目 录

1 PKI ····· 1-1

1.1 PKI 配置命令 ····· 1-1

1.1.1 attribute ····· 1-1

1.1.2 ca identifier ····· 1-2

1.1.3 certificate request entity ····· 1-3

1.1.4 certificate request from ····· 1-4

1.1.5 certificate request mode ····· 1-5

1.1.6 certificate request polling ····· 1-6

1.1.7 certificate request url ····· 1-7

1.1.8 common-name ····· 1-8

1.1.9 country ····· 1-8

1.1.10 crl check enable ····· 1-9

1.1.11 crl url ····· 1-10

1.1.12 display pki certificate access-control-policy ····· 1-11

1.1.13 display pki certificate attribute-group ····· 1-12

1.1.14 display pki certificate domain ····· 1-13

1.1.15 display pki certificate renew-status ····· 1-18

1.1.16 display pki certificate request-status ····· 1-20

1.1.17 display pki crl domain ····· 1-21

1.1.18 fqdn ····· 1-23

1.1.19 ip ····· 1-24

1.1.20 ldap-server ····· 1-24

1.1.21 locality ····· 1-25

1.1.22 organization ····· 1-26

1.1.23 organization-unit ····· 1-27

1.1.24 pkcs7-encryption-algorithm ····· 1-27

1.1.25 pki abort-certificate-request ····· 1-28

1.1.26 pki certificate access-control-policy ····· 1-29

1.1.27 pki certificate attribute-group ····· 1-29

1.1.28 pki delete-certificate ····· 1-30

1.1.29 pki domain ····· 1-32

1.1.30 pki entity ····· 1-32

1.1.31 pki export ····· 1-33

1.1.32 pki import ····· 1-40
1.1.33 pki request-certificate ····· 1-44
1.1.34 pki retrieve-certificate ····· 1-45
1.1.35 pki retrieve-crl ····· 1-46
1.1.36 pki storage ····· 1-47
1.1.37 pki validate-certificate ····· 1-48
1.1.38 public-key dsa ····· 1-50
1.1.39 public-key ecdsa ····· 1-51
1.1.40 public-key rsa ····· 1-52
1.1.41 public-key sm2 ····· 1-54
1.1.42 revocation-check method ····· 1-55
1.1.43 root-certificate fingerprint ····· 1-56
1.1.44 rule ····· 1-57
1.1.45 source ····· 1-58
1.1.46 state ····· 1-59
1.1.47 subject-dn ····· 1-60
1.1.48 usage ····· 1-61
1.1.49 vpn-instance ····· 1-61

1 PKI

1.1 PKI配置命令

1.1.1 attribute

attribute 命令用来配置属性规则，用于根据证书的颁发者名、主题名以及备用主题名来过滤证书。

undo attribute 命令用来删除证书属性规则。

【命令】

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

【缺省情况】

不存在属性规则，即对证书的颁发者名、主题名以及备用主题名没有限制。

【视图】

证书属性组视图

【缺省用户角色】

network-admin

context-admin

【参数】

id：证书属性规则序号，取值范围为 1～16。

alt-subject-name：表示证书备用主题名（Subject Alternative Name）。

fqdn：指定实体的 FQDN。

ip：指定实体的 IP 地址。

dn：指定实体的 DN。

issuer-name：表示证书颁发者名（Issuer Name）。

subject-name：表示证书主题名（Subject Name）。

ctn：表示包含操作。

equ：表示相等操作。

nctn：表示不包含操作。

nequ：表示不等操作。

attribute-value：指定证书属性值，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

各证书属性中可包含的属性域个数有所不同：

- 主题名和颁发者名中均只能包含一个 DN，但是均可以同时包含多个 FQDN 和 IP；

- 备用主题名中不能包含 DN，但是可以同时包含多个 FQDN 和 IP。

不同类型的证书属性域与操作关键字的组合代表了不同的匹配条件，具体如下表所示：

表1-1 对证书属性域的操作涵义

操作	DN	FQDN/IP
ctn	DN中包含指定的属性值	任意一个FQDN/IP中包含了指定的属性值
nctn	DN中不包含指定的属性值	所有FQDN/IP中均不包含指定的属性值
equ	DN等于指定的属性值	任意一个FQDN/IP等于指定的属性值
nequ	DN不等于指定的属性值	所有FQDN/IP均不等于指定的属性值

如果证书的相应属性中包含了属性规则里指定的属性域，且满足属性规则中定义的匹配条件，则认为该属性与属性规则相匹配。例如：属性规则 2 中定义，证书的主题名 DN 中包含字符串 abc。如果某证书的主题名的 DN 中确实包含了字符串 abc，则认为该证书的主题名与属性规则 2 匹配。

只有证书中的相应属性与某属性组中的所有属性规则都匹配上，才认为该证书与此属性组匹配。如果证书中的某属性中没有包含属性规则中指定的属性域，或者不满足属性规则中的匹配条件，则认为该证书与此属性组不匹配。

【举例】

创建一个名为 mygroup 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
```

创建证书属性规则 1，定义证书主题名中的 DN 包含字符串 abc。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

创建证书属性规则 2，定义证书颁发者名中的 FQDN 不等于字符串 abc。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

创建证书属性规则 3，定义证书主题备用名中的 IP 地址不等于 10.0.0.1。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

【相关命令】

- **display pki certificate attribute-group**
- **rule**

1.1.2 ca identifier

ca identifier 命令用来指定设备信任的 CA 名称。

undo ca identifier 命令用来恢复缺省情况。

【命令】

ca identifier *name*

undo ca identifier

【缺省情况】

未指定设备信任的 CA。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

name：设备信任的 CA 名称，为 1～63 个字符的字符串，区分大小写。

【使用指导】

获取 CA 证书时，必须指定信任的 CA 名称，这个名称会被作为 SCEP 消息的一部分发送给 CA 服务器。但是一般情况下，CA 服务器会忽略收到的 SCEP 消息中的 CA 名称的具体内容。但是如果在同一台服务器上配置了两个 CA，且它们的 URL 是相同的，则服务器将根据 SCEP 消息中的 CA 名称选择对应的 CA。因此，使用此命令指定的 CA 名称必须与希望获取的 CA 证书对应的 CA 名称一致。

【举例】

指定设备信任的 CA 名称为 new-ca。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

1.1.3 certificate request entity

certificate request entity 命令用来指定用于申请证书的 PKI 实体名称。

undo certificate request entity 命令用来恢复缺省情况。

【命令】

certificate request entity *entity-name*

undo certificate request entity

【缺省情况】

未指定设备申请证书所使用的 PKI 实体名称。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

entity-name：用于申请证书的 PKI 实体名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

本命令用于在 PKI 域中指定申请证书的 PKI 实体。PKI 实体描述了申请证书的实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。

一个 PKI 域中只能指定一个 PKI 实体名称，多次执行本命令，最后一次执行的命令生效。

【举例】

指定申请证书的 PKI 实体名称为 en1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request entity en1
```

【相关命令】

- **pki entity**

1.1.4 certificate request from

certificate request from 命令用来配置证书申请的注册受理机构。

undo certificate request from 命令用来恢复缺省情况。

【命令】

certificate request from { **ca** | **ra** }

undo certificate request from

【缺省情况】

未指定证书申请的注册受理机构。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ca：表示实体从 CA 申请证书。

ra：表示实体从 RA 申请证书。

【使用指导】

选择从 CA 还是 RA 申请证书，由 CA 服务器决定，需要了解 CA 服务器上由什么机构来受理证书申请。

推荐使用独立运行的 RA 作为注册受理机构。

【举例】

指定实体从 RA 申请证书。

```
<Sysname> system-view
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] certificate request from ra
```

1.1.5 certificate request mode

certificate request mode 命令用来配置证书申请方式。

undo certificate request mode 命令用来恢复缺省情况。

【命令】

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string* | **renew-before-expire** *days* [**reuse-public-key**] [**automatic-append common-name**]] * | **manual** }

undo certificate request mode

【缺省情况】

证书申请方式为手工方式。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

auto：表示用自动方式申请证书。

password：指定吊销证书时使用的密码。

cipher：以密文方式设置密码。

simple：以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。明文密码为 1～31 个字符的字符串，密文密码为 1～73 个字符的字符串。

renew-before-expire *days*：表示证书自动续签功能。*days* 是证书自动续签提前的时间，取值范围为 0～365，单位为天。如果取值为 0 则表示证书到期时再自动续签，会出现暂时的业务中断。

reuse-public-key：表示证书自动续签时使用原有密钥对。若不指定该参数，则表示证书自动续签的过程中会自动生成新的密钥对，且证书续签成功后原有密钥对被立即覆盖。

automatic-append common-name：表示证书自动续签时在 PKI 实体的通用名后添加随机值。若不指定该参数，则证书自动续签时在 PKI 实体的通用名后不添加随机值。

manual：表示用手工方式申请证书。

【使用指导】

两种申请方式都属于在线申请，具体情况如下：

- 如果是自动方式，则设备会在与 PKI 域关联的应用（例如 IKE）需要做身份认证时，自动向证书注册机构发起获取 CA 证书和申请本地证书的操作。自动方式下，可以指定吊销证书时使用的密码，是否需要指定密码是由 CA 服务器的策略决定的。
- 如果为手工方式，则需要手工完成获取 CA 证书、申请本地证书的操作。

为避免由于证书过期造成业务中断，请在选择自动方式申请证书时配置证书自动续签功能。证书自动续签是指，系统在证书有效期到达之前自动申请新的证书，申请成功后新证书立即替换原有证书。

由于某些 CA 服务器不支持 PKI 实体使用相同的通用名多次申请证书，为了保证自动续签证书成功，请配置 **automatic-append common-name** 参数使设备每次都使用新的通用名为 PKI 实体申请新的证书。

【举例】

指定证书申请方式为自动方式。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto
```

指定证书申请方式为自动方式，并设置吊销证书时使用的密码为明文 123456。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
```

