Use certreq & certutil to request and approve a cert request as the same user

learn.microsoft.com/en-us/answers/questions/431223/use-certreq-certutil-to-request-and-approve-a-cert

Mike Bruno 136 Reputation points
Jun 11, 2021, 3:11 AM

I am working on a "break glass" process by which our certificate managers can create certificates on behalf of customers in the event that our RA is offline. In this use case, the certificate template has the "CA Manager Approval" check box enabled. The account peforming the task is requesting a cert against this template and also has the "Manage Certificates" permission on the CA.

Step 1: Create a certreq policy file
I created a very simple INF file as I'm leaning on the certificate template to dictate most of the aspects of the issued certificate. Here's what my policy file looks like:

```
[Version]
Signature = "$WindowsNT$"

[NewRequest]
Subject = "CN=miketest.fabricam.com,OU=29727 - PKI Engineering"
Exportable = TRUE
KeyLength = 2048

[RequestAttributes]
CertificateTemplate=TestTemplate

[Extensions]
2.5.29.17  = "{text}"
_continue_ = "dns=miketest.fabricam.com&"
```

Step 2: Generate the certificate request

```
certreq.exe -new -q -config "caserver.fabricam.com\Fabricam Issuing CA" policy.inf
request.csr
```

After running this command, I'm making the assumption that a public/private keypair has been generated in my account profile, & that it will be there when I'm ready to associate the issued certificate with it.

Step 3: Submit the certificate request

```
certreq.exe -submit -q -config "caserver.fabricam.com\Fabricam Issuing CA"
request.csr response.cer cert.p7b response.ful
```

So my assumption about the output files here are:

- response.cer is supposed to be the Base64 encoded leaf certificate, but we won't get that since the cert request will enter pending state rather than being issued
- cert.p7b is supposed to be the leaf certificate with the full chain attached
- response.ful is supposed to be the fully fleshed-out response from the CA.

Here's where it gets interesting. Whereas when I request against a template where no approval is necessary, response.ful is a pretty detailed file, in this case, I get what looks to be a very small (maybe 1024-bit key) Base64-encoded certificate. As part of my troubleshooting, I tried to get certutil to dump the contents of the cert, but it indicates that it's not a properly-formatted certificate file. Oh well, moving on...

**Step 4: Approve the certificate request **
From the output of the -submit command, I have the request Id which was taken under submission. Since I happen to have the *Manage Certificates* permission on the CA, I now use certutil to "approve" that certificate request:

```
certutil.exe -config "caserver.fabricam.com\Fabricam Issuing CA" -resubmit 12345
```

Step 5: Retrieve the CA response
After step 2 (submit) I didn't receive a valid certificate in the CA response since the cert was not yet issued. So, instead, I need to use a roundabout method to obtain the public certificate from the CA. To do this, I use a certutil -view command:

```
certutil.exe -config "caserver.fabricam.com\Fabricam Issuing CA" -view -restrict
"requestid=12345" -out rawcertificate
```

The output of this command contains the fully-formed Base64-encoded leaf certificate along with some other junk that we just have to programmatically filter out. I save the filtered contents as "response.cer". If I use certutil or OpenSSL to inspect this file, it definitely contains the properly-formed certificate. So, now all that's left is to create an association between this certificate and the keypair I generated in step 2 with certreq -new, right? ....Right?

Step 6: Accept the CA Response

```
certreq.exe -accept -user response.cer
```

This command *appears* to work, however, there's no output in either standard out or standard error. Odd, but ok.

Step 7: Locate the certificate in the cert store
This is where we fail. Even though the certreq -accept command appeared to work, the issued certificate is nowhere to be found in my cert store.

I'm guessing that there is something simple that I'm missing here, but I'm not sure what.

Thanks in advance!