PKI配置命令

目 录

第 1 章 PKI 配置命令.....1
1.1 RSA 密钥配置命令.....1
1.1.1 RSA 密钥对生成.....1
1.1.2 RSA 密钥对导出.....2
1.1.3 RSA 密钥对导入.....3
1.1.4 RSA 密钥对删除.....3
1.1.5 RSA 公钥管理.....4
1.1.6 RSA 密钥对从 flash 中导入.....5
1.1.7 RSA 公钥信息显示.....5
1.2 CA 信任点配置命令.....6
1.2.1 信任点生成与删除.....6
1.2.2 信任点 RSA 密钥对配置.....6
1.2.3 信任点主题设置.....7
1.2.4 信任点域名设置.....8
1.2.5 CA 证书获取.....9
1.2.6 证书申请.....10
1.2.7 证书获取.....11
1.2.8 信任点导出.....13
1.2.9 信任点导入.....14
1.2.10 信任点证书链管理.....15
1.2.11 信任点证书链证书管理.....15

第1章　PKI 配置命令

1.1　RSA密钥配置命令

1.1.1　RSA 密钥对生成

命令描述

crypto key generate [rsa] [general-keys | encryption | signature] [exportable] [label *NAME***] [modulus** *NUMBER***]**

该命令产生一对 RSA 密钥。该命令同时可以设置 RSA 密钥对的属性，如是否可导出、密钥对名称、密钥对模数、密钥对用途。

参数

参数	参数说明
NAME	该密钥对的名称。长度不超过40个字符。可选参数。若不提供，使用当前路由器的主机名作为密钥对的名称。
NUMBER	生成RSA密钥对的模数。目前仅支持512和1024。可选参数。若不提供，使用512作为默认模数。

缺省

密钥对的缺省名称为主机名。缺省模数为 512。密钥对缺省为不可导出。

说明

不同的密钥对不可同名，因此在生成同名密钥对时会提示是否覆盖之前的密钥对：

% You already have keys defined named Router.

% Do you really want to replace them? [yes/no]:

生成密钥对时若设置为可导出，在密钥对生成之后可以将该密钥对的公钥及私钥导出至其他的存储空间以备份。

示例

下面的命令将生成与主机名同名的 RSA 密钥对，且该密钥对不可导出：

```
Router_config#crypto key generate rsa
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
Router_config#
```

1.1.2 RSA 密钥对导出

命令描述

crypto key export rsa *NAME* **pem { terminal | flash** *FILE* **| http** *URL***} {des | 3des}** *PASSWORD*

该命令将可导出的 RSA 密钥对以 PEM 文件的形式导出。不可导出的 RSA 密钥对则显示操作失败。可导出至 3 种位置：直接打印至终端、导出为 flash 中的文件，以及导出至 http 服务器。

参数

参数	参数说明
FILE	选择导出至flash时，指定文件名。长度不超过32个字符。
URL	选择导出至http服务器时，指定URL。需以http://开头，且长度不超过256个字符。
PASSWORD	为PEM文件提供的对称密钥。长度不超过32个字符。导入时需要提供相同的对称密钥才能成功。

缺省

无

说明

无

示例

下面的命令将主机中名为 key1 的 RSA 密钥对导出至终端，并以 test 作为对称密钥予以 des 加密：

```
Router_config#cry key export rsa key1 pem terminal des test
% Key name: key1
    Usage: General Purpose Key
    Key data:
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5PUWSA+ZVS4OwpMYaLC089+YV
dbjo9HrSFYgwCqRytkWq9Y7nXs8ppNkgay9G/NjnDNqyeJXIQt88hUutSGMlGhwo
dB/TTjeQ6pLBjIigK/L3YmsFkMc6kW7gQXVH4x2KAFD01VIXBPE4wRYFE10EXV8r
aI0RFQ+9zgArrxlJkQIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE-CBC,DB4985CA12ECFE1A

9TGEYOy1EcFIhX0LmMW0XmTo65s/EaLvTUR/WLNLDy6KVNMjtS+q1Q/zPJP+Xf5/
OPdgAcKU5p5uVk8negtA3VYwx9l3m/zfeF13XKYg1GWrFhzf9Js4AzAMWZmABISJ
pzp0dWDVWhNjtwaCsQTuTes3IC+vMQy/64bV/UlgqCuLph5u2R8Wy1dBlVEv2XKN
```

