

## Re: 3rd party cert vs self signed

---

*Source:*

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.setup/2008-10/msg00032.html>

---

- *From:* "Elan Shudnow" <[SubstituteThisWithMyFirstName@xxxxxxxxxxx](mailto:SubstituteThisWithMyFirstName@xxxxxxxxxxx)>
  - *Date:* Thu, 2 Oct 2008 20:38:32 +0000
- 

Another thing is, depending on the CA, you can request a NetBIOS name in your certificate. This should allow you to use your 3rd party certificate for SMTP. Also, if you have an internal CA, you should be able to request a PKI cert and use that for SMTP.

--  
Elan Shudnow  
<http://www.shudnow.net>

"Elan Shudnow" <[SubstituteThisWithMyFirstName@xxxxxxxxxxx](mailto:SubstituteThisWithMyFirstName@xxxxxxxxxxx)> wrote in message [news:#Ihzq2MJJHA.1160@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:#Ihzq2MJJHA.1160@xxxxxxxxxxxxxxxxxxxxxxxx):

I'm not an MVP, but hey, I'll give it a shot anyways!

All you need to do is disable the 3rd party certificate from doing SMTP. You can do "Enable-ExchangeCertificate -Thumbprint thumbprinthere -Services None" and then do another "Enable-ExchangeCertificate -Thumbprint thumbprinthere -Services ServicesotherthanSMTP." You can then use your self-signed certificate and enable it for anything you want really. I would just choose SMTP. But even if you enabled the other services, as I stated, the PKI cert will have a higher precedence.

So yes, certs can co-exist. It just depends on what services are enabled on them and order of precedence. Since SMTP will be disabled on the PKI cert, it will still see SMTP enabled on the self-signed cert and use that.

--  
Elan Shudnow  
<http://www.shudnow.net>

"John Oliver, Jr. [MVP]" <[jcoliverjr@xxxxxxxxxxx](mailto:jcoliverjr@xxxxxxxxxxx)> wrote in message [news:#IIFHtMJJHA.4280@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:#IIFHtMJJHA.4280@xxxxxxxxxxxxxxxxxxxxxxxx):

Re: 3rd party cert vs self signed

> Daniel,  
>  
> I don't think this is possible without renaming your domain but the other  
> MVP's may chime in with a different solution. I always recommend naming  
> internal domain with .local suffix to avoid this scenario.  
>  
> --  
> John Oliver, Jr  
> MCSE, MCT, CCNA  
> Exchange MVP 2009  
> Microsoft Certified Partner  
>  
> "Daniel Lund" <spaz@xxxxxxxxxxxx> wrote in message  
> [news:F8A8151D-9EAA-4BB4-8318-0481B11EEB41@xxxxxxxxxxxxxxxxxxx](mailto:news:F8A8151D-9EAA-4BB4-8318-0481B11EEB41@xxxxxxxxxxxxxxxxxxx)  
>  
  
>> I originally posted this so I could be assured of my fallback position  
>> should  
>> something go horribly wrong. Since installing the 3rd party cert  
>> something  
>> has happened, not horribly wrong but annoying. I posted it with a subject  
>> of  
>> "Can PKI and Self signed certs coexist" which no one has replied to so  
>> I'll  
>> include it here since it's related to this thread:  
>>  
>> So we obtained a 3rd party UC certificate for our external domain name  
>> (call  
>> it external.com) and installed it on our Exchange 2007 transport server  
>> and  
>> enabled it for all services. Now my Exchange clients in Outlook 2007 get a  
>> certificate error that the internal FQDN for the transport server is not  
>> on  
>> the certificate. Which makes sense. So I went to add the internal AD  
>> domain  
>> name (call it internal.com) to the UC certificate. Problem is internal.com  
>> is  
>> an internet domain name registered to someone else, so I'll never get a  
>> certificate for it. How to eliminate the error for my Exchange clients.  
>> The  
>> self signed cert is still installed. Would I be able to remove SMTP from  
>> the  
>> 3rd party cert and enabled it on the self signed cert? If that's even  
>> possible  
>> would it solve the problem?  
>> Thanks in advance,  
>> -Dan  
>>  
>>  
>> "Elan Shudnow" wrote:

Re: 3rd party cert vs self signed

>>  
>

>>> Yep, I'll agree to this as well. If you have a PKI cert and remote  
>>> users, I have no idea why you'd go back to a self-signed cert.

>>>  
>>> --

>>> Elan Shudnow  
>>> <http://www.shudnow.net>

>>>  
>>>  
>>>

>>> "John Oliver, Jr. [MVP]" <jcoliverjr@xxxxxxxxxxxx> wrote in message  
>>> [news:OeHIP12IJHA.3424@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OeHIP12IJHA.3424@xxxxxxxxxxxxxxxxxxxxxxxx):

>>>  
>

>>>> It was just a wild guess!

>>>>  
>>>> --

>>>> John Oliver, Jr  
>>>> MCSE, MCT, CCNA  
>>>> Exchange MVP 2008  
>>>> Microsoft Certified Partner

>>>>

>>>> "Martin Blackstone [MVP]" <martinb@xxxxxxxxxxxx> wrote in message  
>>>> [news:O6utXs2IJHA.4600@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:O6utXs2IJHA.4600@xxxxxxxxxxxxxxxxxxxxxxxx)

>>>>  
>

>>>>>

>>>>> "Andy David {MVP}" <adavid@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
>>>>> message [news:49g5e4p7ck7fm83b1jr07fm1hmv1pvjuru@xxxxxxxx](mailto:news:49g5e4p7ck7fm83b1jr07fm1hmv1pvjuru@xxxxxxxx)

>>>>>  
>

>>>>>> On Tue, 30 Sep 2008 16:09:53 -0400, "John Oliver, Jr. [MVP]"  
>>>>>> <jcoliverjr@xxxxxxxxxxxx> wrote:

>>>>>>  
>>>>>>

>

>>>>>>> Yes, I do not know why one would go back to the default Exchange  
>>>>>>> cert

>>>>>>> from

>>>>>>> 3rd party SAN if they have remote users unless they do not have any  
>>>>>>> remote

>>>>>>> users at some point or they decide to use a VPN Client would be my  
>>>>>>> best

>>>>>>> guesses.

>>>>>>>

Re: 3rd party cert vs self signed

>>>>>>

>>>>

>

>>>>>> Yea, I cant imagine thats a common scenario!

>>>>>>

>>>>>

>

>>>>>> Yea!

>>>>

>

>>>>