Replacing the VSOM Login Certificate

Note that this process is not officially supported by Cisco, and you make these modifications at your own risk. The Cisco quality assurance team does not test product operation after such modifications have been made to the system. However, this process has been verified in Cisco TAC labs, and used by customers that needed to replace the default SSL certificate and key with one of their own.

Author: Sean Merrow

This document assumes that you already have a certificate and private key available to use for your VSOM login. To get to this point, you should have done the following:

1. Generated a private key
2. Used this private key to generate a CSR (Certificate Signing Request)
3. The CSR should have been signed by a trusted CA (Certificate Authority) such as Verisign. Once a CSR is signed by a trusted CA, it is now a certificate

Your certificate will look something like what you see below:

```
-----BEGIN CERTIFICATE-----
MIIC9zCCAmCgAwIBAgIDEAACMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYDVQQGEwJV
UzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czETMBEGA1UEBxMKQm94Ym9yb3VnaDEO
MAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8GA1UEAxMIU2FtcGxlQ0Ex
ITAfBgkqhkiG9w0BCQEWEnNhbXBsZWNhQGNpc2NvLmNvbTAeFw0wNzExMDIxMjI0
NDNaFw0xMjEwMzAxMjI0NDNaMHUxCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1NYXNz
YWNodXNldHRzMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMQ8wDQYDVQQD
EwZTZXJ2ZXIxHzAdBgkqhkiG9w0BCQEWEHNlcnZlckBjaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKBk5a2neweUSoTRyylOFjvDHOqt7PpIvT4c
LbwPRhw9WK4Seiefha6/l3wGZotgKaeFML8Uy16ZQ4MH0Ka/PrIgfEPwx1qglq7H
Q6DSJgV9D5RqT4Km4myKCd1N5QhOpXn2Cwq/go+m05iUvSVTRYeVlno8KgWqJH6I
kHFreL3VAgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5T
U0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBQ9rKxjPiFRI70bYcCN
WUh3Uoc7JzAfBgNVHSMEGDAWgBRZgKEbqymLN25RE/h2slb723sbbTANBgkqhkiG
9w0BAQUFAAOBgQCpfZQYViwtvEdWIBl7ZItvAFrf2zYHABChT858nqqmikOCX0Z9
Kg7plWasYx1jft+7d299wg4XAjxtl8kJHKQhIHeGnnD261OgP6U08IaGsWtetPoA
r3ROu1yyxN3ZDBkYfZDeJy326kir/AFCq7LXwIWSzlj+pBBh+WVb+jq24w==
-----END CERTIFICATE-----
```

The private key, if not encrypted, will look something like what you see below:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQCgZOWtp3sHlEqE0cspThY7wxzqrez6SL0+HC28D0YcPViuEnon
n4Wuv5d8BmaLYCmnhTC/FMtemUODB9Cmvz6yIHxD8MdaoJaux0Og0iYFfQ+Uak+C
puJsigndTeUITqV59gsKv4KPptOYlL0lU0WHlZZ6PCoFqiR+iJBxa3i91QIDAQAB
AoGABMoehan7pYVLGF4/Z9NaHJy971AURIEJjaI/x17ZZBx82m3Y0fgUgNxdxKlY
RI8xjzwN8ZbIX+HJv07rbx9E2va9O/1Ep9vbpn4obR3xngZo+f8UpCTPBFyhavCo
o+I3GD89pe06gtiMdCcPmK0dzK7p4tLxqdlZWTbAt5cxRR0CQQDLq0gKNP7Z9Qrb
YxqqIJ8CAEaTl9tL6/z0ULqikG+WKuQq/KNl4g/bGBbtaiXWiKhZlbe4Ouy7ZySS
66Iowm3bAkEAyZsf8G3YX3wNHqSTc2diB41apqA1fVhkYY7O8HRQI3x8oiAsG7IE
sYff5u6RgvRc2hSteg8sbAg7uoaMCOlKDwJAAhqZ2ukjPNMoMo36h4lgux+PmxS1
gjpE2a0/0FAXpwB4bO1BLts/+K5uBjPTgjzVKF/AjxmkumbdXNssSKmBgwJATIYh
PXW0Z6oCoNr/TRK01wEEo7K0GvvuPkmiqwq7UHz0IeXsWCbeOTTF/DYZ7Ycrp2up
3WbdCbSmV0qy5L8IaQJAO2a60HfXcI2BXfCOLsGsxINtFzL60MJVdlHz0ktnZqlU
AfUO0DQwtRahMy1/Qx1doQhmBrGu0e87CxtreCyR4g==
-----END RSA PRIVATE KEY-----
```

You will need to place these files on the VSOM server in the **/usr/BWhttpd/conf** directory. The example in this document will assume the new certificate and key files are named **server.crt** and **server.key**, respectively.

If the private key was not already encrypted, you will need to encrypt it using 3-DES encryption with the following command. This will take the private key called **server.key** and encrypt it using the 3-DES encryption algorithm, using the password **password123**, and call the new encrypted key file **server-key.3des:**