mrq0KvU+s/GzQCFV6ZjxtTOh97YDZzKN7mUQ5c50goGv5x6k+aUiQd0AwzUrlLQo
YnZw+tc/0UlPQOlqflK5ePwtUO9uXWH5bci9aGzcHIIa7vttsRFUngyOSN5uxhvC
4XmU8ABh8Q138p5X5RR09v9RqjTDdFuCOU3vYFNFpr8p+ugk2ED8aiGwlQBNYuSY
CnX9tJp+9rvsfA+0StkRuof/gzd8EFZJyKy/XSPJbGbClOlq4xgkC6rvAnC/yhEn
vgasQO2QLYCtYHKH0erGc2Npln0JTnc4faG6UykFO3DzGwYaxCQtTGSdJiWOCiVx
K1GRDaSDgQnbrPL0chsTICWpBmJ41x0ogJWJvJkSodZZowTZnJhpKgFiEcHokjlW
MaAQBURfkzELttMqDxlh4slklPiEz8j85GwzRhRpnQpRX3PnkCaSD7EX6ejhIIHM
ZIe5PRmza0amwk0N7BG5jschUg/yDrmjexfKdQt8S7gO38hjQAUdMQvGYeJkqqXu
oIe3m569swqJpIqXoLIT13yNd1E+ixY/3C3ND/v+l5cJYqQhXBBY67vKxTqjfa06
STMxw3iusEORHenp0z4+FFDWjpViGXOfjHjOMkR95WGfdyQQMERKWg==
-----END RSA PRIVATE KEY-----
Router_config#

1.1.3 RSA 密钥对导入

命令描述

crypto key import rsa *NAME* **pem {terminal | flash** *FILE* **| http** *URL***}** *PASSWORD* **[exportable]**

该命令将 PEM 文件导入为 RSA 密钥对。可从 3 种位置导入：直接从终端输入、从 flash 中的文件导入，以及从 http 服务器导入。

参数

参数	参数说明
FILE	选择从flash导入时，指定文件名。长度不超过32个字符。
URL	选择从http导入服务器时，指定URL。需以http://开头，且长度不超过256个字符。
PASSWORD	为PEM文件提供的对称密钥。长度不超过32个字符。需要提供导出时相同的对称密钥才能成功。

缺省

无

说明

导入成功的密钥对标记为不可导出。若需要再次导出该密钥对，需要在导入时指定 exportable 属性。

示例

1.1.4 RSA 密钥对删除

命令描述

crypto key zeroize [rsa [*NAME***]]**

删除 RSA 密钥对。若不指定删除的密钥对名称，则删除当前的所有 RSA 密钥对。

参数

参数	参数说明
NAME	指定删除的RSA密钥对名称。可选参数。

缺省

无

说明

密钥对删除时，与该密钥对绑定的 X509 证书也将从主机中删除。

示例

下面的命令将删除主机中名为 Router 的 RSA 密钥对：

```
Router_config#cry key zeroize rsa Router
% Keys to be removed are named 'Router'.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]:yes
Router_config#
```