指定证书申请方式为自动方式，并设置吊销证书时使用的口令为明文 123456，设置证书到期前 60 天自动申请新证书替换原有证书，申请新证书时生成新密钥对。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
renew-before-expire 60
```

【相关命令】

- **pki request-certificate**

1.1.6 certificate request polling

certificate request polling 命令用来配置证书申请状态的查询周期和最大次数。

undo certificate request polling 命令用来恢复缺省情况。

【命令】

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

【缺省情况】

证书申请状态的查询周期为 20 分钟，最多查询 50 次。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

count *count*：表示证书申请状态的查询次数，取值范围为 1～100。

interval *interval*：表示证书申请状态的查询周期，取值范围为 5～168，单位为分钟。

【使用指导】

设备发送证书申请后，如果 CA 服务器采用手工方式来签发证书申请，则不会立刻响应设备的申请。这种情况下，设备通过定期向 CA 服务器发送状态查询消息，能够及时获取到被 CA 签发的证书。CA 签发证书后，设备将通过发送状态查询得到证书，之后停止发送状态查询消息。如果达到最大查询次数时，CA 服务器仍未签发证书，则设备停止发送状态查询消息，本次证书申请失败。

如果 CA 服务器采用自动签发证书的方式，则设备可以立刻得到证书，这种情况下设备不会向 CA 服务器发送状态查询消息。

【举例】

指定证书申请状态的查询周期为 15 分钟，最多查询 40 次。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request polling interval 15
[Sysname-pki-domain-aaa] certificate request polling count 40
```

【相关命令】

- **display pki certificate request-status**

1.1.7 certificate request url

certificate request url 命令用来配置实体通过 SCEP 进行证书申请的注册受理机构服务器的 URL。

undo certificate request url 命令用来恢复缺省情况。

【命令】

certificate request url *url-string*

undo certificate request url

【缺省情况】

未指定注册受理机构服务器的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：表示证书申请的注册受理机构服务器的 URL，为 1～511 个字符的字符串，区分大小写。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

本命令配置的 URL 内容包括注册受理机构服务器的位置及 CGI 命令接口脚本位置，格式为 http://*server_location/cgi_script_location*。

【举例】

指定实体进行证书申请的注册受理机构服务器的 URL 为 http://169.254.0.1/certsrv/mscep/mscep.dll。

```
<Sysname> system-view
[Sysname] pki domain a
[Sysname-pki-domain-a] certificate request url http://169.254.0.1/certsrv/mscep/mscep.dll
```

1.1.8 common-name

common-name 命令用来配置 PKI 实体的通用名，比如用户名称。

undo common-name 命令用来恢复缺省情况。

【命令】

common-name *common-name-sting*

undo common-name

【缺省情况】

未配置 PKI 实体的通用名。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

common-name-sting：PKI 实体的通用名，为 1～63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 的通用名为 test。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name test
```

1.1.9 country

country 命令用来配置 PKI 实体所属的国家代码。

undo country 命令用来恢复缺省情况。

【命令】

country *country-code-string*

undo country

【缺省情况】

未配置 PKI 实体所属的国家代码。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

country-code-string：PKI 实体所属的国家代码，为标准的两字符代码，区分大小写，例如中国为 CN。

【举例】

配置 PKI 实体 en 所属的国家代码为 CN。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] country CN
```

1.1.10 crl check enable

crl check enable 命令用来开启 CRL 检查。

undo crl check enable 命令用来关闭 CRL 检查。

【命令】

crl check enable

undo crl check enable

【缺省情况】

CRL 检查处于开启状态。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

CRL（Certificate Revocation List，证书废除列表）是一个由 CA 签发的文件，该文件中包含被该 CA 吊销的所有证书的列表。一个证书有可能在有效期达到之前被 CA 吊销。使能 CRL 检查的目的是查看设备上的实体证书或者即将要导入、获取到设备上的实体证书是否已经被 CA 吊销，若检查结果表明实体证书已被吊销，那么该证书就不被设备信任。

【举例】

关闭 CRL 检查。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] undo crl check enable
```

【相关命令】

- **pki import**
- **pki retrieve-certificate**
- **pki validate-certificate**

1.1.11 crl url

crl url 命令用来设置 CRL 发布点的 URL。

undo crl url 命令用来恢复缺省情况。

【命令】

crl url *url-string*

undo crl url

【缺省情况】

未设置 CRL 发布点的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string：表示 CRL 发布点的 URL，为 1～511 个字符的字符串，区分大小写。格式为 ldap://*server_location* 或 http://*server_location*，其中 *server_location* 可以为 IP 地址和 DNS 域名。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

如果 CRL 检查处于使能状态，则进行 CRL 检查之前，需要首先从 PKI 域指定的 CRL 发布点获取 CRL。若 PKI 域中未配置 CRL 发布点的 URL 时，从该待验证的证书中获取发布点信息：优先获取待验证的证书中记录的发布点，如果待验证的证书中没有记录发布点，则获取 CA 证书中记录的发布点（若待验证的证书为 CA 证书，则获取上一级 CA 证书中记录的发布点）。如果无法通过任何途径得到发布点，则通过 SCEP 协议获取 CRL。

若配置了 LDAP 格式的 CRL 发布点 URL，则表示要通过 LDAP 协议获取 CRL。若该 URL 中未携带主机名，则需要根据 PKI 域中配置的 LDAP 服务器地址信息来得到完整的 LDAP 发布点 URL。

【举例】

指定 CRL 发布点的 URL 为 http://169.254.0.30。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

【相关命令】

- **ldap-server**

- **pki retrieve-crl**

1.1.12 display pki certificate access-control-policy

display pki certificate access-control-policy 命令用来显示证书访问控制策略的配置信息。

【命令】

display pki certificate access-control-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

policy-name：指定证书访问控制策略名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书访问控制策略的名称，则显示所有证书访问控制策略的配置信息。

【举例】

显示证书访问控制策略 mypolicy 的配置信息。

```
<Sysname> display pki certificate access-control-policy mypolicy
 Access control policy name: mypolicy
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
```

显示所有证书属性访问控制策略的配置信息。

```
<Sysname> display pki certificate access-control-policy
 Total PKI certificate access control policies: 2
 Access control policy name: mypolicy1
     Rule 1  deny    mygroup1
     Rule 2  permit  mygroup2
 Access control policy name: mypolicy2
     Rule 1  deny    mygroup3
     Rule 2  permit  mygroup4
```

表1-2 display pki certificate access-control-policy 命令显示信息描述表

字段	描述
Total PKI certificate access control policies	PKI证书访问控制策略的总数
Access control policy name	证书访问控制策略名
Rule *number*	访问控制规则编号

字段	描述
permit	当证书的属性与属性组里定义的属性匹配时，认为该证书有效，通过了访问控制策略的检测
deny	当证书的属性与属性组里定义的属性匹配时，认为该证书无效，未通过访问控制策略的检测

【相关命令】

- **pki certificate access-control-policy**
- **rule**

1.1.13 display pki certificate attribute-group

display pki certificate attribute-group 命令用来显示证书属性组的配置信息。

【命令】

display pki certificate attribute-group [*group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-name：指定证书属性组名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书属性组的名称，则显示所有证书属性组的配置信息。

【举例】

显示证书属性组 mygroup 的信息。

```
<Sysname> display pki certificate attribute-group mygroup
 Attribute group name: mygroup
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
```

显示所有证书属性组的信息。

```
<Sysname> display pki certificate attribute-group
 Total PKI certificate attribute groups: 2.
 Attribute group name: mygroup1
      Attribute  1 subject-name     dn    ctn   abc
      Attribute  2 issuer-name      fqdn  nctn  app
Attribute group name: mygroup2
      Attribute  1 subject-name     dn    ctn   def
```

```
Attribute  2 issuer-name      fqdn  nctn  fqd
```

表1-3 display pki certificate attribute-group 命令显示信息描述表

字段	描述
Total PKI certificate attribute groups	PKI证书属性组的总数
Attribute group name	证书属性组名称
Attribute *number*	属性规则编号
subject-name	证书主题名
alt-subject-name	证书备用主题名
issuer-name	证书颁发者名
dn	实体的DN
fqdn	实体的FQDN
ip	实体的IP地址
ctn	表示包含操作
nctn	表示不包含操作
equ	表示等于操作
nequ	表示不等操作
Attribute 1 subject-name dn ctn abc	属性规则内容，包括以下参数： • alt-subject-name：表示证书备用主题名 • issuer-name：表示证书颁发者名 • subject-name：表示证书主题名 • fqdn：表示实体的 FQDN • ip：表示实体的 IP 地址 • dn：表示实体的 DN • ctn：表示包含操作 • equ：表示相等操作 • nctn：表示不包含操作 • nequ：表示不等操作

【相关命令】

- **attribute**
- **pki certificate attribute-group**

1.1.14 display pki certificate domain

display pki certificate domain 命令用来显示证书的内容。

【命令】

display pki certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain-name：显示指定证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

ca：显示 CA 证书。

local：显示本地证书。

peer：显示对端证书。

serial *serial-num*：指定要显示的对端证书的序列号。

【使用指导】

显示 CA 证书时，会显示此 PKI 域中所有 CA 证书的详细信息，若 PKI 域中存在 RA 证书，则同时显示 RA 证书的详细信息。

显示本地证书时，会显示此 PKI 域中所有本地证书的详细信息。

显示对端证书时，如果不指定序列号，将显示所有对端证书的简要信息；如果指定序列号，将显示该序号对应的指定对端证书的详细信息。

【举例】

显示 PKI 域 aaa 中的 CA 证书。

```
<Sysname> display pki certificate domain aaa ca
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
```

```
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
                    57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                    7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                    6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                    c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                    84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                    52:db:7b:cd:5d:2b:66:5a:fb
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

显示 PKI 域 aaa 中的本地证书。

```
<Sysname> display pki certificate domain aaa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
```

```
            CA:FALSE
        Netscape Cert Type:
            SSL Client, S/MIME
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
        Netscape Comment:
            User Certificate of OpenCA Labs
        X509v3 Subject Key Identifier:
            91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
        X509v3 Authority Key Identifier:
            keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

        X509v3 Subject Alternative Name:
            email:fips@ccc.com
        X509v3 Issuer Alternative Name:
            email:pki@openca.org
        Authority Information Access:
            CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
            OCSP - URI:http://titan:2560/
            1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

        X509v3 CRL Distribution Points:

            Full Name:
              URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
        dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
        65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
        04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
        cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
        50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
        3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
        de:18:9d:c1
```

