证书和密钥技术说明

生成自签名根 CA

生成自签名根证书颁发机构 (CA)。

```
openssl genrsa -out myca.key 2048
# password protect key: openssl genrsa -out myca.key -des3 2048
openssl req -x509 -new -key myca.key -sha384 -days 1825 -out myca.crt \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=SecurityOU/CN=rootca.myorg.com/emailAddress=rootca@myorg.com"
```

此根 CA 必须作为受信任的根 CA 安装在用户（客户端）计算机上

Note 使用 **MacOS** 生成自签名证书不会生成可用于正向和反向代理场景的正确证书。证书必须将 是 *CA* 选项设置为 *True* ， 而使用 MacOS 生成的证书则没有。建议从 多云防御 UI（证书 > 创建 > 生成）或使用 **Linux**生成自签名证书。

生成由您的自签名根 CA 签名的证书

生成由上述根证书颁发机构 (CA) 签名的证书。此证书可在应用中使用。

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA myca.crt -CAkey myca.key -out app1.crt -sha384\
```

```
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

生成由根 CA 签名的中间 CA

如果您不想使用根证书颁发机构 (CA) 对应用证书进行签名，请创建由根 CA 签名的中间 CA，然后使用中间 CA 对应用证书进行签名。将中间证书附加到应用证书。此时，应用 crt 有 2 个证书（作为链）。

```
openssl genrsa -out interca.key 2048
# password protect key: openssl genrsa -out -des3 interca.key 2048
openssl req -new -key interca.key -out interca.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=InterSecurityOU/CN=interca1.myorg.com/emailAddress=interca1@myorg.com"
openssl x509 -req -in interca.csr -CA myca.crt -CAkey myca.key -out interca.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "[SAN]\nbasicConstraints=CA:true")
```

使用中间 CA 签名的应用证书

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA interca.crt -CAkey interca.key -out app1.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

附加文件 app1.crt 和 interca.crt，以创建组合证书并在应用中使用组合证书。根 CA 必须作为受信任的根 CA 安装在客户端计算机上。

在主机上将根 CA 安装为受信任 CA

操作系统	命令
Ubuntu	将 crt 文件复制到 `/usr/local/share/ca-certificates`，运行命令 `sudo update-ca-certificates`。
CentOS	将 crt 文件复制到 `/etc/pki/ca-trust/source/anchors`，运行命令 `sudo update-ca-trust extract`。
Windows	双击该文件并将证书添加到受信任的根，或运行命令 `certutil -addstore "Root"`<crt-file> 。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。