1.1.5 RSA 公钥管理

命令描述

cry key pubkey-chain rsa

该命令进入 RSA 公钥管理模式。在此模式下，可以输入其他主机使用的 RSA 公钥。

addressed-key {*A.B.C.D* **|** *X:X:X::X***}**

该命令进入 RSA 公钥键入模式，且该 RSA 公钥与提供的 IP/IPv6 地址绑定。

key-string

该命令直接输入 DER 编码的 RSA 公钥。以输入 quit 表示输入完毕。

参数

参数	参数说明
A.B.C.D	指定绑定的IP地址。
X:X:X::X	指定绑定的IPv6地址。

缺省

无

说明

公钥输入成功后，该命令为可见命令。

示例

1.1.6 RSA 密钥对从 flash 中导入

命令描述

crypto key load-keyconf *NAME*

从路由器 flash 中读取保存的 RSA 密钥对。

crypto key load-keyconf end

从路由器 flash 中读取 RSA 密钥对操作结束。

参数

参数	参数说明
NAME	从flash中导入的RSA密钥对名称。

缺省

缺省设备中没有 RSA 密钥对。

说明

读取 RSA 密钥对时，flash 中需存在与密钥对同名的文件。

示例

1.1.7 RSA 公钥信息显示

命令描述

show crypto key mypubkey rsa

该命令显示在主机上生成的所有 RSA 密钥对的公钥信息。

show crypto key pubkey-chain rsa

该命令显示在非该主机生成的所有 RSA 密钥对的公钥信息。

参数

无

缺省

无

说明

公钥以 DER 编码形式显示。

示例

下面命令显示主机生成了一个名为 ike 的 RSA 密钥对，该密钥对不可导出：

```
Router_config#show crypto key mypubkey rsa
% Key name: ike
    Usage: General Purpose Key
    Key data:
keys will be non-exportable
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A1BBEA DB3E48FF
95BD2AA9 9829CC9C 70E1ABFA 52FE7920 ABEC4E25 409D6550 9856BD59 3418B7DE
EEF1E833 A81911A6 CF0FADF5 2A651663 DF430D76 DB2B16D4 BD020301 0001
```

1.2 CA信任点配置命令

1.2.1 信任点生成与删除

命令描述

crypto pki trustpoint *NAME*

该命令创建一个新的信任点，并进入信任点配置模式。

no crypto pki trustpoint *NAME*

命令删除一个信任点，该新信任点关联的证书将一并删去。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。

缺省

无

说明

无

示例

下面命令显示创建了一个名为 ca 的信任点：

```
Router_config#crypto pki trustpoint ca
```

1.2.2 信任点 RSA 密钥对配置

命令描述

rsakeypair *NAME*

no rsakeypair

该命令将当前信任点与主机中的 RSA 密钥对进行绑定。申请证书时，该信任点的主题名将与该 RSA 密钥对的公钥进行绑定。

no 命令取消信任点与 RSA 密钥对的绑定。取消绑定时，若该证书已经申请到证书，该证书将被删除。

参数

参数	参数说明
NAME	主机上已生成的RSA密钥对名称。长度不超过40个字符。

缺省

若没有配置 RSA 密钥对绑定，在申请证书时，信任点将尝试与默认的 RSA 密钥对（即名称为主机名的 RSA 密钥对）进行绑定。

说明

命令于信任点配置模式下。

若配置的 RSA 密钥对不存在，则绑定失败。

当绑定的密钥对被删除时，信任点与该密钥对的绑定关系也将解除；同时，信任点下该密钥对对应的证书也将删除。

示例

下面命令在主机上创建了一个名为 ike 的 RSA 密钥对与一个名为 ca 的信任点，并将该信任点与该密钥对绑定：

```
Router_config#crypto key generate rsa general-keys label ike
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
Router_config#crypto pki trustpoint ca
Router-ca-trustpoint#rsakeypair ike
```

1.2.3 信任点主题设置

命令描述

subject-name *NAME*

no subject-name

该命令配置信任点的主题，申请证书时该主题将与 RSA 密钥对的公钥绑定。

no 命令取消配置信任点的主题。

参数

参数	参数说明

NAME	主题。长度不超过128个字符。格式为"type=value"的键值对，常用的type有C，ST,O,OU,CN。其中CN是必须项。多个键值对之间以","分隔。例如:C=CN,O=AAA,CN=ca

缺省

无

说明

命令于信任点配置模式下。

主题是信任点的必配配置。申请证书时，若未配置主题，申请则失败。

示例

下面命令在主机上创建了一个名为 ca 的信任点，并设置在该信任点下，主机的主题名为“C=CN, O=ORGANIZE,OU=UNIT,CN=NAME”

```
Router_config#crypto pki trustpoint ca
Router-ca-trustpoint#subject-name C=CN,O=ORGANIZE,OU=UNIT,CN=NAME
```

