Configuring Support for 4096 Key Pair

RSA-4096 is an encryption system that offers enhanced security to protect your data during transmission. From Cisco IOS XE 17.14.1a, Cisco VG400 Voice Gateway and Cisco VG420 Voice Gateway support 4096 key pair with SHA256 hash function during a TLS handshake process.

Cisco VG420 Voice Gateway and Cisco VG400 Voice Gateways, via Signaling Connection Control Protocol (SCCP), use TLS to secure the signaling channel to CUCM and SRST. As a default, Cisco IOS XE devices support 2048 RSA key encryption for TLS handshake process. For enhanced security and protection during data transmission, you can enable 4096 key pair with SHA256 hash function for these two voice gateways.

Note Currently, Cisco VG400 Voice Gateway supports up to 8 FXS ports and Cisco VG420 Voice Gateway supports up to 144 ports for the TLS handshake process.

Configuring 4096 Key Pair Support

During a TLS session, certificate authentication and key exchange are critical. During certificate authentication, the client verifies the server's digital certificate to ensure it is valid and whether it is issued by a trusted Certificate Authority (CA). This step confirms the server's identity. Key exchange is then established, where the client and server negotiate and agree upon keys that will be used for encryption and decryption of data during the TLS session.

During a TLS session, all the STCAPP-based FXS ports of the voice gateways are enabled for a short period of time, for example, during a shut/no shut or boot up period. When you configure the 4096 key pair, these FXS ports securely interface with the CUCM.

To configure 4096 key pair, perform the following steps:

1. Create a new key pair.
2. Associate a trustpoint with this keypair.
3. Authenticate the certificate by a CA Server.

For detailed information on each of these steps, see Configuring and Managing a Certificate Server.

Create a New Key Pair

The following is the sample configuration to create a new RSA-4096 key pair.

```
vg400# crypto key generate rsa exportable general-keys label 4k_keypair modulus 4096
The name for the keys will be: 4k_keypair
% The key modulus size is 4096 bits
% Generating crypto RSA keys in background ...
```

Create a Trustpoint and Associate with the Key Pair

The following is the sample configuration to create a trustpoint and associate it with the keypair you've already created. The enrollment URL is the CA server whose keypair was created in the above-mentioned sample configuration.

```
vg400(config)# crypto pki trustpoint 4k_keypair
vg400(ca-trustpoint)# enrollment url http://10.75.167.250:80
vg400(ca-trustpoint)# serial-number none
vg400(ca-trustpoint)# fqdn none
vg400(ca-trustpoint)# ip-address none
vg400(ca-trustpoint)# subject-name cn=6c:03:09:ac:f9:80
vg400(ca-trustpoint)# revocation-check none
vg400(ca-trustpoint)# hash sha256
vg400(ca-trustpoint)# rsakeypair 4k_keypair
vg400(ca-trustpoint)# end
```

Authenticate the Certificate by a CA Server

The following is a sample configuration to authenticate the CA certificate.

```
vg400(config)# crypto pki authenticate 4k_keypair
Certificate has the following attributes:
      Fingerprint MD5: 7BD20233 A5078333 8CC8C7C5 DAE614EC
      Fingerprint SHA1: B452068C CD39D071 046EEED6 5B0424F6 2439D5BE
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
vg400(config)#crypto pki enroll 4k_keypair
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration.
 Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: cn=6c:03:09:ac:f9:80
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose 4k_keypair' command will show the fingerprint.
```

Verifying Support for 4096 Key Pair

After configuring the 4096 key pair, use the following show commands to verify the configuration.

