PKI Configuration Commands

Table of Contents

Chapter 1 PKI Configuration Commands

1.1 RSA Key Configuration Commands

1.1.1 Generating an RSA Key Pair

Syntax

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

The command generates an RSA key pair. The command also configures the attributes of RSA key pair, such as its exporting, name, modulus-size and usage.

Parameters

Parameters	Description
NAME	Name of the RSA key pair Its length is within 40 characters. optional parameter If the name is not specified, the host name will be taken as the name of the RSA key pair.
NUMBER	Specifies the IP size of the key modulus. The supported modulus is 512 bits and 1024 bits at present. optional parameter By default, the modulus is 512 bits.

Default value

The default name of the RSA key pair is the host name. By default, the modulus is 512 bits. The default modulus cannot be exported.

Remarks

The key pair cannot share the same name. Or here will be a prompt if generating a RSA key pair named the same with the existing one.

% You already have keys defined named Router.

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

The public key and the private key of RSA can be exported to other devices if RSA is configured exportable.

Example

The following example generates an non-exportable RSA key pair named the same with the host:

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 Exporting an RSA Key Pair

Syntax

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

The command exports the RSA key pair to the PEM file. Here prompts "operation failure" if RSA key pair is non-exportable. The RSA key pair can be exported to 3 locations: directly printed out files; flash files and the http server.

Parameters

Parameters	Description
FILE	Specifies the file name when being exported to the flash file. Its length must be within 32 characters.
URL	Specifies URL when being exported to the http server. The URL must be headed with *http://* and of no less than 256 characters.
PASSWORD	The symmetric password provided for PEM document. Its length must be within 32 characters. The import is successful provided that there is the same symmetric password as the export.

Default value

No default behavior or values.

Remarks

None

Example

The following command shows how to export the RSA key pair named **key 1** to the device and set des encryption whose symmetric key is **test**.

```
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 Importing an RSA Key Pair

Syntax

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

The command imports PEM file as RSA key pair. The PEM file can be imported through 3 locations: import from the device, the flash file and the http server.

Parameters

Parameters	Description
FILE	Specifies the file name when importing the flash file. Its length must be within 32 characters.
URL	Specifies URL when being imported from the http server. The URL must be headed with *http://* and of no less than 256 characters.
PASSWORD	The symmetric password provided for PEM document. Its length must be within 32 characters. The import is successful provided that there is the same symmetric password as export.

Default value

None

Remarks

The successfully imported key pair will be identified as non-exportable. Specify the attribute of **exportable** when exporting the key pair once more.

Example

1.1.4 Deleting an RSA Key Pair

Syntax

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

Delete RSA key pair All RSA key pairs will be deleted if no key pair is specified.

Parameters

Parameters	Description
NAME	Specifies the name to be deleted RSA key pair. optional parameter

Default value

None

Remarks

When the key pair is deleted, the X509 certificate binding with the key pair will be deleted from the host too.

Example

The following command shows how to delete the RSA key pair named Router from the host.

```
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 Public Key Administration

Syntax

cry key pubkey-chain rsa

The command enters RSA public key administration mode. In this mode, the RSA public key of other host can be input.

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

The command is to enter the RSA public key input mode and the RSA public key will be bound with IP/IPv6 address.

key-string

The command will directly input the RSA public key of DER code. quit means the input is finished.

Parameters

Parameters	Description
A.B.C.D	Specifies the binding IP address.
X:X:X::X	Specifies the binding IPv6 address.

Default value

None

Remarks

The command is visible when the public key is successfully input.

Example

1.1.6 Importing RSA key pair from the flash file

Syntax

crypto key load-keyconf *NAME*

Read stored RSA key pair from the router flash

crypto key load-keyconf end

End the process of reading stored RSA key pair from the router flash.

Parameters

Parameters	Description
NAME	Name of the RSA key pair imported from flash

Default value

There is no RSA key pair by default.

Remarks

In reading RSA key pair, there must be a file named the same in flash with the key pair.

Example

1.1.7 Showing RSA Public Key Information

Syntax

show crypto key mypubkey rsa

The command shows the public key information of all RSA key pair generated on the host.

show crypto key pubkey-chain rsa

The command shows the public key information of all RSA key pair generated not on the host.

Parameters

None

Default value

None

Remarks

The public key is displayed in form of DER code.

Example

The following example shows the host generates an non-exportable RSA key pair named **ike**:

```
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 Trustpoint Configuration Commands

1.2.1 Generating and deleting CA Trustpoint

Syntax

crypto pki trustpoint *NAME*

The command creates a new trust point and enters the trust point mode.

no crypto pki trustpoint *NAME*

The command deletes the trust point and the certificate associated with the new trust point will be deleted too.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.

Default value

None

Remarks

None

Example

The following command creates a trust point named **ca**.

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

1.2.2 Configuring Trust Point RSA Key Pair

Syntax

rsakeypair *NAME*

no rsakeypair

The command binds the trust point with the RSA key pair of the host. When applying for the certificate, the name of the trust point and the public key of the RSA key pair will be bound.

To disable this feature, use the command **no rsakeypair**. The certificate will be deleted when canceling the binding.

Parameters

Parameters	Description
NAME	Name of the RSA key pair generated on the host. Its length must be within 40 characters.

Default value

If RSA key pair binding is not configured, the trust point will try to bind with the default RSA key pair (RSA key pair name with the host name) when applying for the certificate.

Remarks

The command runs in trust point mode.

The binding is failed if the configured RSA key pair does not exist.

When the binding key pair is deleted, the trust point and the key pair will not be bound. Meanwhile, the corresponding certificate will be deleted too.

Example

The following command creates a RSA key pair named **ike** and a trust point named **ca**, and bind the trust point and the key pair.