1.2.4 信任点域名设置

命令描述

fqdn *NAME*

no fqdn

该命令将配置信任点的域名。申请证书时，该域名将作为证书的替代主题。

no 命令取消信任点域名配置。

参数

参数	参数说明
NAME	域名。长度不超过256个字符。

缺省

无

说明

命令于信任点配置模式下。

该命令为可选配置。

示例

下面命令在主机上创建了一个名为 ca 的信任点，并设置在该信任点下，主机的替代主题名为 name.unit.org

```
Router_config#crypto pki trustpoint ca
Router-ca-trustpoint#fqdn name.unit.org
```

1.2.5 CA 证书获取

命令描述

crypto pki authencate *NAME* **pem {terminal | flash** *FILE* **| http** *URL***}**

信任点配置为默认手动方式时，命令从不同的位置获取 PEM 格式的 CA 证书。terminal 直接从终端获取；flash 从 flash 中的文件获取；http 从 http 服务器获取。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。
FILE	flash中的文件名称。长度不超过32个字符。
URL	CA证书的http URL地址。长度不超过256个字符。

缺省

无

说明

命令中提供名称的信任点不存在时，操作失败。

示例

下面命令在主机上创建了一个名为 ca 的信任点，并通过终端直接获取该信任点的 CA 证书：

```
Router_config#crypto pki trustpoint ca
Router_config#cry pki authenticate ca pem terminal
Enter the base 64 encoded certificate.
End with a blank line.
-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgIJAJ2iRGpjugMwMA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEO
MAwGA1UEChMFQkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjAe
Fw0xMTA1MTcxNjE5MTZaFw0yMTA1MTQxNjE5MTZaMGUxCzAJBgNVBAYTAkFVMRMw
EQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEOMAwGA1UEChMF
QkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjBcMA0GCSqGSIb3
DQEBAQUAA0sAMEgCQQDLZEw9TrYYq99T+rLSKXEPYtz1akrCxwUz2/rUh+nc2CWe
mibZTnHTjSkxn3LH9JueNrneGBFPhrA74SGfEcvNAgMBAAGjgcowgccwHQYDVR0O
BBYEFPJg+rpCD1LxgyNLrtLy3YDZrmt+MIGXBgNVHSMEgY8wgYyAFPJg+rpCD1Lx
gyNLrtLy3YDZrmt+oWmkZzBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1T
dGF0ZTERMA8GA1UEBxMIc2hhbmdoYWkxDjAMBgNVBAoTBUJEQ09NMQ4wDAYDVQQL
EwVyb3V0ZTEOMAwGA1UEAxMFUVVYSU6CCQCdokRqY7oDMDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBBQUAA0EAZbep4wXX1UTyoPceeYR61W/HkiRoVZZhCGTnQrMv
BKokwjtN0IuGDfiVXugzxcfLXYcQt1yk4P46IdOvr+5Jog==
```

```
-----END CERTIFICATE-----

Router_config#
```

1.2.6 证书申请

命令描述

crypto pki enroll *NAME* **pem {terminal | flash** *FILE* **| http** *URL***}**

信任点配置为默认手动方式时，命令向不同的位置输出证书申请。terminal 直接向终端输出；flash 向 flash 中的文件输出；http 向 http 服务器输出。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。
FILE	flash中的文件名称。长度不超过32个字符。
URL	证书申请的http URL地址。长度不超过256个字符。