```
openssl rsa -des3 -passout pass:password123 -in server.key -out server-key.3des
```

Your encrypted private key should now look something like the following output. Notice that it shows that the key is now encrypted using 3-DES. It can only be accessed now with the password used when encrypting it.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,34EED1361F014B7A

DmE6Gt506LrJKclbWxH6w8USYbcNvktMu/egHldPDKZNocTpIdmcRJfLN2WbvkPl
bXCLdqt7yTGMrYKr8Xc7Xu0vYKhuGqN6UI89hO2QzhYRZqEUY730qKqH3ntGZkmg
XYTcjFroSll/oYT+4JM8o1xzSIWLnvbrTSVRbgAQ6u7fiw5aB4Rukc9aWjnel1pq
dPHwBsfq8A3HQBqOBMEI7rMPO+maGs59r6w9AaNcQFlTOsC1i7EkdVwT/JNBdrY7
ps9OJaU12ahlJnaP2n4DqHMyQXSVmBReVdiFWTM13V4Kv6XhJwiDcPrW8KhS+hJx
maC879+HrZMIn38VLSJDF47Aj9yJSJf+FOHdTmGpVey0lyF8WqUkbcpY6GHidoyU
Zyf2G55QkJr7eQxeDBRfgX4cQl4ebORXerxYbtJiz/V0BQhmtkmsGpkaQ+F4WJNz
I+K5yiDWG6HFacxbw7JdhgVJ3jZncb31m+Yh0HblBF12J1YbAO5qY/Nos2Rn32/L
9xyx7UVznRuY4T+d/xUDI5bFvzMjlMJxUE0tkZsMGnredO7cRdbe4qbpklNV8WUD
XetE31QZRv0ST2bYGCRdp+QRVqr4MrSAjWOCKnHfJqTXvK5kuzLF1xgfildKot1o
Ac7koMAH6UcuVTFdfO8gdMGcjjsqMid6ybJ4UjA4iTQAUYsytrejct9jVa5fUUE9
Q1tcEBiSNUVH3hFfMC2vLQbQerqHZuz92KYIPWc8zXNhdFup+RkEPwwQvZIzH8gV
pL2zZmI3j759vUJegjymRhnlVqPAugzTIuTDGXlgs0k=
-----END RSA PRIVATE KEY-----
```

Now it is time to create a single file that has both the certificate and encrypted key. You can do this with the following command. Make sure that the certificate is listed first:

```
cat server.crt server-key.3des > vsom-certkey.pem
```

You can now use the following command to see your new file containing both the certificate and encrypted private key:

```
bxb-vsm:/usr/BWhttpd/conf # cat vsom-certkey.pem
```

