与第三方证书配置示例的安全Cisco Unified CME

目录

简介

许多网络管理员选择实现Cisco Unified Communications Manager Express (CME)以安全。而不是内置的IOS认证机关(IOS-CA)，网络管理员能选择集成与他们的现有公共密钥基础设施(PKI)基础设施的安全CME。本文描述如何配置安全CME运行与安全信令和媒体，通过第三方证书。

先决条件

要求

本文假设， Cisco Unified Communications Manager Express (CME)在您的环境运行和功能完备的。 一定是可操作的在Secure Cisco Unified CME的所有电话需要能成功首先注册到CME。 关于如何配置CME的信息，参考Cisco Unified Communications Manager Express系统管理员指南。

本文也假设，语音和安全功能启用。

使用的组件

本文档中的信息根据Cisco Unified Communications Manager Express (CME)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

配置

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

概略的配置步骤

1. 创建IOS-CA实例。
2. 创建信任点有第三方CA证书。
3. 生成证书签名请求(CSR)从信任点。
4. 签署与服务器验证使用情况的CSR，并且获取CA证明。
5. 验证与CA证书的信任点，并且导入各自身份证书。
6. 验证第三方证书信任点。
7. 创建IOS CA CME信任点。
8. 配置证书信任列表(CTL)客户端。
9. 配置认证机关代理功能(CAPF)服务器。
10. 配置电话服务。
11. 配置测试电话。
12. 验证。

详细配置示例

1. 创建IOS-CA实例。IOS-CA实例生产使用签署电话的局部重要的证书的自签名证书(LSC)。

```
crypto key gen rsa label ios-ca mod 2048
The name for the keys will be: ios-ca
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 17 seconds)

crypto pki server ios-ca
database level complete
grant auto
lifetime cert 7305
exit
ip http server
crypto pki trust ios-ca
enrollment url http://10.2.3.4:80
revo none
rsakey ios-ca
exit
crypto pki server ios-ca
no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: Cisco123
Re-enter password: Cisco123
% Certificate Server enabled.
exit
```

2. 创建将生成第三方签字的CSR的信任点。 这些信任点最终有第三方CA证书，以及身份证书，是CSR的结果。

```
crypto key generate rsa label tac-sast mod 2048
The name for the keys will be: tac-sast
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 52 seconds)

crypto pki trust tac-sast
enroll term
serial-number none
fqdn none
ip-address none
subject-name CN=tac-sast
revo none
rsakeypair tac-sast
exit
```

3. 生成从信任点的CSR。**crypto pki登记**提供给第三方CA签字的命令生产CSR。

示例 1：

```
crypto pki enroll tac-sast
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=tac-sast
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
MIICfjCCAWYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFO
V7SdNOfjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fcO9sdxfRqi8jEf
UbndH9yZit912wX14nxC2Wa2S3O/p6vXEwKfQMGZe4nO7SJPtJ/vNHx/HNCkJxHV
H1V0JH7Affffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4IB
AQB++utK7EpeGYYyPfNALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtSl
H7jRey4ew9GZVTeqq7cxwz1f7d6ZP4BRqzp1f0HVvu7HC+bAR0jB2FNvVaN27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnq
TwbMF4998BXmlPIQigJBInACY2SUszqcDih7Nc1Y6viYaSiN0ZCuzEyKI2tjbwUU
EU/o0fcWMXsnBc44WQBAEpTBSLYFVb4kGl9AgAyOW7q9ACiBTpmul1kwuDyTPg5X
fCIWUjVfTWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

示例 2：

```
crypto pki enroll tac-sast
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=tac-sast
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
MIICfjCCAWYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFO
V7SdNOfjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fcO9sdxfRqi8jEf
UbndH9fffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffHNCkJxHV
H1V0JH7AwWLdnUgEWGoSFOL5j/lwIHmemUDpSuL9IY+9EP622E0CAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4IB
AQB++utK7EpeGYYyPfNALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtSl
H7jRey4ew9GZVTeqq7cxwz1f7d6ZP4BRqzp1f0HVvu7HC+bAR0jB2FNvVaN27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnq
```