```
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 bits 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 Configuring Trust Point Subject Name

Syntax

subject-name *NAME*

no subject-name

The command configures the subject of the trust point. When applying for the certificate, the subject and the RSA key pair will be bound.

To disable this feature, use the command **no subject-name**.

Parameters

Parameters	Description
NAME	subject Its length must be within 128 characters. The form of a key value pair is "type=value". The common type is C, ST,O,OU,CN. Of them, CN is mandatory. The key-value pairs are isolated with ",". For instance: C=CN,O=AAA,CN=ca

Default value

None

Remarks

The command runs in trust point mode.

The subject is compulsory when configuring. The certificate application is failed if the subject is not configured.

Example

The following command created a trust point named **ca** and configure the subject name of the host as “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 Configuring Trust Point Domain Name

Syntax

fqdn *NAME*

no fqdn

The command configures the domain name of the trust point. When applying for the certificate, the domain name will be taken as the secondary subject of the certificate.

To disable this feature, use the command **no fqdn**.

Parameters

Parameters	Description
NAME	domain name Its length must be within 256 characters.

Default value

None

Remarks

The command runs in trust point mode.

The command is optional configuration.

Example

The following command created a trust point named **ca** and configure the subject name of the host as **name.unit.org**.

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

1.2.5 Acquiring CA certificate

Syntax

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

When the trust point is configured manually by default, the command can acquire CA certificates in form of PEM from different locations. **terminal** means acquiring from the device; **flash** means acquiring from the flash file; **http** means acquiring from the http server.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.
FILE	The file name in flash Its length must be within 32 characters.
URL	http URL of CA certificate Its length must be within 256 characters.

Default value

None

Remarks

The configuration is failed if the trust point provided by the command doesn't exist.

Example

The following command shows how to create a trust point named **ca** and acquire the CA certificate from the device.

```
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 Applying for Certificate

Syntax

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

When the trust point is configured manually by default, the command can export CA certificates to different locations. **terminal** means acquiring from the device; **flash** means acquiring from the flash file; **http** means acquiring from the http server.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.
FILE	The file name in flash Its length must be within 32 characters.
URL	http URL applied by CA certificate Its length must be within 256 characters.

Default value

None

Remarks

The trust point must configure the subject and RSA key pair (or default RSA key pair). Applying for the certificate is impossible only after the CA certificate is acquired.

The certificate application is failed if RSA key pair is not configured and RSA key pair is not generated by default.

Example

The following command creates a trust point named **ca**, configures the subject name as "C=CN, O=ORGANIZE,OU=UNIT,CN=NAME" and binds RSA key pair named ike. Generate local certificate application after importing the CA certificate.

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
BKokwjtN0luGDfiVXugzxcfLXYcQt1yk4P46IdOvr+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 Acquiring Certificate

Syntax

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

The command enables acquiring certificates from different locations after applying for the certificate: **terminal** means acquiring from the device; **flash** means acquiring from the flash file; **http** means acquiring from the http server.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.
FILE	The file name in flash Its length must be within 32 characters.
URL	http URL of the certificate Its length must be within 256 characters.

Default value

None

Remarks

None

Example

The following command creates a trust point named **ca**, binds RSA key pair named ike and configures the subject name as “C=CN, O=ORGANIZE,OU=UNIT,CN=NAME”. Import the local certificate after importing CA certificate and generating local certificate application:

```
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 Exporting Trust Point

Syntax

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

PASSWORD

The command exports the certificate chain of the trust point and the certificate bound RSA key pair to the PEM file in different locations: **terminal** means exporting to the device; **flash** means exporting to the flash file; **http** means exporting to the http server.

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

The command exports the certificate chain of the trust point and the certificate bound RSA key pair to the PKCS12 file in different locations: **flash** means exporting to the flash file; **http** means exporting to the http server.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.
FILE	The file name exported to flash Its length must be within 32 characters.
URL	URL of exported file in http Its length must be within 256 characters.
PASSWORD	The encryption symmetric password of PEM file and PKCS 12 file Its length must be within 32 characters.

Default value

None

Remarks

Exporting the trust point is conducive to backup the key pair and the relevant certificate chain. Only trust points with certificates can be exported.

Example

The following example is to export the trust point named **ca** to PEM file, set des encryption whose symmetric key is **test** and output to the device:

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 Importing Trust Point

Syntax

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

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

The command imports the certificate chain and the certificate bound RSA key pair. Except importing from the flash file and the http server, the PEM file can directly input from the device.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.
FILE	The file name in flash Its length must be within 32 characters.
URL	URL of imported file in http Its length must be within 256 characters.
PASSWORD	The encrypt symmetric password of PEM file and PKCS 12 file Its length must be within 32 characters.

Default value

None

Remarks

The original trust point will be overlapped if a trust point with the same name is imported. The original key pair will be overlapped if an RSA key pair shares the same name with the key pair and the trust point is imported.

Example

The following command shows how to import the trust point named **ca** from **a.file** in the PEM file and the decrypt is **test**.

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

1.2.10 Trust Point Certificate Chain Administration

Syntax

crypto pki certificate chain *NAME*

The command enters the configuration mode of the trust point certificate chain.

Parameters

Parameters	Description
NAME	Name of the trust point. Its length must be within 32 characters.

Default value

None

Remarks

None

Example

1.2.11 Trust Point Certificate Chain Administration

Syntax

certificate ca *SERIAL*

Enter CA certificate input mode by input CA certificate serial number. Input CA certificate DER code in the input mode and end with "quit".

certificate *SERIAL*

Enter CA certificate input mode by input CA certificate serial number. Input CA certificate DER code in the input mode and end with "quit".

Parameters

Parameters	Description
SERIAL	hexadecimal serial number of the certificate

Default value

None

Remarks

None

Example

None