And it should look something like this:

```
-----BEGIN CERTIFICATE-----
MIIC9zCCAmCgAwIBAgIDEAACMA0GCSqGSIb3DQEBBQUAMIGOMQswCQYDVQQGEwJV
UzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czETMBEGA1UEBxMKQm94Ym9yb3VnaDEO
MAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8GA1UEAxMIU2FtcGxlQ0Ex
ITAfBgkqhkiG9w0BCQEWEnNhbXBsZWNhQGNpc2NvLmNvbTAeFw0wNzExMDIxMjI0
NDNaFw0xMjEwMzAxMjI0NDNaMHUxCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1NYXNz
YWNodXNldHRzMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMQ8wDQYDVQQD
EwZTZXJ2ZXIxHzAdBgkqhkiG9w0BCQEWEHNlcnZlckBjaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKBk5a2neweUSoTRyylOFjvDHOqt7PpIvT4c
LbwPRhw9WK4Seiefha6/l3wGZotgKaeFML8Uy16ZQ4MH0Ka/PrIgfEPwx1qglq7H
Q6DSJgV9D5RqT4Km4myKCd1N5QhOpXn2Cwq/go+m05iUvSVTRYeVlno8KgWqJH6I
kHFreL3VAgMBAAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5T
U0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBQ9rKxjPiFRI70bYcCN
WUh3Uoc7JzAfBgNVHSMEGDAWgBRZgKEbqymLN25RE/h2slb723sbbTANBgkqhkiG
9w0BAQUFAAOBgQCpfZQYViwtvEdWIBl7ZItvAFrf2zYHABChT858nqqmikOCX0Z9
Kg7plWasYx1jft+7d299wg4XAjxtl8kJHKQhIHeGnnD261OgP6U08IaGsWtetPoA
r3ROu1yyxN3ZDBkYfZDeJy326kir/AFCq7LXwIWSzlj+pBBh+WVb+jq24w==
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,34EED1361F014B7A

DmE6Gt506LrJKclbWxH6w8USYbcNvktMu/egHldPDKZNocTpIdmcRJfLN2WbvkPl
bXCLdqt7yTGMrYKr8Xc7Xu0vYKhuGqN6UI89hO2QzhYRZqEUY730qKqH3ntGZkmg
XYTcjFroSll/oYT+4JM8o1xzSIWLnvbrTSVRbgAQ6u7fiw5aB4Rukc9aWjnel1pq
dPHwBsfq8A3HQBqOBMEI7rMPO+maGs59r6w9AaNcQFlTOsC1i7EkdVwT/JNBdrY7
ps9OJaU12ahlJnaP2n4DqHMyQXSVmBReVdiFWTM13V4Kv6XhJwiDcPrW8KhS+hJx
maC879+HrZMIn38VLSJDF47Aj9yJSJf+FOHdTmGpVey0lyF8WqUkbcpY6GHidoyU
Zyf2G55QkJr7eQxeDBRfgX4cQl4ebORXerxYbtJiz/V0BQhmtkmsGpkaQ+F4WJNz
I+K5yiDWG6HFacxbw7JdhgVJ3jZncb31m+Yh0HblBF12J1YbAO5qY/Nos2Rn32/L
9xyx7UVznRuY4T+d/xUDI5bFvzMjlMJxUE0tkZsMGnredO7cRdbe4qbpklNV8WUD
XetE31QZRv0ST2bYGCRdp+QRVqr4MrSAjWOCKnHfJqTXvK5kuzLF1xgfildKot1o
Ac7koMAH6UcuVTFdfO8gdMGcjjsqMid6ybJ4UjA4iTQAUYsytrejct9jVa5fUUE9
Q1tcEBiSNUVH3hFfMC2vLQbQerqHZuz92KYIPWc8zXNhdFup+RkEPwwQvZIzH8gV
pL2zZmI3j759vUJegjymRhnlVqPAugzTIuTDGXlgs0k=
-----END RSA PRIVATE KEY-----
```

Now that you have a file containing your certificate and encrypted private key, you can edit the **mediaout.xml** file which gives the system the necessary information to use the file during the HTTPS login.

First, you should make a copy of the original file. The following command will make a copy of **mediaout.xml** called **mediaout.xml.old**:

```
bxb-vsm:/usr/BWhttpd/conf # cp mediaout.xml mediaout.xml.old
```

Now you can use **vi** to edit the original **mediaout.xml** file. You will need to change the value of **default-keyfile** to point to your new certificate and key file. You'll also need to change the **default-password** value to the password you used when encrypting your private key.

Below is an example of what your mediaout.xml file will look like when you're finished.

```
bxb-vsm:/usr/BWhttpd/conf # cat mediaout.xml
<mediaout>
       <keyfile-dir>/usr/BWhttpd/conf</keyfile-dir>
       <default-keyfile>vsom-certkey.pem</default-keyfile>
       <default-password>password123</default-password>
       <httphost>
        <port>80</port>
        <proxyport>9090</proxyport>
        <sslport>443</sslport>
       </httphost>
       <rtsphost>
        <port>554</port>
        <rtpports></rtpports>
       </rtsphost>

</mediaout>
```

The only thing left is to restart the Cisco services, then test out your HTTPS login to verify the VSOM server sends your own certificate instead of the self-signed certificate generated at install time.

```
bxb-vsm:/usr/BWhttpd/conf # /etc/init.d/cisco restart
```

In the event that this causes any problems, or you simply want to roll back your changes for any reason, simply enter the following two commands, and you'll be back to where you started:

```
bxb-vsm:/usr/BWhttpd/conf # mv mediaout.xml.old mediaout.xml

bxb-vsm:/usr/BWhttpd/conf # /etc/init.d/cisco restart
```