

2K3 Cert Svcs gives invalid policy error on OpenSSL gen'd cert req

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-06/msg00007.html>

- *From:* matt.kerr@xxxxxxxxxx
 - *Date:* Mon, 04 Jun 2007 17:56:52 -0000
-

Hello Microsoft security gurus,

I'm currently trying to test a PKI architecture system where I have an OpenSSL-based UNIX SSL client and server and a Windows Server 2003 Standard Edition with Certificate Services for the CA. If I generate a PKCS #10 PEM and use the COM Interop in C# to submit and retrieve the requested certificate programmatically, I can only get the error:

"The certificate has invalid policy. 0x800b0113"

"Error Constructing or Publishing Certificate Resubmitted by <DOMAIN/USER>"

Where <DOMAIN/USER> is a local Administrator for the CA box logged in locally and using the C# program to submit the request file off a USB drive to the Certificate Services, then retrieve the issued certificate into a file on the USB drive.

If I generate PKCS#10 request files using the COM Interop with XEnroll then I can get the certificates to issue properly, but never with the OpenSSL generated ones.

The OpenSSL generated ones look like, using the command:

```
openssl req -noout -text -inform pem -in <file>.p10
```

Data:

Version: 0 (0x0)

Subject: CN=<Fully qualified hostname>

Subject Public Key Info: Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

<snip>

Exponent: 17

Attributes:

Requested Extensions:

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

2K3 Cert Svcs gives invalid policy error on OpenSSL gen'd cert req

X509v3 Key Usage:

Digital Signature, Non Repudiation, Key Encipherment

Signature Algorithm: sha1WithRSAEncryption

<snip>

The snipped bits are the hex outputs of the binary portions.

I've tried several different things such as changing the Subject to use just the hostname, adding/removing "critical" from the extended and regular key usage flags, adding/removing a CA=FALSE flag, removing all regular key usage flags and just have the extended flags, etc.

Nothing seemed to make any difference, although once I had a different error relating to an ASN1 tag value being invalid.

.