缺省

无

说明

信任点必须配置主题、配置 RSA 密钥对（或默认 RSA 密钥对）、且已获取 CA 证书后才可以申请证书。

若未配置 RSA 密钥对且未生成默认 RSA 密钥对时，申请证书则失败。

示例

下面命令在主机上创建了一个名为 ca 的信任点，设置主题名为“C=CN, O=ORGANIZE,OU=UNIT,CN=NAME”，绑定 RSA 密钥对 ike。在导入 CA 证书后生成本地证书申请：

```
Router_config#crypto pki trustpoint ca
Router-ca-trustpoint#subject-name C=CN,O=ORGANIZE,OU=UNIT,CN=NAME
Router-ca-trustpoint#rsakeypair ike
Router_config#crypto pki authenticate ca pem terminal
-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgIJAJ2iRGpjugMwMA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEO
MAwGA1UEChMFQkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjAe
Fw0xMTA1MTcxNjE5MTZaFw0yMTA1MTQxNjE5MTZaMGUxCzAJBgNVBAYTAkFVMRMw
EQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEOMAwGA1UEChMF
QkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjBcMA0GCSqGSIb3
DQEBAQUAA0sAMEgCQQDLZEw9TrYYq99T+rLSKXEPYtz1akrCxwUz2/rUh+nc2CWe
mibZTnHTjSkxn3LH9JueNrneGBFPhrA74SGfEcvNAgMBAAGjgcowgccwHQYDVR0O
BBYEFPJg+rpCD1LxgyNLrtLy3YDZrmt+MIGXBgNVHSMEgY8wgYyAFPJg+rpCD1Lx
gyNLrtLy3YDZrmt+oWmkZzBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1T
```

dGF0ZTERMA8GA1UEBxMIc2hhbmdoYWkxDjAMBgNVBAoTBUJEQ09NMQ4wDAYDVQQL
EwVyb3V0ZTEOMAwGA1UEAxMFUVVYSU6CCQCdokRqY7oDMDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBBQUAA0EAZbep4wXX1UTyoPceeYR61W/HkiRoVZZhCGTnQrMv
BKokwjtN0IuGDfiVXugzxcfLXYcQt1yk4P46IdOvr+5Jog==
-----END CERTIFICATE-----

Router_config#crypto pki enroll ca pem terminal
-----BEGIN CERTIFICATE REQUEST-----
MIIBDTCBuAIBADBTMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEO
MAwGA1UEChMFQkRDT00xDzANBgNVBAsTBlJPVVRFUjEOMAwGA1UEAxMFbmFtZTEw
XDANBgkqhkiG9w0BAQEFAANLADBIAkEAtTYxSC6aCJVqCdPj1fapTmtX6WPpZr6k
53ikMotn8b2Go9qyA9A0vKo4FDTsw65tRHfqt1i5D7JuFLa8a70nMwIDAQABoAAw
DQYJKoZIhvcNAQEEBQADQQBL6rRm6MlTJBfuPVtaWiiatc1In2bJ6CIlBPzVUHTU
WU+aWNgQ95tgMIU6ck6jElmp2sqLggXmWrMzdZV10fj0
-----END CERTIFICATE REQUEST-----
Router_config#

1.2.7 证书获取

命令描述

crypto pki import *NAME* **certificate pem {terminal | flash** *FILE* **| http** *URL***}**

申请证书后，命令从不同的位置获取证书：terminal 直接从终端获取证书；flash 从 flash 中的文件获取证书；http 从 http 服务器上获取证书。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。
FILE	flash中的文件名称。长度不超过32个字符。
URL	证书的http URL地址。长度不超过256个字符。

缺省

无

说明

无

示例

下面示例创建一个名为 ca 的信任点，绑定 RSA 密钥对 ike，设置主题名为“C=CN, O=ORGANIZE, OU=UNIT, CN=NAME”。在导入 CA 证书、生成本地证书申请后成功导入本地证书：

```
Router_config#crypto pki trustpoint ca
Router-ca-trustpoint#subject-name C=CN,O=ORGANIZE,OU=UNIT,CN=NAME
Router-ca-trustpoint#rsakeypair ike
Router_config#crypto pki authenticate ca pem terminal
```