```
TwbMF4998BXmlPIQigJBInACY2SUszqcDih7Nc1Y6viYaSiN0ZCuzEyKI2tjbwUU
EU/o0fcWMXsnBc44WQBAEpTBSLYFVb4kGl9AgAyOW7q9ACiBTpmul1kwuDyTPg5X
fCIWUjVfTWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

4. 请使用两CSR为了生成与服务器验证权限的证书。
   注意： 重要的是全双工证书链为两证书之一得到从CA。 证书链提供CA和身份证书从签署的CA。保证证书在base64格式下载。按该顺序重要的是非常CA证书使用每信任点的验证，并且身份证书导入到每信任点。
5. 验证与CA证书的信任点，并且导入SAST身份证书。

   示例 1：

```
crypto pki auth tac-sast
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIFQTCCBCmgAwIBAgIQUt2XjpaAwaJIEkcOebj7AjANBgkqhkiG9w0BAQUFADBs
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAg
BgoJkiaJk/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3Vu
Z3RhLWNhc2VydmVyMB4XDTEyMDgxMzE1NTczM1oXDTE3MDgxNDE2MDY0M1owbDET
MBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmSJomT8ixkARkWBWNpc2NvMSIwIAYK
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYWluMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNxJJpgY2yE8CjBsL4H
eryNvcvUFeA90kXbEncl1uoI7t1JEf5ifQBopqGO54E0t1YUHrcT5LgXdBU839yp
lNm9VtFfffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffo45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc14lYuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxE
aXN0cmliffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffyLmp5b3Vu
Z3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNl
cnZlci5jcmwwEgYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUWjZQ
/W2X5GoSeibbuvAKHH8/97MwDQYJKoZIhvcNAQEFBQADggEBAI8nivQcicltdXnt
X30+QO+FKK0Cu6WWFIozqKE0eeSJ0C3fPv88jjkae4+YjF/gK2wPt/mezWeQm0MO
S4m0LHnMMZGU7ezAHTd+yh5oWI2Q2iBFnslvSIUboJZazNkDEFm7Dl8gDKajEvE/
JUNtebgOJPJUXvV/v0Rpry1Nckxrn3tsiCF62acgAZke1hSrscoeqzkygk8vIr1K
lv9W2Vy2TPa6i8ZWG8at36jAsNAk5HJUEl7mFyirMIJcc+diZ12WPoRqrQ+CE7ZL
Mw+ydSS5x0XvFqily0VE649TsvtKCOMkJjbLLX8wZp9SU2AgXutHr3CdlrVlaElC
ZW4J3cQ=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint MD5: C198A185 83575520 EBE6E03D 33BA9B2C
Fingerprint SHA1: B0A9668D 42D36311 E82B0A33 480127B5 BEB02B60
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported


crypto pki import tac-sast cert
% The fully-qualified domain name will not be included in the certificate
Enter the base 64 encoded certificate.
```

```
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIGpzCCBY+gAwIBAgIKGdhyPgABAAABpDANBgkqhkiG9w0BAQUFADBsMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAgBgoJkiaJ
k/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3VuZ3RhLWNh
c2VydmVyMB4XDTEyMDgyOTEzMzIyOVoXDTE0MDgyOTEzMzIyOVowGDEWMBQGA1UE
AxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFOV7SdNOfjoXCRpqCZwFavR82/Wuko
ho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE10Qk9YHpBzLAcNEvRWvnyVnMaBSc6
Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM8swgaomqlAj8LbmYE/PQdtfxOEne
IF1FHHXj4fffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffWa2S3O/
p6vXEwKfQMGZe4nO7SJPtJ/vNHx/HNCkJxHVH1V0JH7AwWLdnUgEWGoSFOL5j/lw
IHmemUDpSuL9IY+9EP622E0CAwEAAaOCA50wggOZMA4GA1UdDwEB/wQEAwIFoDAd
BgNVHQ4EFgQUtP6NbC/kpe3uSa2oeZy9rTDGMHAwHwYDVR0jBBgwFoAUsuXXNeJW
LhdYasmJ260ABz7CElswggGYBgNVHR8EggGPMIIBizCCAYegggGDoIIBf4aB2Wxk
YXA6Ly8vQ049anlvdW5ndGEtY2FzZXJ2ZXIoMSksQ049anlvdW5ndGEtY2FzZXJ2
ZXIsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2Vz
LENOPUNvbmZpZ3VyYXRpb24sREM9anlvdW5ndGEtbGFiZG9tYWluLERDPWNpc2Nv
LERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xh
c3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGWWh0dHA6Ly9qeW91bmd0YS1jYXNlcnZl
ci5qeW91bmd0YS1sYWJkb21haW4uY2lzY28uY29tL0NlcnRFbnJvbGwvanlvdW5n
dGEtY2FzZXJ2ZXIoMSkuY3JshkZodHRwOi8vanlvdW5ndGEtY2FzZXJ2ZXIuY2lz
Y28uY29tL0NlcnRFbnJvbGwvanlvdW5ndGEtY2FzZXJ2ZXIoMSkuY3JsMIIBcQYI
KwYBBQUHAQEEggFjMIIBXzCBxAYIKwYBBQUHMAKGgbdsZGFwOi8vL0NOPWp5b3Vu
Z3RhLWNhc2VydmVyLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWfffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffLWxhYmRvbWFp
bixEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNz
PWNlcnRpZmljYXRpb25BdXRob3JpdHkwgZUGCCsGAQUFBzAChoGIaHR0cDovL2p5
b3VuZ3RhLWNhc2VydmVyLmp5b3VuZ3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2Vy
dEVucm9sbC9qeW91bmd0YS1jYXNlcnZlci5qeW91bmd0YS1sYWJkb21haW4uY2lz
Y28uY29tX2p5b3VuZ3RhLWNhc2VydmVyKDEpLmNydDAhBgkrBgEEAYI3FAIEFB4S
AFcAZQBiAFMAZQByAHYAZQByMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3
DQEBBQUAA4IBAQCayeYa7pauRGAgGPHmAHQt6iiqBsS+uVwArgO1u0HEjs4EkPm8
xQZNexVBOmGyzTwlwjpD8jTDIO1AEWP67b/gB2xViktVqvaVfKfMR+3cxODoTUNJ
DbMKR7tOyLrfv+7hNVcsKlAo+XpohVKdP4XOPXeEquYrTmzInsB55PtMxJ7qnYU6
29kJUZdVQZUjZSy4dVhtVYVO9Gmj5XIkzUneS4QC7N/3CXGZQilH11PzulUvAAFh
h2o6c7QgKtHGxOwrkXuPl6+GN4mV+uFXh1B5DTEXG7/yJNNE2yNN+Flb05yLcyEA
Y0p/cksKkNhpRDh+YNT1uHa0AjY8fa1AJqpp
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

示例 2：