显示 PKI 域 aaa 中的所有对端证书的简要信息。

```
<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1
```

```
Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=sldsslserver
```

显示 PKI 域 aaa 中的一个特定序号的对端证书的详细信息。

```
<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=ccc, OU=sec, CN=ssl
        Validity
            Not Before: Oct 15 01:23:06 2010 GMT
            Not After : Jul 26 06:30:54 2012 GMT
        Subject: CN=sldsslserver
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:
                    a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:
                    68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:
                    04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:
                    97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:
                    39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:
                    29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:
                    ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:
                    8b:a3:4d:b2:17:08:8d:dd:81
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key
Agreement
            Netscape Cert Type:
                SSL Server
            X509v3 Subject Alternative Name:
                DNS:docm.com
            X509v3 Subject Key Identifier:
                3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://s03130.ccc.sec.com:447/ssl.crl
```

```
Signature Algorithm: sha1WithRSAEncryption
    61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
    31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
    36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
    85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
    17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
    ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
    ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
    f0:a5
```

表1-4 display pki certificate 命令显示信息描述表

字段	描述
Version	证书版本号
Serial Number	证书序列号
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期
Subject	证书所属的实体信息
Subject Public Key Info	证书所属的实体的公钥信息
X509v3 extensions	X.509版本3格式的证书扩展属性

【相关命令】

- **pki domain**
- **pki retrieve-certificate**

1.1.15 display pki certificate renew-status

display pki certificate renew-status 命令用来显示 PKI 域的证书续签状态。

【命令】

display pki certificate renew-status [**domain** *domain-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain *domain-name*：指定 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。若未指定 PKI 域的名称，则显示所有 PKI 域的证书续签状态。

【举例】

显示所有 PKI 域的证书续签状态，其中 PKI 域 domain1 的证书申请方式配置中未指定 **reuse-public-key**，续签时生成了新的密钥对。

```
<Sysname> display pki certificate renew-status
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2016/06/13
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

显示指定 PKI 域的证书续签状态。

```
<Sysname> display pki certificate renew-status domain domain1
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when  key pair created: 15:40:48 2016/06/13
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

表1-5 display pki certificate renew-status 命令显示信息描述表

字段	描述
Domain Name	PKI域名
Renew Time	预计证书续签发生的时刻
Renew public key	证书续签时使用的新密钥对的信息，只有在证书续签过程比较慢或续签失败的情况下才会显示出此密钥对信息
Key type	密钥对的类型，取值包括：RSA、DSA、ECDSA和SM2
Time when key pair created	密钥对的创建时间和日期
Key code	密钥对的密钥信息

【相关命令】

- **certificate request mode**
- **pki domain**

1.1.16 display pki certificate request-status

display pki certificate request-status 命令用来显示证书的申请状态。

【命令】

display pki certificate request-status [**domain** *domain-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain *domain-name*：指定证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

【使用指导】

若不指定 PKI 域的名称，则显示所有 PKI 域的证书申请状态。

【举例】

显示 PKI 域 aaa 的证书申请状态。

```
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
    Domain name: aaa
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
```

显示所有 PKI 域的证书申请状态。

```
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
```

```
Key usage: Signature
Remain polling attempts: 10
Next polling attempt after : 188 seconds
```

表1-6 display pki certificate request 命令显示信息描述表

字段	描述
Certificate Request Transaction *number*	证书申请任务的编号，从1开始顺序编号
Domain name	PKI域名
Status	证书申请状态。目前，仅有一种取值Pending，表示等待
Key usage	证书用途，包括以下取值： • General：表示通用，既可以用于加密也可以用于签名 • Signature：表示用于签名 • Encryption：表示用于加密
Remain polling attempts	剩余的证书申请状态的查询次数
Next polling attempt after	当前到下次查询证书申请状态的时间间隔，单位为秒

【相关命令】

- **certificate request polling**
- **pki domain**
- **pki retrieve-certificate**

1.1.17 display pki crl domain

display pki crl domain 命令用来显示存储在本地的 CRL。

【命令】

display pki crl domain *domain-name*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

domain *domain-name*：指定 CRL 所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

【使用指导】

用户可以通过该命令查看证书吊销列表，看所需的证书是否已经被吊销。

【举例】

显示 PKI 域 aaa 存储在本地的 CRL。

```
<Sysname> display pki crl domain aaa
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=cn/O=docm/OU=sec/CN=therootca
        Last Update: Apr 28 01:42:13 2011 GMT
        Next Update: NONE
        CRL extensions:
            X509v3 CRL Number:
                6
            X509v3 Authority Key Identifier:
                keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
        Revocation Date: Apr 28 01:37:52 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:37:49 2011 GMT
    Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
        Revocation Date: Apr 28 01:33:28 2011 GMT
        CRL entry extensions:
            Invalidity Date:
                Apr 28 01:33:09 2011 GMT
    Signature Algorithm: sha1WithRSAEncryption
        57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
        5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
        36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
        99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
        8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
        4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
        52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
        ba:aa
```

表1-7 display pki crl domain 显示信息描述表

字段	描述
Version	CRL版本号
Signature Algorithm	CA签名该CRL采用的签名算法
Issuer	颁发该CRL的CA证书名称
Last Update	上次更新CRL的时间
Next Update	下次更新CRL的时间
CRL extensions	CRL扩展属性

字段	描述
X509v3 CRL Number	X509版本3格式的CRL序号
X509v3 Authority Key Identifier	X509版本3格式的签发该CRL的CA的标识符
keyid	公钥标识符 一个CA可能有多个密钥对，该字段用于标识CA用哪个密钥对对该CRL进行签名
Revoked Certificates	撤销的证书信息
Serial Number	被吊销证书的序列号
Revocation Date	证书被吊销的日期
CRL entry extensions:	CRL项目扩展属性
Signature Algorithm:	签名算法以及签名数据

【相关命令】

- **pki retrieve-crl**

1.1.18 fqdn

fqdn 命令用来配置 PKI 实体的 FQDN。

undo fqdn 命令用来恢复缺省情况。

【命令】

fqdn *fqdn-name-string*

undo fqdn

【缺省情况】

未配置 PKI 实体的 FQDN。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

fqdn-name-string：PKI 实体的 FQDN，为 1～255 个字符的字符串，区分大小写。形式为 *hostname@domainname*

【使用指导】

FQDN 是实体在网络中的唯一标识，由一个主机名和一个域名组成。

【举例】

配置 PKI 实体 en 的 FQDN 为 abc@pki.domain.com。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

1.1.19 ip

ip 命令用来配置 PKI 实体的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

ip { *ip-address* | **interface** *interface-type interface-number* }

undo ip

【缺省情况】

未配置 PKI 实体的 IP 地址。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address：指定 PKI 实体的 IP 地址。

interface *interface-type interface-numbe*：指定接口的主 IP 地址作为 PKI 实体的 IP 地址。*interface-type interface-number* 表示接口类型及接口编号。

【使用指导】

通过本命令，可以直接指定 PKI 实体的 IP 地址，也可以指定设备上某接口的主 IP 地址作为 PKI 实体的 IP 地址。如果指定使用某接口的 IP 地址，则不要求本配置执行时该接口上已经配置了 IP 地址，只要设备申请证书时，该接口上配置了 IP 地址，就可以直接使用该地址作为 PKI 实体身份的一部分。

【举例】

配置 PKI 实体 en 的 IP 地址为 192.168.0.2。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

1.1.20 ldap-server

ldap-server 命令用来指定 LDAP 服务器。

undo ldap-server 命令用来恢复缺省情况。

【命令】

ldap-server host *hostname* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ldap-server

【缺省情况】

未指定 LDAP 服务器。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

host *hostname*：LDAP 服务器的主机名，为 1～255 个字符的字符串，区分大小写，支持 IPv4 与 IPv6 地址的表示方法以及 DNS 域名的表示方法。

port *port-number*：LDAP 服务器的端口号，取值范围为 1～65535，缺省值为 389。

vpn-instance *vpn-instance-name*：指定 LDAP 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，则表示该 LDAP 服务器属于公网。

【使用指导】

以下两种情况下，需要配置 LDAP 服务器：

- 通过 LDAP 协议获取本地证书或对端证书时，需要指定 LDAP 服务器。
- 通过 LDAP 协议获取 CRL 时，若 PKI 域中配置的 LDAP 格式的 CRL 发布点 URL 中未携带主机名或 IP 地址，则需要根据此处配置的 LDAP 服务器地址来得到完整的 LDAP 发布点 URL。

在一个 PKI 域中，只能指定一个 LDAP 服务器，多次执行本命令，最后一次执行的命令生效。

【举例】

指定 LDAP 服务器的 IP 地址为 10.0.0.1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

指定 LDAP 服务器，IP 地址为 10.0.0.11，端口号为 333，所在的 MPLS L3VPN 的实例名称为 vpn1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.11 port 333 vpn-instance vpn1
```

【相关命令】

- **pki retrieve-certificate**
- **pki retrieve-crl**

1.1.21 locality

locality 命令用来配置 PKI 实体所在的地理区域名称，比如城市名称。

undo locality 命令用来恢复缺省情况。

【命令】

locality *locality-name*

undo locality

【缺省情况】

未配置 PKI 实体所在的地理区域名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

locality-name：PKI 实体所在的地理区域的名称，为 1～63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所在地理区域的名称为 pukras。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] locality pukras
```

1.1.22 organization

organization 命令用来配置 PKI 实体所属组织的名称。

undo organization 命令用来恢复缺省情况。

【命令】

organization *org-name*

undo organization

【缺省情况】

未配置 PKI 实体所属组织名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

org-name：PKI 实体所属的组织名称，为 1～63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所属的组织名称为 abc。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization abc
```

1.1.23 organization-unit

organization-unit 命令用来指定实体所属的组织部门的名称。

undo organization-unit 命令用来恢复缺省情况。

【命令】

organization-unit *org-unit-name*

undo organization-unit

【缺省情况】

未配置 PKI 实体所属组织部门的名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

org-unit-name：PKI 实体所属组织部门的名称，为 1～63 个字符的字符串，区分大小写，不能包含逗号。使用该参数可在同一个组织内区分不同部门的 PKI 实体。

【举例】

配置 PKI 实体 en 所属组织部门的名称为 rdtest。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization-unit rdtest
```