1. **show crypto key**

```
vg400# show crypto key mypubkey rsa 4k_keypair
% Key pair was generated at: 22:20:02 UTC Feb 19 2024
Key name: 4k_keypair
Key type: RSA KEYS      4096 bits
 Storage Device: private-config
 Usage: General Purpose Key
 Key is exportable. Redundancy enabled.
 Key Data:
  30820222 300D0609 2A864886 F70D0101 01050003 82020F00 3082020A 02820201
  00CF7270 D5B4A356 69B55B18 0CEA4927 6CEC9A48 0B191804 72D316CE 97A97BA8
  37F5690B B3A169B9 6E2A12F8 5595435A 8FA2AE7F BD7996ED 3C406EA4 266C9542
  A3ACE221 9943AB27 9B16397E FA438E7C D9D95689 B9F8F508 CC38CDD1 C7F56489
  0FB3A18C F90066A5 42AE9F36 A1FA29BD 7A70A7A9 A0C96C8B 543A6217 C1B9D751
  682BEF3A 84B82045 9C2A9C22 0D6005E8 3F30DA9B 67F1BE1F F366813F 65B8F2DC
  AC48E6B4 65DFCFCA F19C6522 F2C25089 D59706CB E03D0C87 5912A26E B4DCE624
  4FCE6D8A FA4333BE F7C40A0D F2CB0D5C 73A66587 664BF192 FEAB5EE1 86081679
  390CF73D 5A11E3C9 B43FCC50 B5478885 B938EBD9 09FDB453 779F8F3E 5E168BCA
  6F7F896B 6A0D941C E087E667 C9CE41CB 029FD40E 31099EBE F2BD5706 8C9E40BF
  1CD432AA 71A91FB4 12388ED9 4C8552F3 B5DFF37C D6EDA7E6 59DDC0EB FD24496D
  F3D1ED6B 6CD17100 502BFEE2 2AFC8707 E32329EF 41E6FBDB 0094D82D 044C78F0
  6F03583E 04D979B6 317B19EB FB1155A9 6F2D9F64 4C99D779 45FCD19F C767177F
  886C4D7F 4E9B39BB 16027A40 D99E1575 AA160CB4 E039BB6D 6C60DAA2 228C0C2D
  492D0BF9 5EF083DC F2ADE958 78F5361D 0502B89A C50D5FFF A4E57865 B8E872C6
  BE6D2630 78C94D06 3D23D46A 5B6E5AEA E9355ADB 7206CD5D A405B996 3834F5D6
  65CE5BEB FE4B6345 7984C4A9 2E302E37 055DC42A 325C6B80 C12820CC BE6233D5
  31020301 0001
```

The highlighted line in the above output displays the 4096 key type, implying a successful configuration.

2. **show pki certificates**

```
vg400# show crypto pki certificates verbose 4k_keypair
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 00DC
  Certificate Usage: General Purpose
  Issuer:
    cn=CA-4k.labtest.com
  Subject:
    Name: 6c:03:09:ac:f9:80
    cn=6c:03:09:ac:f9:80
  Validity Date:
    start date: 06:35:09 UTC Feb 20 2024
    end   date: 08:48:45 UTC Aug 12 2033
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 5C2556ED 55BA2D9C 47CE2668 B1927DF7
  Fingerprint SHA1: 42CD404B 43BF7AD0 AD516F90 565087D4 04277F15
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: 6B466F52 A518B5E7 902DAFA7 658D15FE 57B2E541
```

```
    X509v3 Authority Key ID: 4773C5C3 A4161090 7442B558 62713E6B 744857F6
    Authority Info Access:
  Cert install time: 22:35:39 UTC Feb 19 2024
  Associated Trustpoints: 4k_keypair
  Key Label: 4k_keypair
  Key storage device: private config

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CA-4k.labtest.com
  Subject:
    cn=CA-4k.labtest.com
  Validity Date:
    start date: 08:48:45 UTC Aug 15 2023
    end   date: 08:48:45 UTC Aug 12 2033
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 7BD20233 A5078333 8CC8C7C5 DAE614EC
  Fingerprint SHA1: B452068C CD39D071 046EEED6 5B0424F6 2439D5BE
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 4773C5C3 A4161090 7442B558 62713E6B 744857F6
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 4773C5C3 A4161090 7442B558 62713E6B 744857F6
    Authority Info Access:
  Cert install time: 13:56:18 UTC Feb 6 2024
  Associated Trustpoints: 4k_keypair TP_IP6 4k
  Storage: nvram:CA-4klabtest#1CA.cer
```

The highlighted portions in the above-mentioned sample output indicate successful 4096 key pair configuration.