```
crypto pki auth tac-cme
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIFQTCCBCmgAwIBAgIQUt2XjpaAwaJIEkcOebj7AjANBgkqhkiG9w0BAQUFADBs
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAg
BgoJkiaJk/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3Vu
Z3RhLWNhc2VydmVyMB4XDTEyMDgxMzE1NTczM1oXDTE3MDgxNDE2MDY0M1owbDET
MBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmSJomT8ixkARkWBWNpc2NvMSIwIAYK
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYWluMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNxJJpgY2yE8CjBsL4H
eryNvcvUFfffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffU839yp
lNm9VtF+MXC0L7dIpu1XRT7/lJgLDAI5alZg5wW6zC9xrgNS88cR1o45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
```

```
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc14lYuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffjUkxE
aXN0cmlidXRpb25Qb2ludIZWaHR0cDovL2p5b3VuZ3RhLWNhc2VydmVyLmp5b3Vu
Z3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNl
cnZlci5jcmwwEgYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUWjZQ
/W2X5GoSeibbuvAKHH8/97MwDQYJKoZIhvcNAQEFBQADggEBAI8nivQcicltdXnt
X30+QO+FKK0Cu6WWFIozqKE0eeSJ0C3fPv88jjkae4+YjF/gK2wPt/mezWeQm0MO
S4m0LHnMMZGU7ezAHTd+yh5oWI2Q2iBFnslvSIUboJZazNkDEFm7Dl8gDKajEvE/
JUNtebgOJPJUXvV/v0Rpry1Nckxrn3tsiCF62acgAZke1hSrscoeqzkygk8vIr1K
lv9W2Vy2TPa6i8ZWG8at36jAsNAk5HJUEl7mFyirMIJcc+diZ12WPoRqrQ+CE7ZL
Mw+ydSS5x0XvFqily0VE649TsvtKCOMkJjbLLX8wZp9SU2AgXutHr3CdlrVlaElC
ZW4J3cQ=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint MD5: C198A185 83575520 EBE6E03D 33BA9B2C
Fingerprint SHA1: B0A9668D 42D36311 E82B0A33 480127B5 BEB02B60
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