-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgIJAJ2iRGpjugMwMA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEO
MAwGA1UEChMFQkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjAe
Fw0xMTA1MTcxNjE5MTZaFw0yMTA1MTQxNjE5MTZaMGUxCzAJBgNVBAYTAkFVMRMw
EQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEOMAwGA1UEChMF
QkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjBcMA0GCSqGSIb3
DQEBAQUAA0sAMEgCQQDLZEw9TrYYq99T+rLSKXEPYtz1akrCxwUz2/rUh+nc2CWe
mibZTnHTjSkxn3LH9JueNrneGBFPhrA74SGfEcvNAgMBAAGjgcowgccwHQYDVR0O
BBYEFPJg+rpCD1LxgyNLrtLy3YDZrmt+MIGXBgNVHSMEgY8wgYyAFPJg+rpCD1Lx
gyNLrtLy3YDZrmt+oWmkZzBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1T
dGF0ZTERMA8GA1UEBxMIc2hhbmdoYWkxDjAMBgNVBAoTBUJEQ09NMQ4wDAYDVQQL
EwVyb3V0ZTEOMAwGA1UEAxMFUVVYSU6CCQCdokRqY7oDMDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBBQUAA0EAZbep4wXX1UTyoPceeYR61W/HkiRoVZZhCGTnQrMv
BKokwjtN0IuGDfiVXugzxcfLXYcQt1yk4P46IdOvr+5Jog==
-----END CERTIFICATE-----

```
Router_config#crypto pki enroll ca pem terminal
```

-----BEGIN CERTIFICATE REQUEST-----
MIIBDTCBuAIBADBTMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEO
MAwGA1UEChMFQkRDT00xDzANBgNVBAsTBlJPVVRFUjEOMAwGA1UEAxMFbmFtZTEw
XDANBgkqhkiG9w0BAQEFAANLADBIAkEAtTYxSC6aCJVqCdPj1fapTmtX6WPpZr6k
53ikMotn8b2Go9qyA9A0vKo4FDTsw65tRHfqt1i5D7JuFLa8a70nMwIDAQABoAAw
DQYJKoZIhvcNAQEEBQADQQBL6rRm6MlTJBfuPVtaWiiatc1In2bJ6CIlBPzVUHTU
WU+aWNgQ95tgMIU6ck6jElmp2sqLggXmWrMzdZV10fj0
-----END CERTIFICATE REQUEST-----

```
Router_config#
Router_config#crypto pki import ca certificate pem terminal
Enter the base 64 encoded certificate.
End with a blank line.
```

-----BEGIN CERTIFICATE-----
MIIChTCCAi+gAwIBAgICAVowDQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCQVUx
EzARBgNVBAgTClNvbWUtU3RhdGUxETAPBgNVBAcTCHNoYW5naGFpMQ4wDAYDVQQK
EwVCRENPTTEOMAwGA1UECxMFcm91dGUxDjAMBgNVBAMTBVFVWElOMB4XDTEyMDcw
NDAzMDQwOFoXDTEzMDcwNDAzMDQwOFowUzELMAkGA1UEBhMCQVUxEzARBgNVBAg
T
ClNvbWUtU3RhdGUxDjAMBgNVBAoTBUJEQ09NMQ8wDQYDVQQLEwZST1VURVIxDjAM
BgNVBAMTBW5hbWUxMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALU2MUgumgiVagnT
49X2qU5rV+lj6Wa+pOd4pDKLZ/G9hqPasgPQNLyqOBQ07MOubUR36rdYuQ+ybhS2
vGu9JzMCAwEAAaOB2jCB1zAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVu
U1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUB3USK/46y3Rz8VD6
HG3VhF9vppEwHwYDVR0jBBgwFoAU8mD6ukIPUvGDI0uu0vLdgNmua34wKAYDVR0f
BCEwHzAdoBugGYYXaHR0cDovLzEuMS4xLjE1OS9jYS5jcmwwMgYIKwYBBQUHAQEE
JjAkMCIGCCsGAQUFBzABhhZodHRwOi8vMS4xLjEuMTU5OjgwODAvMA0GCSqGSIb3
DQEBBQUAA0EAbXTRbQTgaGIuE6CMgqdQidxjw3iy01KvOa1dGARCSxIcaCD/cvVN
lubNi02xW5zowShBv0Z6OAW3glWpwEPUcQ==
-----END CERTIFICATE-----

```
Router_config#
```

