. 81)

■从本机导出证书

执行以下步骤导出证书。

1. **启动远程用户界面。**
2. **单击门户页面上的[设置/注册]。**
3. **单击[设备管理] ▶ [导出设备签名]。**
4. **单击[开始导出] ▶ 将文件保存到所选的位置。**

■将证书注册到其他机器

执行以下步骤以将证书注册到其他机器。

1. **启动远程用户界面。**
2. **单击门户页面上的[设置/注册]。**
3. **单击[设备管理] ▶ [S/MIME 证书设置]。**

4 单击[注册 S/MIME 证书]。

5 注册 S/MIME 证书。

- 单击[浏览...] ▶ 指定要注册的文件（S/MIME 证书） ▶ 单击[注册]。

适用于蓝牙设置的附加步骤

适用于蓝牙设置的附加步骤

更新本机的固件后，会自动更新蓝牙的密钥。如果将 Canon PRINT Business 应用程序用于移动设备，则必须重新注册设备。

适用于蓝牙的步骤(P. 85)

适用于蓝牙的步骤

步骤 1：删除在 Canon PRINT Business 中注册的设备（蓝牙）

如果蓝牙设置为<打开>，请执行以下步骤。

适用于 iOS 的操作(P. 86)
适用于 Android 的操作(P. 86)

■适用于 iOS 的操作

1 点击 Canon PRINT Business 主页屏幕左上角的[ ]。

[选择打印机]屏幕随即显示。

2 通过点击[ ] ▶ [删除]，从列表中删除设备。

■适用于 Android 的操作

1 点击 Canon PRINT Business 主页屏幕左上角的[ ]。

[选择打印机]屏幕随即显示。

2 按住设备名称 ▶ 在显示的对话框中点击[删除]。

步骤 2：将设备重新注册到 Canon PRINT Business (Bluetooth)

如果蓝牙设置为<打开>，请执行以下步骤。

适用于 iOS 的操作(P. 87)
适用于 Android 的操作(P. 87)

■适用于 iOS 的操作

1 点击 Canon PRINT Business 主页屏幕左上角的[ ]。

[选择打印机]屏幕随即显示。

2 点击[附近打印机]。

检测到的设备随即出现。

■如未检测到设备

靠近本机，然后点击[搜索]。蓝牙可检测 2 米或 80 英寸距离范围内设备。

3 选择设备 ▶ 点击[添加]。

■适用于 Android 的操作

1 点击 Canon PRINT Business 主页屏幕左上角的[ ]。

[选择打印机]屏幕随即显示。

2 点击[附近打印机]。

检测到的设备随即出现。

■如未检测到设备

靠近本机，然后点击[搜索]。蓝牙可检测 2 米或 80 英寸距离范围内设备。

3 选择设备。

4 在显示的对话框中检查设备信息 ▶ 点击[添加]。

如果显示 Wi-Fi 网络设置屏幕，请按照屏幕上的说明操作。

适用于 Access Management System 设置的附加步骤

适用于 Access Management System 设置的附加步骤

更新本机的固件后，会自动更新 Access Management System 的密钥。

在密钥自动更新大约 30 分钟后，将再次自动检索限制信息。然后即可使用 Access Management System 功能正常进行打印。

如果要在更新固件后立即使用打印机驱动程序的 Access Management System 功能进行打印，必须重新手动检索 Access Management System 的限制信息。

适用于 Access Management System 的步骤(P. 90)

如果在没有重新检索限制信息的情况下尝试打印，则会发生错误。

适用于 Access Management System 的步骤

如果要在更新固件后立即使用打印机驱动程序的 Access Management System 功能进行打印，必须手动检索 Access Management System 的限制信息。

按照以下步骤执行操作。

在更新固件大约 30 分钟后，不需要执行以下步骤，因为到那时候将已经自动检索了限制信息。

1 登录计算机。

2 显示启用了 Access Management System 功能的打印机驱动程序所使用的打印机属性。

■对于 Windows Vista

- 单击[开始] ▶ [控制面板] ▶ [硬件和声音] ▶ 选择[打印机]。
- 右键单击打印机图标 ▶ 选择[属性]。

■对于 Windows Server 2008

- 单击[开始] ▶ [控制面板] ▶ [硬件和声音] ▶ 选择[打印机]。
- 右键单击打印机图标 ▶ 选择[属性]。

■对于 Windows Server 2008 R2

- 单击[开始] ▶ [控制面板] ▶ [硬件] ▶ 选择[设备和打印机]。
- 右键单击打印机图标 ▶ 选择[打印机属性]。

■对于 Windows 7

- 单击[开始] ▶ [控制面板] ▶ [硬件和声音] ▶ 选择[设备和打印机]。
- 右键单击打印机图标 ▶ 选择[打印机属性]。

■对于 Windows 8.1/Windows Server 2012

- 导航至桌面，在屏幕的右侧显示超级按钮。
- 单击 [设置] ▶ [控制面板] ▶ 选择[查看设备和打印机]。
- 右键单击打印机图标 ▶ 选择[打印机属性]。

■对于 Windows 10/Windows Server 2016

- 右键单击 [开始] ▶ 选择[控制面板] ▶ [查看设备和打印机]。
- 右键单击打印机图标 ▶ 选择[打印机属性]。

3 单击[AMS]选项卡。

4 单击[获取限制信息]。

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.