crypto pki import tac-cme cert
% The fully-qualified domain name will not be included in the certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIGpjCCBY6gAwIBAgIKGdmLjgABAAABpTANBgkqhkiG9w0BAQUFADBsMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAgBgoJkiaJ
k/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3VuZ3RhLWNh
c2VydmVyMB4XDTEyMDgyOTEzMzM0MVoXDTE0MDgyOTEzMzM0MVowFzEVMBMGA1UE
AxMMam9jYXNhbGUtY21lMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uVz/50eRaTmlnvOKRFp9ZcZuqw3We6DVqsBMuTpQg0Bg/VQTgCa9NFD8LW2UXGO8
YFANV8ABVn9q/1TET6Fg5YbcTePsd5/lNlL1zpSHiAtBuwfGzKKiMgZJ1XFYeb9p
heqpTj2d22CoghFQnKbRUOPpjfPcElFq07/z5m7blEkAmsAQh2y+bIH5T7UNdgtf
smLqWZMqIsMEvNEi3gbkPUTatmZlgFac1TXvxyIIv95rIeqs07WZXn0GsgkNsO3i
CjcFY1UXxxYV5Wg/uPQlFnbRpTefd5Ms253Dm9Ey2E8v+E3HsOfn0JvpY4vIkKz2
KDesetXsIOw747tf1wXHmQIDAQABo4IDnTCCA5kwDgYDVR0PAQH/BAQDAgWgMB0G
A1UdDgQWBBR8xG8ZaDVcquSU+0n40KSH+7SmSDAfBgNVHSMEGDAWgBSy5dc14lYu
F1hqyYnbrQAHPsISWzCCAZgGA1UdHwSCAY8wggGLMIIBh6CCAYOgggF/hoHZbGRh
cDovLy9DTj1qeW91bmd0YS1jYXNlcnZlcigxKSxDTj1qeW91bmd0YS1jYXNlcnZl
cixDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28s
REM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
cz1jUkffffffffffffffffffffffffffffffffffffffffffffffffffffcDovL2
p5b3VuZ3RhLWNhc2VydmVy
Lmp5b3VuZ3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0
YS1jYXNlcnZlcigxKS5jcmyGRmh0dHA6Ly9qeW91bmd0YS1jYXNlcnZlci5jaXNj
by5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNlcnZlcigxKS5jcmwwggFxBggr
BgEFBQcBAQSCAWMwggFfMIHEBggrBgEFBQcwAoaBt2xkYXA6Ly8vQ049anlvdW5n
dGEtY2FzZXJ2ZXIsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENO
PVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9anlvdW5ndGEtbGFiZG9tYWlu
LERDPWNpc2NvLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9
Y2VydGlmaWNhdGlvbkF1dGhvcml0eTCBlQYIKwYBBQUHMAKGgYhodHRwOi8vanlv
dW5ndGEtY2FzZXJ2ZXIuanlvdW5ndGEtbGFiZG9tYWluLmNpc2NvLmNvbS9DZXJ0
RW5yb2xsL2p5b3VuZ3RhLWNhcffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffFpbi5jaXNj
by5jb21fanlvdW5ndGEtY2FzZXJ2ZXIoMSkuY3J0MCEGCSsGAQQBgjcUAgQUHhIA
VwBlAGIAUwBlAHIAdgBlAHIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcN
AQEFBQADggEBAHNVNEMcys1z4sXGiI2jZzT5Nt/q8dLl4LCJ2iZkmS3F8tG14UEf
```