1.1.24 pkcs7-encryption-algorithm

pkcs7-encryption-algorithm 命令用来指定 PKCS#7 证书使用的加密算法。

undo pkcs7-encryption-algorithm 命令用来恢复缺省情况。

【命令】

pkcs7-encryption-algorithm { **3des-cbc** | **aes-cbc-128** | **des-cbc** | **sm4-cbc** }

undo pkcs7-encryption-algorithm

【缺省情况】

PKCS#7 证书使用的加密算法为 **dec-cbc**。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

3des-cbc：指定证书使用的加密算法为 CBC 模式的 3DES 算法，3DES 算法采用 168 比特的密钥进行加密。

des-cbc：指定证书使用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

sm4-cbc：指定证书使用的加密算法为 CBC 模式的 SM4 算法，SM4 算法采用 128 比特的密钥进行加密。

aes-cbc-128：指定证书使用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

【使用指导】

在线申请证书过程中需要生成 PKCS#7 证书。本命令指定 PKCS#7 证书封装与解封过程中需要使用的加密算法类型。加密算法类型需要与 CA 服务器支持的对称加密算法类型保持一致。

【举例】

指定 PKCS#7 证书使用的加密算法为 CBC 模式的 3DES 算法。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] pkcs7-encryption-algorithm 3des-cbc
```

1.1.25 pki abort-certificate-request

pki abort-certificate-request 命令用来停止证书申请过程。

【命令】

pki abort-certificate-request domain *domain-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

【使用指导】

用户在证书申请时，可能由于某种原因需要改变证书申请的一些参数，比如通用名、国家代码、FQDN 等，而此时证书申请正在运行，为了新的申请不与之前的申请发生冲突，建议先停止之前的申请程序，再进行新的申请。

【举例】

停止证书申请过程。

```
<Sysname> system-view
[Sysname] pki abort-certificate-request domain 1
```

```
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

【相关命令】

- **display pki certificate request-status**
- **pki request-certificate domain**

1.1.26 pki certificate access-control-policy

pki certificate access-control-policy 命令用来创建证书访问控制策略，并进入证书访问控制策略视图。如果指定的证书访问控制策略已存在，则直接进入其视图。

undo pki certificate access-control-policy 命令用来删除指定的证书访问控制策略。

【命令】

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

【缺省情况】

不存在证书访问控制策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：表示证书访问控制策略名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

一个证书访问控制策略中可以定义多个证书属性的访问控制规则。

【举例】

配置一个名称为 mypolicy 的证书访问控制策略，并进入证书访问控制策略视图。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

【相关命令】

- **display pki certificate access-control-policy**
- **rule**

1.1.27 pki certificate attribute-group

pki certificate attribute-group 命令用来创建证书属性组并进入证书属性组视图。如果指定的证书属性组已存在，则直接进入其视图。

undo pki certificate attribute-group 命令用来删除指定的证书属性组。

【命令】

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

【缺省情况】

不存在证书属性组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name：证书属性组名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

一个证书属性组就是一系列证书属性规则（通过 **attribute** 命令配置）的集合，这些属性规则定义了对证书的颁发者名、主题名以及备用主题名进行过滤的匹配条件。当证书属性组下没有任何属性规则时，则认为对证书的属性没有任何限制。

【举例】

创建一个名为 mygroup 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

【相关命令】

- **attribute**
- **display pki certificate attribute-group**
- **rule**

1.1.28 pki delete-certificate

pki delete-certificate 命令用来删除 PKI 域中的证书。

【命令】

pki delete-certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

ca：表示删除 CA 证书。

local：表示删除本地证书。

peer：表示删除对端证书。

serial *serial-num*：表示通过指定序列号删除一个指定的对端证书。*serial-num* 为对端证书的序列号，为 1～127 个字符的字符串，不区分大小写。在每个 CA 签发的证书范围内，序列号可以唯一标识一个证书。如果不指定本参数，则表示删除本 PKI 域中的所有对端证书。

【使用指导】

删除 CA 证书时将同时删除所在 PKI 域中的本地证书和所有对端证书，以及 CRL。

如果需要删除指定的对端证书，则需要首先通过 **display pki certificate** 命令查看本域中已有的对端证书的序列号，然后再通过指定序列号的方式删除该对端证书。

【举例】

删除 PKI 域 aaa 中的 CA 证书。

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa ca
Local certificates, peer certificates and CRL will also be deleted while deleting the CA certificate.
Confirm to delete the CA certificate? [Y/N]:y
[Sysname]
```

删除 PKI 域 aaa 中的本地证书。

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa local
[Sysname]
```

删除 PKI 域 aaa 中的所有对端证书。

```
<Sysname> system-view
[Sysname] pki delete-certificate domain aaa peer
[Sysname]
```

首先查看 PKI 域 aaa 中的对端证书，然后通过指定序列号的方式删除对端证书。

```
<Sysname> system-view
[Sysname] display pki certificate domain aaa peer
Total peer certificates: 1


Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
Subject  Name: CN=abc
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7
```

【相关命令】

- **display pki certificate**

1.1.29 pki domain

pki domain 命令用来创建 PKI 域，并进入 PKI 域视图。如果指定的 PKI 域已存在，则直接进入 PKI 域视图。

undo pki domain 命令用来删除指定的 PKI 域。

【命令】

pki domain *domain-name*

undo pki domain *domain-name*

【缺省情况】

不存在 PKI 域。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name：PKI 域名，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"”和“'”。

【使用指导】

删除 PKI 域的同时，会将该域相关的证书和 CRL 都删除掉，因此请慎重操作。

【举例】

创建 PKI 域 aaa 并进入 PKI 域视图。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa]
```

1.1.30 pki entity

pki entity 命令用来创建 PKI 实体，并进入 PKI 实体视图。如果指定的 PKI 实体已存在，则直接进入 PKI 实体视图。

undo pki entity 命令用来删除指定的 PKI 实体。

【命令】

pki entity *entity-name*

undo pki entity *entity-name*

【缺省情况】

不存在 PKI 实体。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

entity-name：PKI 实体的名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

在 PKI 实体视图下可配置 PKI 实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。当申请证书时，PKI 实体的信息将作为证书中主题（Subjuct）部分的内容。

【举例】

创建名称为 en 的 PKI 实体，并进入该实体视图。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

【相关命令】

- **pki domain**

1.1.31 pki export

pki export 命令用来将 PKI 域中的 CA 证书、本地证书导出到文件中或终端上。

【命令】

pki export domain *domain-name* **der** { **all** | **ca** | **local** } **filename** *filename*

pki export domain *domain-name* **p12** { **all** | **local** } **passphrase** *p12-key* **filename** *filename*

pki export domain *domain-name* **pem** { { **all** | **local** } [{ **3des-cbc** | **aes-128-cbc** | **aes-192-cbc** | **aes-256-cbc** | **des-cbc** } *pem-key*] | **ca** } [**filename** *filename*]

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

der：指定证书文件格式为 DER 编码（包括 PKCS#7 格式的证书）。

p12：指定证书文件格式为 PKCS#12 编码。

pem：指定证书文件格式为 PEM 编码。

all：表示导出所有证书，包括 PKI 域中所有的 CA 证书和本地证书，但不包括 RA 证书。

ca：表示导出 CA 证书。

local：表示导出本地证书或者本地证书和其对应私钥。

passphrase *p12-key*：指定对 PKCS12 编码格式的本地证书对应的私钥进行加密所采用的口令。

3des-cbc：对本地证书对应的私钥数据采用 3DES_CBC 算法进行加密。

aes-128-cbc：对本地证书对应的私钥数据采用 128 位 AES_CBC 算法进行加密。

aes-192-cbc：对本地证书对应的私钥数据采用 192 位 AES_CBC 算法进行加密。

aes-256-cbc：对本地证书对应的私钥数据采用 256 位 AES_CBC 算法进行加密。

des-cbc：对本地证书对应的私钥数据采用 DES_CBC 算法进行加密。

pem-key：指定对 PEM 编码格式的本地证书对应的私钥进行加密所采用的口令。

filename *filename*：指定保存证书的文件名，不区分大小写。如果不指定本参数，则表示要将证书直接导出到终端上显示，这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

导出 CA 证书时，如果 PKI 域中只有一个 CA 证书则导出单个 CA 证书到用户指定的一个文件或终端，如果是一个 CA 证书链则导出整个 CA 证书链到用户指定的一个文件或终端。

导出本地证书时，设备上实际保存证书的证书文件名称并不一定是用户指定的名称，它与本地证书的密钥对用途相关，具体的命名规则如下（假设用户指定的文件名为 certificate）：

- 如果本地证书的密钥对用途为签名，则证书文件名称为 certificate-signature；
- 如果本地证书的密钥对用途为加密，则证书文件名称为 certificate-encryption；
- 如果本地证书的密钥对用途为通用（RSA/ECDSA/DSA），则证书文件名称为用户输入的 certificate。

导出本地证书时，如果 PKI 域中有两个本地证书，则导出结果如下：

- 若指定文件名，则将每个本地证书分别导出到一个单独的文件中；
- 若不指定文件名，则将所有本地证书一次性全部导出到终端上，并由不同的提示信息进行分割显示。

导出所有证书时，如果 PKI 域中只有本地证书或者只有 CA 证书，则导出结果与单独导出相同。如果 PKI 域中存在本地证书和 CA 证书，则具体导出结果如下：

- 若指定文件名，则将每个本地证书分别导出到一个单独的文件，该本地证书对应的完整 CA 证书链也会同时导出到该文件中。
- 若不指定文件名，则将所有的本地证书及域中的 CA 证书或者 CA 证书链一次性全部导出到终端上，并由不同的提示信息进行分割显示。

以 PKCS12 格式导出所有证书时，PKI 域中必须有本地证书，否则会导出失败。

以 PKCS12 格式导出所有证书时，如果此时本地证书没有匹配的私钥，则导出该本地证书失败。

以 PEM 格式导出本地证书或者所有证书时，若不指定私钥的加密算法和私钥加密口令，则不会导出本地证书对应的私钥信息。

以 PEM 格式导出本地证书或者所有证书时，若指定私钥加密算法和私钥加密口令，且此时本地证书有匹配的私钥，则同时导出本地证书的私钥信息；如果此时本地证书没有匹配的私钥，则导出该本地证书失败。

以 PKCS12 格式或 PEM 格式导出本地证书或者所有证书时，若该本地证书对应的私钥是由加密设备生成的 SM2 密钥对，则导出该本地证书失败。

导出本地证书时，若当前 PKI 域中的密钥对配置已被修改，导致本地证书的公钥与该密钥对的公钥部分不匹配，则导出该本地证书失败。

导出本地证书或者所有证书时，如果 PKI 域中有两个本地证书，则导出某种密钥用途的本地证书失败并不会影响导出另外一个本地证书。

指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会导出失败。

【举例】

导出 PKI 域中的 CA 证书到 DER 编码的文件，文件名称为 cert-ca.der。