1.2.8 信任点导出

命令描述

crypto pki export *NAME* **pem {terminal | flash** *FILE* **| http** *URL***} {des | 3des}** *PASSWORD*

命令将信任点的证书链以及证书绑定的 RSA 密钥对导出为 PEM 文件，分别导出至不同的位置：terminal 直接导出至终端；flash 导出至 flash 中的文件；http 导出至 http 服务器。

crypto pki export *NAME* **pkcs12 {flash** *FILE* **| http** *URL***}** *PASSWORD*

命令将信任点的证书链以及证书绑定的 RSA 密钥对导出为 PKCS12 文件，分别导出至不同的位置：flash 导出至 flash 中的文件；http 导出至 http 服务器。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。
FILE	导出至flash中的文件名称。长度不超过32个字符。
URL	导出文件的http URL地址。长度不超过256个字符。
PASSWORD	用于PEM文件或PKCS12文件加密的对称密钥。长度不超过32个字符。

缺省

无

说明

信任点导出可以方便备份密钥对以及相关证书链。只有获取了证书的信任点可以导出。

示例

下面示例将一个名为 ca 的信任点导出为 PEM 格式，加密方式采用 DES，密钥为"test"，并输出至终端：

```
Router_config#crypto pki export ca pem terminal des test
-----BEGIN CERTIFICATE-----
MIICjjCCAjigAwIBAgIJAJ2iRGpjugMwMA0GCSqGSIb3DQEBBQUAMGUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEO
MAwGA1UEChMFQkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjAe
Fw0xMTA1MTcxNjE5MTZaFw0yMTA1MTQxNjE5MTZaMGUxCzAJBgNVBAYTAkFVMRMw
EQYDVQQIEwpTb21lLVN0YXRlMREwDwYDVQQHEwhzaGFuZ2hhaTEOMAwGA1UEChMF
QkRDT00xDjAMBgNVBAsTBXJvdXRlMQ4wDAYDVQQDEwVRVVhJTjBcMA0GCSqGSIb3
DQEBAQUAA0sAMEgCQQDLZEw9TrYYq99T+rLSKXEPYtz1akrCxwUz2/rUh+nc2CWe
mibZTnHTjSkxn3LH9JueNrneGBFPhrA74SGfEcvNAgMBAAGjgcowgccwHQYDVR0O
BBYEFPJg+rpCD1LxgyNLrtLy3YDZrmt+MIGXBgNVHSMEgY8wgYyAFPJg+rpCD1Lx
gyNLrtLy3YDZrmt+oWmkZzBlMQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1T
dGF0ZTERMA8GA1UEBxMIc2hhbmdoYWkxDjAMBgNVBAoTBUJEQ09NMQ4wDAYDVQQL
EwVyb3V0ZTEOMAwGA1UEAxMFUVVYSU6CCQCdokRqY7oDMDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBBQUAA0EAZbep4wXX1UTyoPceeYR61W/HkiRoVZZhCGTnQrMv
```

BKokwjtN0IuGDfiVXugzxcfLXYcQt1yk4P46IdOvr+5Jog==
-----END CERTIFICATE-----
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALU2MUgumgiVagnT49X2qU5rV+lj6Wa+
pOd4pDKLZ/G9hqPasgPQNLyqOBQ07MOubUR36rdYuQ+ybhS2vGu9JzMCAwEAAQ==
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE-CBC,AB30D745D437A706