```
C/e28VWavV4piIXK4FuZKB1iltOo9MZAGH9PvVEO+yG8zpeIcwOgDq951qJejeBA
+N+ryCFy5TEbiMF3pw1XjdbBAProJ1s1Q0QcjoigPNtPyqRfehdlhMUo4NgC/svX
5VZSfxpagaBhdpUNVYo2s0ujXujuI/aTRpbDan2h7n27tMMBtDcocpQgPv6txDoR
b+Qb8CPZt3IvuEXAru4cRv1O1jYUWlY59ta5uELSnA+2WA36PiMxIyLu67W1RI05
1rFcBOmIQ8vTpqyNp8/TFOpOSnQMO30w9Fs=
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

6. 一旦CA和身份证书装载到各自信任点，请验证每信任点的证书链。此步骤保证上一个步骤顺利地完成。

```
crypto pki cert validate tac-cme
Chain has 2 certificates
Certificate chain for tac-cme is valid

crypto pki cert validate tac-sast
Chain has 2 certificates
Certificate chain for tac-sast is valid
```

7. 创建IOS CA CME信任点。

   由于IOS-CA信任点不可能用于客户端验证(传输级安全性(TLS)连接用电话)，您在它必须创建另一信任点和放置IOS-CA证书。

   此信任点用于只授权IP电话的要求TLS连接(因此他们能适当地注册)。

```
crypto pki trust ios-ca-cme
enroll url http://10.2.3.4:80
revo none
rsakey ios-ca
exit

crypto pki auth ios-ca-cme
Certificate has the following attributes:
Fingerprint MD5: 0120A3AB 44155DF9 091F31BF C3E26B80
Fingerprint SHA1: 90F9DDDE 20A792B5 3693A065 8BDAD50E 588E011C
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

8. 配置CTL客户端。

```
ctl-client
server capf 10.2.3.4 trust tac-cme
server cme-tftp 10.2.3.4 trust tac-cme
sast1 trust tac1-cme
sast2 trust tac-sast
regenerate
```

   Note:保证CTL文件顺利地创建：

```
do sh flash | iCTL
58 8642 Aug 29 2012 13:57:22 +00:00 CTLFile.tlv
```

9. 配置CAPF服务器。

```
capf-server
auth-mode null-string
cert-enroll-trust ios-ca pass 0 null
```

```
trustpoint-label tac-cme
source-addr 10.2.3.4
end
```

10. 配置电话服务。

```
confi t
Enter configuration commands, one per line. End with CNTL/Z.
telephony-service
secure-signaling trust tac-cme
tftp-server-credentials trust tac-cme
server-security-mode secure
cnf-file perphone
device-security-mode encrypted
exit
```

11. 配置测试电话(ephone)为了升级其证书和使用加密的模式。

```
ephone 1
capf-ip-in-cnf
cert-oper upgrade auth-mode null
device-security-mode encrypted
telephony-service
cre cnf
Creating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
end
```

一旦配置完成，重置电话并且等待它注册。

Note:在电话重置前，请保证已经没有安全配置存在。如果安全配置存在，必须手工删除或在注册之前完成测试电话的出厂重置获取Cisco Unified CME。

要重置电话，请执行这些命令：

```
confi t
ephone 1
reset
end
```

一旦电话接收更新LSC， CERT**操作升级验证模式空字符串**命令删除。

```
do sh run | sec ephone
ephone 1
device-security-mode encrypted
mac-address ABCD.ABCD.ABCD
type 7960
capf-ip-in-cnf
button 1:1
sh ephone
```

12. 验证电话注册与验证和加密。

```
sh ephone
ephone-1[0] Mac:ABCD.ABCD.ABCD TCP
socket:[2] activeLine:0 whisperLine:0
REGISTERED in SCCP ver 11/9
max_streams=0 + Authentication + Encryption with TLS connection
mediaActive:0 whisper_mediaActive:0
startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0 caps:8
IP:10.2.3.10 * 51685 Telecaster 7960
keepalive 4 max_line 6 available_line 6
button 1: cw:1 ccw:(0 0)
dn 1 number 2090 CH1 IDLE CH2 IDLE
```

```
      Preferred Codec: g711ulaw
      Lpcor Type: none
```

安全Cisco Unified CME应该是功能完备的与第三方证书。

相关信息

- Cisco Unified Communications Manager Express 系统管理员指南
- 在Cisco TAC维基的安全语音
- 技术支持和文档 - Cisco Systems