```
<Sysname> system-view
[Sysname] pki export domain domain1 der ca filename cert-ca.der
```

导出 PKI 域中的本地证书到 DER 编码的文件，文件名称为 cert-lo.der。

```
<Sysname> system-view
[Sysname] pki export domain domain1 der local filename cert-lo.der
```

导出 PKI 域中的所有证书到 DER 编码的文件，文件名称为 cert-all.p7b。

```
<Sysname> system-view
[Sysname] pki export domain domain1 der all filename cert-all.p7b
```

导出 PKI 域中的 CA 证书到 PEM 编码的文件，文件名称为 cacert。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

导出 PKI 域中的本地证书及其对应的私钥到 PEM 编码的文件，指定保护私钥信息的加密算法为 DES_CBC、加密口令为 111，文件名称为 local.pem。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111 filename local.pem
```

导出 PKI 域中所有证书到 PEM 编码的文件，不指定加密算法和加密口令，不导出本地证书对应的私钥信息，文件名称为 all.pem。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all filename all.pem
```

以 PEM 格式导出 PKI 域中本地证书及其对应的私钥到终端，指定保护私钥信息的加密算法为 DES_CBC、加密口令为 111。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111

*** The general usage local certificate: ***
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
```

```
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIAbfcE+KoYYoCAggA
MBEGBSsOAwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzxHU0rExgn+6cQsK5uK99FPBmy4q9/nnyrooTX8BVlXAjenvgyii
WQLwnIg1IuM8j2aPkQ3wbae1+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvUOCc
/gxdgk97XZSW/0qnOSZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFToixROTxWTtf8SEsKGPDfrEKq3fSTW1xokB8nM
bkRtU+fUiY27V/mr1RHO6+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yxkSi
JdL+X3uEjHnQ/rvnPSKBEU/URwXHxMX9CdCTSqh/SajnrGuB/E4JhOEnS/H9dIM+
DN6iz1IwPFklbcK9KMGwV1bosymXmuEbYCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeEDiHGEMcQU+g0EtfpOLTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BElDVjJq3ioyHSJca8C+3lzcueuAF+lO7Y4Zluq3dqWeuJjE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsV+9IYRYasjzoXE5dhZ5sIPOd
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKywm3Yg+Bgg8Df4bBrFrsH1U0ifmmp
ir2+OuhlC+GbHOxWNeBCa8iAq91k6FGFJ0OLA2oIvhCnh45tM7BjjKTHk+RZdMiA
0TKSWuOyihrwxdUEWh999GKUpkwDHLZJFd21z/kWspqThodEx8ea
-----END ENCRYPTED PRIVATE KEY-----
```

以PEM格式导出PKI域中所有证书到终端，指定保护本地证书对应私钥的加密算法为DES_CBC、加密口令为111。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem all des-cbc 111

 %The signature usage local certificate:
Bag Attributes
```

```
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBfYgwDQYJKoZIhvcNAQELBQAwRTELMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
ZTENMAsGA1UEAwwEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFiczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrlSvAy
cnPaSUko2QbO9sg3ycye1zqpbbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgMDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIvY3Bz
L2Jhc2ljMBEGCWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAwIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIvY2FjZXJ0L2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDAuMTI4L3BraS9wdWIvY3Js
L2NhY3JsLmNybDANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJDTjEU
MBIGA1UECgwLT3BlbkNBIExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTExMDQxODExNDQ0N1oXDTEzMDQxNzExNDQ0N1owRTELMAkGA1UE
BhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2FyZTEN
MAsGA1UEAwwEYWJjZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51bOwjKFUBwxyvOy4D897LmOSedaCyDt6Lvp+PBEHfwWBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2VlcctsYKyvAQapuaThy1tuOcphAB+jQQL9dPoqdk0xp
jvmPDlW+k832Konn9U4dIivS0n+/KMGh0g5UyzHGqUUOo7s9qFuQf5EjQon40TZg
BwUnFYRlvGe7bSQpXjwi8LTyxHPy+dDVjO5CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7ZludNus5vKWTihgx2Qalgb+sqUMwI/WUET7ghO2dRxPUdUbgIYF0saTndKPYd
4oBgl6M0SMsHhe9nF5UCAwEAAaOCAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBBQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAWgBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEEjAQgQ5wa2lAb3BlbmNh
```

```
Lm9yZzAZBgNVHRIEEjAQgQ5wa2lAb3BlbmNhLm9yZzCBgQYIKwYBBQUHAQEEdTBz
MDIGCCsGAQUFBzAChiZodHRwOi8mdcGl0YW4vcGtpL3B1Yi9jYWNlcnQvY2FjZXJ0
LmNydDAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFuOjI1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcGl0YW46ODMwLzA8BgNVHR8ENTAzMDGgL6AthitodHRwOi8vMTky
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcmwuY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0q0SSmvQNfa5ELtRKYF62C/Y8QTLbk6lZDTZuIzN15SGKQcbNM970ffCD
Lk1zosyEVE7PLnii3bZ5khcGO3byyXfluAqRyOGVJcudaw7uIQqgv0AJQ+zaQSHi
d4kQf5QWgYkQ55/C5puOmcMRgCbMpR2lYkqXLDjTIAZIHRZ/sTp6c+ie2bFxi/YT
3xYbO0wDMuGOKJJpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bMfBduwhQWKSoYE
6vZsPGAEisCmAl3dIp49jPgVkixoShraYF1jLsWzJGlzem8QvWYzOqKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAmd1kAPX
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
    localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQ0wMDAbBgkqhkiG9w0BBQwwDgQIcUSKSW9GVmICAggA
MBEGBSsOAwIHBAi5QZM+lSYWPASCAoBKDYulE5f2BXL9ZhI9zWAJpx2cShz/9PsW
5Qm106D+xSj1eAzkx/m4Xb4xRU8oOAuzu1DlWfSHKXoaa0OoRSiOEX1eg0eo/2vv
CHCvKHfTJr4gVSSa7i4I+aQ6AItrI6q99WlkN/e/IE5U1UE4ZhcsIiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP7O2SdLVlUb5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nm114EwPtPMMbHefcuQ6b82y1M+dWfVxBN9K03lN4tZNfPWwLSRrPvjUzBG
dKtjf3/IFdV7/tUMy9JJSpt4iFt1h7SZPcOoGp1ZW+YUR30I7YnFE+9Yp/46KWT8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXralLMYt/4jg4M0jUvoi3GS2Kbo+czsUn
gKgqwYnxVfRSvt8d6GBYrpF2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhvyLkH0UuQE95emXBD/K0HlD73cMrtmogL8F4yS5B2hpIr/v5/
eW35+1QMnJ9FtHFnVsLx9wl9lX8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzxPVfEhO8
5ajQxWlidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsVmr5sk+fRaELD/cwL6VjtXO6x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uiF
RLCfFAwaJMBdIQ6jDQHnpWT67uNDwdEzaPmuTVMme5Woc5zsqE5DY3hWu4oqFdDz
kPLnbX74IZ0gOLki9eIJkVswnF5HkBCKS50ejlW6TgbMNZ+JPk2w
-----END ENCRYPTED PRIVATE KEY-----
```

以 PEM 格式导出 PKI 域中 CA 证书到终端。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB+TCCAWICEQDMbgjRKygg3vpGFVY6pa3ZMA0GCSqGSIb3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMB4XDTExMDMyMjA0NDQyNFoXDTE0MDMyMzA0MzUyNFowPTELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzERMA8GA1UECxMIaDNjLXRlc3QxDTALBgNV
BAMTBDgwNDMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOvDAYQhyc++G7h5
eNDzJs22OQjCn/4JqnNKIdKz1BbaJT8/+IueSn9JIsg64Ex2WBeCd/tcmnSW57ag
dCvNIUYXXVOGca2iaSOElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqwqIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAElm7
W2Lp9Xk4nZVIpVV76CkNe8/C+Id00GCRUUVQFSMvo7Pded76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTFO80aKJGe6NapsfhJHKS+Q7mL0XpXeMONgK+e3dX7rsDxsY7hF+j
0gwsHrjV7kWvwJvDlhzGW6xbpr4DRmdcao19Cr6o=
```

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

导出 PKI 域中 CA 证书到 PEM 编码的文件，指定文件名称为 cacert。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
```

导出 PKI 域中 CA 证书（证书链）到终端。