ks7rYBGWi7Gp2QlnuI+jWTe1tmYCX7bjYANoOylstUfWIuqScrfl9RRUloGD6vMS
LvhJXU0xUQn8y6aHYlRSmw+MzKpeHa3H/iw+m33I2I7onKnIL/lV2ZiqKKMeuid+
XgWhzAR+3EyBUuQ/0x3JtzS09XOVg5VYtp1W8Pt/T7YXHhxvXkptBhAaY6YvbEoi
1/fs4YcK+kG6Lfc1idd1TODwVMcOiuy8BQJdDEsdaBi2mF0U8KxGJ0es0vHidjdB
9ddNPothlQaflZAH9VjhrwLr/XIhP8HA5mgCfYKRtuWXfAxbVhnh/XOc+DVhq+82
52/eSvXWKjlPs/luwwaXBJ82aPHBgsqQa5/+LdITCC1cmxQ6X23hmVL4GnRpSOvW
mHFLQ1m5gJHqfClBUAK3riKRP7lgINanEUiwD7ED5jM=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIChTCCAi+gAwIBAgICAVowDQYJKoZIhvcNAQEFBQAwZTELMAkGA1UEBhMCQVUx
EzARBgNVBAgTClNvbWUtU3RhdGUxETAPBgNVBAcTCHNoYW5naGFpMQ4wDAYDVQQK
EwVCRENPTTEOMAwGA1UECxMFcm91dGUxDjAMBgNVBAMTBVFVWElOMB4XDTEyMDcw
NDAzMDQwOFoXDTEzMDcwNDAzMDQwOFowUzELMAkGA1UEBhMCQVUxEzARBgNVBAg
T
ClNvbWUtU3RhdGUxDjAMBgNVBAoTBUJEQ09NMQ8wDQYDVQQLEwZST1VURVIxDjAM
BgNVBAMTBW5hbWUxMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALU2MUgumgiVagnT
49X2qU5rV+lj6Wa+pOd4pDKLZ/G9hqPasgPQNLyqOBQ07MOubUR36rdYuQ+ybhS2
vGu9JzMCAwEAAaOB2jCB1zAJBgNVHRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGVu
U1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUB3USK/46y3Rz8VD6
HG3VhF9vppEwHwYDVR0jBBgwFoAU8mD6ukIPUvGDI0uu0vLdgNmua34wKAYDVR0f
BCEwHzAdoBugGYYXaHR0cDovLzEuMS4xLjE1OS9jYS5jcmwwMgYIKwYBBQUHAQEE
JjAkMCIGCCsGAQUFBzABhhZodHRwOi8vMS4xLjEuMTU5OjgwODAvMA0GCSqGSIb3
DQEBBQUAA0EAbXTRbQTgaGIuE6CMgqdQidxjw3iy01KvOa1dGARCSxIcaCD/cvVN
lubNi02xW5zowShBv0Z6OAW3glWpwEPUcQ==
-----END CERTIFICATE-----

1.2.9 信任点导入

命令描述

crypto pki import *NAME* **pem terminal** *PASSWORD*

crypto pki import *NAME* **{pem | pkcs12} {flash** *FILE* **| http** *URL***}** *PASSWORD*

命令导入信任点的证书链以及证书绑定的 RSA 密钥对。除了从 flash 文件导入和从 http 服务器导入外，PEM 文件形式还可以直接从终端输入。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。
FILE	flash中的文件名称。长度不超过32个字符。

URL	文件的http URL地址。长度不超过256个字符。
PASSWORD	用于PEM文件或PKCS12文件解密的对称密钥。长度不超过32个字符。

缺省

无

说明

信任点导入时，若存在同名信任点，原有信任点将被覆盖；导入的 RSA 密钥对与信任点同名，且若存在同名 RSA 密钥对，原有密钥对将被覆盖。

示例

下面示例将从 flash 中的 PEM 文件 a.file 中导入名为 ca 的信任点，解密密钥为"test"：

Router_config#crypto pki import ca2 pem flash a.file test

1.2.10 信任点证书链管理

命令描述

crypto pki certificate chain *NAME*

命令进入信任点的证书链配置模式。

参数

参数	参数说明
NAME	信任点名称。长度不超过32个字符。

缺省

无

说明

无

示例

1.2.11 信任点证书链证书管理

命令描述

certificate ca *SERIAL*

命令输入 CA 证书的序列号后，进入 CA 证书的输入模式。输入模式下需要输入 CA 证书的 DER 编码，并以 quit 结束。

certificate *SERIAL*

命令输入证书的序列号后，进入证书的输入模式。输入模式下需要输入证书的 DER 编码，并以 quit 结束。

参数

参数	参数说明
SERIAL	证书的十六进制序列号。

缺省

无

说明

无

示例

无