```
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB7jCCAVcCEQCdSVShJFEMifVG8zRRoSsWMA0GCSqGSIb3DQEBBQUAMDcxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTExMDEwNjAyNTc0NFoXDTEzMTIwMTAzMTMyMFowODELMAkGA1UEBhMC
Y24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ0wCwYDVQQDEwRhYWNhMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcuJsWhAJXEDmowGb5z7VDVms54TKi
xnaNJCWvBOrU64ftvpVB7xQekbkjgAS9FjDyXlLQ8IyIsYIp5ebJr8P+n9i9Pl7j
lBx5mi4XeIldyv2OjfNx5oSQ+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPp6GQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeyiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJsO1hAqMpsCW6G2zh
5mus7FTHhywXpJ22/fnHg61m
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8DCCAVkCEQD2PBUx/rvslNw9uTrZB3DlMA0GCSqGSIb3DQEBBQUAMDoxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEPMA0GA1UEAxMG
cm9mdcGNhMB4XDTExMDEwNjAyNTY1OFoXDTEzMTIwNDAzMTMxMFowNzELMAkGA1UE
BhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQwwCgYDVQQDEwNhY2Ew
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOeklR7DpeEV72N1OLz+dydIDTx0
zVZDdPxF1gQYWSfIBwwFKJEyQ/4y8VIfDIm0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKrB82WZ2mah5Nuekus3LSZZBoZKTAOY5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVVgYBPwVpYglhJDOuIZxKdR2pfQOA4f35wM
Vz6kAujLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iROhJjc1NMV3pvIs
CuFiCLxRQcMGhCNHlOn4wuydssc=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIB8jCCAVsCEFxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwOjELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDaDNjMQ8wDQYDVQQDEwZy
b290Y2EwHhcNMTEwMTA2MDI1MTQxWhcNMTMxMjA3MDMxMjA1WjA6MQswCQYDVQQG
EwJjbjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNoM2MxDzANBgNVBAMTBnJvb3Rj
YTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxP2XLFE230zq6MhwZvAomOxa
7tc1r4bESXZu3UBKno3Ay9kQm2HrDOAizvZXfLu7Gx22ga2Qdz0lIeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHFoG8nS+P7n83BkRj/Fu7Yz4zjTKMbCF2EfhEyXxr4NSXA
fhC9qg9S23vNXStmWvsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBtsU7X77sdZ1Nn
0I98lh0qA5g7SEEIpI+pwZjjrH0FVHw01e4JWhHjyHqrOyfXYqe7vH4SXp5MHEqf
14nKIEbexbPONspebtznxv4/xTjd1aM2rfQ95jJ/SN8H8KIyiYZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pC2ZNiIpg==
-----END CERTIFICATE-----
```

导出 PKI 域中的本地证书及其对应的私钥到 PKCS12 编码的文件，指定保护私钥信息的加密口令为 123，文件名称为 cert-lo.der。

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
```

导出 PKI 域中的所有证书到 PKCS12 编码的文件，指定文件名称为 cert-all.p7b。

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

【相关命令】

- **pki domain**

1.1.32 pki import

pki import 命令用来将 CA 证书、本地证书或对端证书导入到指定的 PKI 域中保存。

【命令】

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：保存证书的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

der：指定证书文件格式为 DER 编码（包括 PKCS#7 格式的证书）。

p12：指定证书文件格式为 PKCS#12 编码。

pem：指定证书文件格式为 PEM 编码。

ca：表示 CA 证书。

local：表示本地证书。

peer：表示对端证书。

filename *filename*：要导入的证书所在的文件名，不区分大小写。如果不指定本参数，则表示要通过直接在终端上粘贴证书内容的方式导入证书，这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

如果设备所处的环境中，没有证书的发布点，或者 CA 服务器不支持通过 SCEP 协议与设备交互，则可通过此命令将证书导入到设备。另外，当证书对应的密钥对由 CA 服务器生成时，CA 服务器会将证书和对应的密钥对打包成一个文件，使用这样的证书前也需要通过此命令将其导入到设备。只有 PKCS#12 格式或 PEM 格式的证书文件中可能包含密钥对。

证书导入之前：

- 需要通过 FTP、TFTP 等协议将证书文件传送到设备的存储介质中。如果设备所处的环境不允许使用 FTP、TFTP 等协议，则可以直接在终端上粘贴证书的内容，但是粘贴的证书必须是 PEM 格式的，因为只有 PEM 编码的证书内容为可打印字符。

- 必须存在签发本地证书（或对端证书）的 CA 证书链才能成功导入本地证书（或对端证书），这里的 CA 证书链可以是保存在设备上的 PKI 域中的，也可以是本地证书（或对端证书）中携带的。因此，若设备和本地证书（或对端证书）中都没有 CA 证书链，则需要首先执行导入 CA 证书的命令。

导入本地证书或对端证书时：

- 如果用户要导入的本地证书（或对端证书）中含有 CA 证书链，则可以通过导入本地证书（或对端证书）的命令一次性将 CA 证书和本地证书（或对端证书）均导入到设备。导入的过程中，如果发现签发此本地证书（或对端证书）的 CA 证书已经存在于设备上的任一 PKI 域中，则系统会提示用户是否将其进行覆盖。
- 如果要导入的本地证书（或对端证书）中不含有 CA 证书链，但签发此本地证书（或对端证书）的 CA 证书已经存在于设备上的任一 PKI 域中，则可以直接导入本地证书（或对端证书）。

导入 CA 证书时：

- 若要导入的 CA 证书为根 CA 或者包含了完整的证书链（即含有根证书），则可以导入到设备。
- 若要导入的 CA 证书没有包含完整的证书链（即不含有根证书），但能够与设备上已有的 CA 证书拼接成完整的证书链，则也可以导入到设备；如果不能与设备上已有的 CA 证书拼接成完成的证书链，则不能导入到设备。

一些情况下，在证书导入的过程中，需要用户确认或输入相关信息：

- 若要导入的证书文件中包含了根证书，且设备上目前还没有任何 PKI 域中有此根证书，且要导入的 PKI 域中没有配置 **root-certificate fingerprint**，则在导入过程中还需要确认该根证书的指纹信息是否与用户的预期一致。用户需要通过联系 CA 服务器管理员来获取预期的根证书指纹信息。
- 当导入含有密钥对的本地证书时，需要输入口令。用户需要联系 CA 服务器管理员取得口令的内容。

导入含有密钥对的本地证书时，系统首先会根据查找到的 PKI 域中已有的密钥对配置来保存该密钥对。若 PKI 域中已保存了对应的密钥对，则设备会提示用户选择是否覆盖已有的密钥对。若 PKI 域中没有任何密钥对的配置，则根据密钥对的算法及证书的密钥用途，生成相应的密钥对配置。密钥对的具体保存规则如下：

- 如果本地证书携带的密钥对的用途为通用，则依次查找指定 PKI 域中通用用途、签名用途、加密用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时用户需要指定一个名称和本地保存的密钥对名称不同的密钥对。
- 如果本地证书携带的密钥对的用途为签名，则依次查找指定 PKI 域中通用用途、签名用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上两种用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时用户需要指定一个名称和本地保存的密钥对名称不同的密钥对。
- 如果本地证书携带的密钥对的用途为加密，则查找指定 PKI 域中加密用途的密钥对配置，并以该配置中的密钥对名称保存密钥对；若加密用途密钥对的配置不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时用户需要指定一个名称和本地保存的密钥对名称不同的密钥对。

由于以上过程中系统会自动更新或生成密钥对配置，因此建议用户在进行此类导入操作后，保存配置文件。

【举例】

向 PKI 域 aaa 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 rootca_pem.cer，证书文件中包含根证书。

```
<Sysname> system-view
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Sysname]
```

向 PKI 域 bbb 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 aca_pem.cer，证书文件中不包含根证书。

```
<Sysname> system-view
[Sysname] pki import domain bbb pem ca filename aca_pem.cer
[Sysname]
```

向 PKI 域 bbb 中导入本地证书，证书文件格式为 PKCS#12 编码，证书文件名称为 local-ca.p12，证书文件中包含了密钥对。

```
<Sysname> system-view
[Sysname] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
******
[Sysname]
```

向 PKI 域 bbb 中通过粘贴证书内容的方式导入 PEM 编码的本地证书。证书中含有密钥对和 CA 证书链。

```
<Sysname> system-view
[Sysname] pki import domain bbb pem local
Enter PEM-formatted certificates.
End with a Ctrl+C on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApybW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGzlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHAth4BiT9v7zetnQqf4q8plfd/
Xqd9zEFlBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiguFPoaDOPia+Pm
```

```
GbRqSyy55clVde5GOccGN1DZ94DW7AypazgLpBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ruO1psxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+dO925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRfE4tkJM7+Uz2QHJOfP10
0VLqMgxMlpk3TvBWgzHGJDe7TdzFCDPMPhod8pi4P8gGXmQd01PbyQ==
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/CN=sldsslserver
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIICjzCCAfigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDE1MDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxzbGRzc2xzZXJ2ZXIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPUytP185JUhbOrVaUDlisZi6NNshcIjd2BAgMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUmoMpEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAgP4MBEGCWCG
SAGG+EIBAQQEAwIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBBQ8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kW474lu4twNzEy5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBzOo8KU=
-----END CERTIFICATE-----
Bag Attributes: <Empty Attributes>
subject=/C=cn/O=ccc/OU=sec/CN=ssl
issuer=/C=cn/O=ccc/OU=sec/CN=ssl
-----BEGIN CERTIFICATE-----
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECxMDc2VjMQwwCgYDVQQDEwNz
c2wwHhcNMDkwNzMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNzZWMxDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAfpXCPIkCAwEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMtYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCxl91+PKM7+i8I/zLcoQO+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBU6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
-----END CERTIFICATE-----


Please input the password:********
Local certificate already exist, confirm to overwrite it? [Y/N]:y
The PKI domain already has a CA certificate. If it is overwritten, local certificates, peer certificates and CRL of this domain will also be deleted.
Overwrite it? [Y/N]:y
```

```
The system is going to save the key pair. You must specify a key pair name, which is a
case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0
to 9, and hyphens (-).
Please enter the key pair name [default name: bbb]:

The key pair already exists.
Please enter the key pair name:
import-key
```

【相关命令】

- **display pki certificate**
- **public-key dsa**
- **public-key ecdsa**
- **public-key rsa**

1.1.33 pki request-certificate

pki request-certificate 命令用来手工申请本地证书或生成 PKCS#10 证书申请。

【命令】

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定证书申请所属的 PKI 域名，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

password *password*：在证书撤销时需要提供的口令，为 1～31 个字符的字符串，区分大小写。该口令包含在提交给 CA 的证书申请中，在吊销该证书时，需要提供该口令。

pkcs10：在终端上显示出 BASE64 格式的 PKCS#10 证书申请信息，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求。

filename *filename*：将 PKCS#10 格式的证书申请信息保存到本地的文件中。其中，*filename* 表示保存证书申请信息的文件名，不区分大小写。

【使用指导】

当 SCEP 协议不能正常通信时，可以通过执行指定参数 **pkcs10** 的本命令打印出本地的证书申请信息（BASE64 格式），或者通过执行指定 **pkcs10 filename** *filename* 参数的本命令将证书申请信息直接保存到本地的指定文件中，然后通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会保存失败。

此命令不会被保存在配置文件中。

【举例】

在终端上显示 PKCS#10 格式的证书申请信息。

```
<Sysname> system-view
[Sysname] pki request-certificate domain aaa pkcs10

*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

手工申请本地证书。

```
[Sysname] pki request-certificate domain openca
Start to request certificate ...
……
Certificate requested successfully.
```

【相关命令】

- **display pki certificate**

1.1.34 pki retrieve-certificate

pki retrieve-certificate 命令用来从证书发布服务器上在线获取证书并下载至本地。

【命令】

pki retrieve-certificate domain *domain-name* { **ca** | **local** | **peer** *entity-name* }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

ca：表示获取 CA 证书。

local：表示获取本地证书。

peer *entity-name*：表示获取对端的证书。其中 *entity-name* 为对端的实体名，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

获取 CA 证书是通过 SCEP 协议进行的。获取 CA 证书时，如果本地已有 CA 证书存在，则该操作将不被允许。这种情况下，若要重新获取 CA 证书，请先使用 **pki delete-certificate** 命令删除已有的 CA 证书与对应的本地证书后，再执行此命令。

获取本地证书和对端证书是通过 LDAP 协议进行的。获取本地证书或对端证书时，如果本地已有本地证书或对端证书，则该操作是被允许进行的。最终，属于一个 PKI 实体的同一种公钥算法的本地证书只能存在一个，后者直接覆盖已有的，但对于 RSA 算法和 SM2 算法的证书而言，可以存在一个签名用途的证书和一个加密用途的证书。

所有获取到的 CA 证书、本地证书或对端证书只有通过验证之后才会被保存到本地证书库中。

此命令不会被保存在配置文件中。

【举例】

从证书发布服务器上获取 CA 证书。（需要用户确认 CA 根证书的指纹）

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

从证书发布服务器上获取本地证书。

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa local
Retrieved the certificates successfully.
```

从证书发布服务器上获取对端证书。

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa peer en1
Retrieved the certificates successfully.
```

【相关命令】

- **display pki certificate**
- **pki delete-certificate**

1.1.35 pki retrieve-crl

pki retrieve-crl 命令用来获取 CRL 并下载至本地。

【命令】

pki retrieve-crl domain *domain-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name：指定 CRL 所属的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

【使用指导】

获取 CRL 的目的是为了验证 PKI 域中的本地证书和对端证书的合法性。若要成功获取 CRL，PKI 域中必须存在 CA 证书。

设备支持通过 HTTP、LDAP 或 SCEP 协议从 CRL 发布点上获取 CRL，具体采用那种协议，由 PKI 域中 CRL 发布点的配置决定：

- 若配置的 CRL 发布点 URL 格式为 HTTP 格式，则通过 HTTP 协议获取 CRL。
- 若配置的 CRL 发布点 URL 格式为 LDAP 格式，则通过 LDAP 协议获取 CRL。若配置的 CRL 发布点 URL（通过命令 **crl url**）中缺少主机名，例如 ldap:///CN=8088,OU=test,U=rd,C=cn，则还需要在 PKI 域中配置 LDAP 服务器的 URL（通过命令 **ldap server**）。此时，设备会将配置的 LDAP 服务器 URL 和配置的 CRL 发布点 URL 中的不完整的 LDAP 发布点拼装成完整的 LDAP 发布点，再通过 LDAP 协议获取 CRL。
- 若 PKI 域中没有配置 CRL 发布点，则设备会依次从本地证书、CA 证书中查找 CRL 的发布点，如果从中查找到了 CRL 发布点，则通过该发布点获取 CRL；否则，通过 SCEP 协议获取 CRL。

【举例】

从 CRL 发布点上获取 CRL。

```
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
Retrieve CRL of the domain aaa successfully.
```

【相关命令】

- **crl url**
- **ldap server**

1.1.36 pki storage

pki storage 命令用来配置证书和 CRL 的存储路径。

undo pki storage 命令用来恢复缺省情况。

【命令】

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

【缺省情况】

证书和 CRL 的存储路径为设备存储介质上的 PKI 目录。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

certificates：指定证书的存储目录。

crls：指定 CRL 的存储目录。

dir-path：存储目录的路径名称，区分大小写，不能以‘/’开头，不能包含“../”。*dir-path* 可以是绝对路径也可以是相对路径，但必须已经存在。

【使用指导】

dir-path 只能是当前主控板上的路径，不能是其它主控板上的路径。（独立运行模式）

dir-path 只能是当前全局主用主控板上的路径，不能是其它主控板上的路径。（IRF 模式）

设备缺省的 PKI 目录在设备首次成功申请、获取或导入证书时自动创建。

如果需要指定的目录还不存在，需要先使用 **mkdir** 命令创建这个目录，再使用此命令配存储路径。若修改了证书或 CRL 的存储目录，则原存储路径下的证书文件（以.cer 和.p12 为后缀的文件）和 CRL 文件（以.crl 为后缀的文件）将被移动到该路径下保存，且原存储路径下的其它文件不受影响。

【举例】

设置证书的存储路径为 flash:/pki-new。

```
<Sysname> system-view
[Sysname] pki storage certificates flash:/pki-new
```

设置 CRL 存储路径为 pki-new。

```
<Sysname> system-view
[Sysname] pki storage crls pki-new
```

1.1.37 pki validate-certificate

pki validate-certificate 命令用来验证证书的有效性。

【命令】

pki validate-certificate domain *domain-name* { **ca** | **local** }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*：指定证书所在的 PKI 域的名称，为 1～31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“"” 和 “'”。

ca：表示验证 CA 证书。

local：表示验证本地证书。

【使用指导】

证书验证的内容包括：证书是否由用户信任的 CA 签发；证书是否仍在有效期内；如果使能了 CRL 检查功能，还会验证证书是否被吊销。如果验证证书的时候，PKI 域中没有 CRL，则会先从本地证

书库中查找是否存在 CRL，如果找到 CRL，则把证书库中保存的 CRL 加载到该 PKI 域中，否则，就从 CA 服务器上获取并保存到本地。

导入证书、申请证书、获取证书以及应用程序使用 PKI 功能时，都会自动对证书进行验证，因此一般不需要使用此命令进行额外的验证。如果用户希望在没有任何前述操作的情况下单独执行证书的验证，可以使用此命令。

验证 CA 证书时，会对从当前 CA 到根 CA 的整条 CA 证书链进行 CRL 检查。

【举例】

验证 PKI 域 aaa 中的 CA 证书的有效性。

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa ca
Verifying certificates......
        Serial Number:
            f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=abc
            OU=test
            CN=aca

Verify result: OK
Verifying certificates......
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Issuer:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca
        Subject:
            C=cn
            O=ccc
            OU=ppp
            CN=rootca

Verify result: OK
```

验证 PKI 域 aaa 中的本地证书的有效性。

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa local
Verifying certificates......
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
```

```
        Issuer:
            C=CN
            O=sec
            OU=software
            CN=bca
        Subject:
            O=OpenCA Labs
            OU=Users
            CN=fips fips-sec

Verify result: OK
```

【相关命令】

- **crl check**
- **pki domain**

1.1.38 public-key dsa

public-key dsa 命令用来指定证书申请使用的 DSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *key-name*：密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length *key-length*：密钥的长度。*key-length* 的取值范围为 512～2048，单位为比特，缺省值为 1024。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA 或 SM2）的密钥对。对于 RSA 和 SM2 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 和 SM2 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 DSA 密钥对为 abc，密钥的长度为 2048 比特。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.39 public-key ecdsa

public-key ecdsa 命令用来指定证书申请使用的 ECDSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *key-name*：密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

secp192r1：密钥对使用的椭圆曲线算法的名称为 secp192r1，密钥长度为 192 比特。

secp256r1：密钥对使用的椭圆曲线算法的名称为 secp256r1，密钥长度为 256 比特。

secp384r1：密钥对使用的椭圆曲线算法的名称为 secp384r1，密钥长度为 384 比特。

secp521r1：密钥对使用的椭圆曲线算法的名称为 secp521r1，密钥长度为 521 比特。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

若未指定任何参数，则缺省使用密钥对 **secp192r1**。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA 或 SM2）的密钥对。对于 RSA 和 SM2 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 和 SM2 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 ECDSA 密钥对为 abc，椭圆曲线算法的名称为 secp384r1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.40 public-key rsa

public-key rsa 命令用来指定证书申请使用的 RSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

encryption：指定密钥对的用途为加密。

name *encryption-key-name*：加密密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

signature：指定密钥对的用途为签名。

name *signature-key-name*：签名密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

general：指定密钥对的用途为通用，既可以用于签名也可以用于加密。

name *key-name*：通用密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length *key-length*：密钥的长度。*key-length* 的取值范围为 512～2048，单位为比特，缺省为 1024。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA 或 SM2）的密钥对。对于 RSA 和 SM2 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 和 SM2 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

分别指定 RSA 签名密钥对和 RSA 加密密钥对时，它们的密钥长度可以不相同。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 RSA 密钥对为 abc，密钥用途为通用，密钥的长度为 2048 比特。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

指定证书申请所使用的加密 RSA 密钥对为 rsa1（密钥的长度为 2048 比特），签名 RSA 密钥对为 sig1（密钥的长度为 2048 比特）。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.41 public-key sm2

public-key sm2 命令用来指定证书申请使用的 SM2 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

public-key sm2 { { **encryption name** *encryption-key-name* | **signature name** *signature-key-name* } * | **general name** *key-name* }

undo public-key

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

encryption name *encryption-key-name*：指定密钥对的用途为加密。*encryption-key-name* 表示加密密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

signature name *signature-key-name*：指定密钥对的用途为签名。*signature-key-name* 表示签名密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

general name *key-name*：指定密钥对的用途为通用，既可以用于签名也可以用于加密。*key-name* 表示通用密钥对的名称，为 1～64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA 或 SM2）的密钥对。对于 RSA 和 SM2 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 和 SM2 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

当 CA 服务器上采用双证书模板时：

- 配置的加密密钥对名称和签名密钥对名称不能相同，否则会导致申请签名证书失败。
- 当未配置加密密钥对时，设备保存加密密钥对会使用 PKI 域名作为其名称，此时签名密钥对名称不要和当前 PKI 域名一致。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定证书申请所使用的 SM2 签名密钥对为 sm21，SM2 加密密钥对为 sm22。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] public-key sm2 signature name sm21 encryption name sm22
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.42 revocation-check method

revocation-check method 命令用来指定证书吊销情况检查的方法。

undo revocation-check method 命令用来恢复缺省情况。

【命令】

revocation-check method *method1* [*method2*]

undo revocation-check method

【缺省情况】

使用 CRL 方法检查证书吊销情况。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

method1 [*method2*]：指定证书吊销情况检查的方法。*method* 取值为：

- **crl**：指定证书吊销时进行 CRL 检查。
- **none**：忽略证书吊销检查。

如果 *method1* 指定为 **none**，则 *method2* 不能再指定 **crl**。

【使用指导】

指定了 **crl** 方法，必须保证 CRL 检查功能处于开启状态（通过 **crl check enable** 命令配置）。如果 CRL 检查功能处于关闭状态，则不进行 CRL 检查，认为所有证书可信。

指定了 **none** 方法，则忽略检查认为所有证书可信，**crl check enable** 命令不生效。

如果同时指定了 **crl** 和 **none** 方法，则先进行 CRL 检查，检查证书是否可信；如果从 CRL 发布点所在的服务器上获取不到 CRL，则使用 **none** 方式，忽略检查认为所有证书可信。

【举例】

配置使用 CRL 方式检查证书吊销情况。

```
<Sysname> system
[Sysname] pki domain abc
```

```
[Sysname-pki-domain-abc] revocation-check method crl
```

【相关命令】

- **crl check enable**

1.1.43 root-certificate fingerprint

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹。

undo root-certificate fingerprint 命令用来恢复缺省情况。

【命令】

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

【缺省情况】

未指定验证 CA 根证书时使用的指纹。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹信息。当选择 MD5 指纹时，*string* 必须为 32 个字符的字符串，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符的字符串，并且以 16 进制的形式输入。

【使用指导】

当本地证书申请模式为自动方式且 PKI 域中没有 CA 证书时，必须通过本命令配置验证 CA 证书时所使用的指纹。当 IKE 协商等应用触发设备进行本地证书申请时，设备会自动从 CA 服务器上获取 CA 证书，如果获取的 CA 证书中包含了本地不存在的 CA 根证书，则设备会验证该 CA 根证书的指纹。此时，如果设备上没有配置 CA 根证书指纹或者配置了错误的 CA 根证书指纹，则本地证书申请失败。

通过 **pki import** 命令导入 CA 证书或者通过 **pki retrieve-certificate** 命令获取 CA 证书时，可以选择是否配置验证 CA 根证书使用的指纹：如果 PKI 域中配置了验证 CA 根证书使用的指纹，则当导入的 CA 证书文件或者获取的 CA 证书中包含本地不存在的 CA 根证书时，直接使用配置的 CA 根证书指纹进行验证。如果配置了错误的 CA 根证书指纹，则 CA 证书导入和 CA 证书获取均会失败；否则，需要用户来确认该 CA 证书的 CA 根证书指纹是否可信。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。

```
<Sysname> system-view
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

【相关命令】

- **certificate request mode**
- **pki import**
- **pki retrieve-certificate**

1.1.44 rule

rule 命令用来配置证书属性的访问控制规则。

undo rule 命令用来删除指定的证书属性访问控制规则。

【命令】

rule [*id*] { **deny** | **permit** } *group-name*

undo rule *id*

【缺省情况】

不存在证书属性的访问控制规则。

【视图】

证书访问控制策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

id：证书属性访问控制规则编号，取值范围为 1～16，缺省值为当前还未被使用的且合法的最小编号，取值越小优先级越高。

deny：当证书的属性与所关联的属性组匹配时，认为该证书无效，未通过访问控制策略的检测。

permit：当证书的属性与所关联的属性组匹配时，认为该证书有效，通过了访问控制策略的检测。

group-name：规则所关联的证书属性组名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

配置证书属性访问控制规则时，可以关联一个当前并不存在的证书属性组，后续可以通过命令 **pki certificate attribute-group** 完成相应的配置。

若规则所关联的证书属性组中没有定义任何属性规则（通过命令 **attribute** 配置），或关联的证书属性组不存在，则认为被检测的证书属性与该属性组匹配。

如果一个访问控制策略中有多个规则，则按照规则编号从小到大的顺序遍历所有规则，一旦证书与某一个规则匹配，则立即结束检测，不再继续匹配其它规则；若遍历完所有规则后，证书没有与任何规则匹配，则认为该证书不能通过访问控制策略的检测。

【举例】

配置一个访问控制规则，要求当证书与证书属性组 mygroup 匹配时，认为该证书有效，通过了访问控制策略的检测。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

【相关命令】

- **attribute**
- **display pki certificate access-control-policy**
- **pki certificate attribute-group**

1.1.45 source

source 命令用来指定 PKI 操作产生的协议报文使用的源 IP 地址。

undo source 命令用来恢复缺省情况。

【命令】

source { **ip** | **ipv6** } { *ip-address* | **interface** *interface-type interface-number* }

undo source

【缺省情况】

PKI 操作产生的协议报文的源 IP 地址为系统根据路由表项查找到的出接口的地址。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip *ip-address*：指定源 IPv4 地址。

ipv6 *ip-address*：指定源 IPv6 地址。

interface *interface-type interface-number*：指定该接口的主 IPv4 地址或接口上最小的 IPv6 地址为源 IP 地址。*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

如果希望 PKI 操作产生的协议报文的源 IP 地址是一个特定的地址，则需要配置此命令，例如 CA 服务器上的策略要求仅接受来自指定地址或网段的证书申请。如果该 IP 地址是动态获取的，则可以指定一个接口，使用该接口上的 IP 地址作为源地址。

此处指定的源 IP 地址，必须与 CA 服务器之间路由可达。

一个 PKI 域中只能存在一个源 IP 地址，后配置的生效。

【举例】

指定 PKI 操作产生的协议报文的源 IP 地址为 111.1.1.8。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip 111.1.1.8
```

指定 PKI 操作产生的协议报文的源 IPv6 地址为 1::8。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 1::8
```

指定 PKI 操作产生的协议报文的源 IP 地址为接口 GigabitEthernet1/0/1 的 IP 地址。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface gigabitethernet 1/0/1
```

指定 PKI 操作产生的协议报文的源 IPv6 地址为接口 GigabitEthernet1/0/1 的 IPv6 地址。

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface gigabitethernet 1/0/1
```

1.1.46 state

state 命令用来配置 PKI 实体所属的州或省的名称。

undo state 命令用来恢复缺省情况。

【命令】

state *state-name*

undo state

【缺省情况】

未配置 PKI 实体所属的州或省的名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

state-name：PKI 实体所属的州或省的名称，为 1～63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所在省为 countryA。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA
```

1.1.47 subject-dn

subject-dn 命令用来配置 PKI 实体的识别名，包括通用名、国家代码、地理区域名称、组织名称、组织部门名称和省份名称参数。

undo subject-dn 命令用来恢复缺省情况。

【命令】

subject-dn *dn-string*

undo subject-dn

【缺省情况】

未配置 PKI 实体的识别名。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

dn-string：PKI 实体的识别名，长度为 1～255 个字符的字符串，不区分大小写。

【使用指导】

PKI 实体识别名的参数格式为：*参数*=*参数值*，多个参数之间以逗号分隔，且可以对同一个参数多次赋值。例如 CN=aaa，CN=bbb，C=cn。PKI 实体识别名支持的参数包括：

- CN：通用名
- C：所属国家代码
- L：所在地理区域名称
- O：所属组织名称
- OU：所属组织部门名称
- ST：所属州省

本命令配置的识别名优先级高于通过 **common-name**、**country**、**locality**、**organization**、**organization-unit** 和 **state** 命令单独配置的识别名。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 PKI 实体 en 的通用名为 test，所属的国家代码为 CN，所属的组织名称为 abc，所属组织部门的名称为 rdtest，所属组织部门的名称为 rstest，所在省为 countryA，所在地理区域的名称为 pukras。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] subject-dn
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

【相关命令】

- **common-name**

- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

1.1.48 usage

usage 命令用来指定证书的扩展用途。

undo usage 命令用来删除指定证书的扩展用途。

【命令】

usage { **ike** | **ssl-client** | **ssl-server** } *

undo usage [**ike** | **ssl-client** | **ssl-server**] *

【缺省情况】

未指定证书的扩展用途，表示可用于 IKE、SSL 客户端和 SSL 服务器端用途。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ike：指定证书扩展用途为 IKE，即 IKE 对等体使用的证书。

ssl-client：指定证书扩展用途为 SSL 客户端，即 SSL 客户端使用的证书。

ssl-server：指定证书扩展用途为 SSL 服务器端，即 SSL 服务器端使用的证书。

【使用指导】

若不指定任何参数，则 **undo usage** 命令表示删除所有指定的证书扩展用途，证书的用途由证书的使用者决定，PKI 不做任何限定。

证书中携带的扩展用途与 CA 服务器的策略相关，申请到的证书中的扩展用途可能与此处指定的不完全一致，最终请以 CA 服务器的实际情况为准。

【举例】

指定证书扩展用途为 SSL 客户端。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] usage ssl-client
```

1.1.49 vpn-instance

vpn-instance 指定注册受理机构服务器和 CRL 发布点所属的 VPN 实例。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

注册受理机构服务器和 CRL 发布点属于公网。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance-name：表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

【举例】

指定注册受理机构服务器和 CRL 发布点所属的 VPN 实例名称为 vpn1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] vpn-instance vpn1
```