

## Re: SBS 2003 Premium and Cert Services

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-02/3296.html>

---

**From:** MCSEGURU (*mcseguruhere\_at\_aol.com*)

**Date:** 02/10/05

Date: Wed, 9 Feb 2005 20:45:44 -0500

Well I certainly agree that you don't want to expose a DC to the net, but that philosophy got blown out of the equation when SBS included Exchange OWA into the package. Agreeing that adding the amount of available services to a public web-server (regardless of the fact that it's an internal DC/File Server/etc...) will always increase your risks, we are again talking about a "Small Business Server" which is MS claim as to why the risk of exposing the OWA isn't a HIGH security risk.

Hackers typically go after things they want, and Small Business environments, don't typically offer much.

That all being said, and accepting that an SBS environment is a constant tug-of-war between security and TCO (Total Cost of Ownership), installing the Certificate Server on another server, if it's available would be preferred.

Now, moving onto certificates. The scenario you outlined in your post [Chad] is typical for host certificate publishing, but I thought the [original post] request was how to integrate user certificates for single sign-on from anonymous computers anywhere on the net. Doesn't that require a challenge-authenticate approach to a CA server for each user session to be accepted without requiring authentication everytime"on top of the host - client SSL session "?

"tester" <tester@testthis.net> wrote in message  
news:110kabihqa5oga1@corp.supernews.com...

> *thanks for the explanation Chad.*

> *SO, in summary, you do not recommend putting it on the SBS server, but*

> *rather on a separate server, and one that is not a file server or an*

> *exchange server. What about a sharepoint portal server that also hosts*

> *other web sites internal and external? Would that be a satisfactory*

> *place?*

> *An I will spend the money for sure.*

>

>

>

> *"Chad A Gross [SBS-MVP]" <chad.gross@laytonflower.nospam.com> wrote in*

> message news:ueqtgxmDFHA.4020@TK2MSFTNGP14.phx.gbl...  
>> (I'm using 'you' in a generic sense here – not referring to you  
>> (MCSEGURU) specifically ;^)  
>>  
>> Well, that is the preferred setup as far as the Certificate Services  
>> configuration is concerned – and you absolutely, positively don't want  
>> to expose Certificate Services to the web when it's running on an SBS.  
>> Due to security concerns, public-facing Certificate Servers should not be  
>> a DC, or an Exchange server, or a file server, or all of these rolled up  
>> into one.  
>>  
>> Now, you could get around this by either manually distributing your CA  
>> Cert, or you could edit the properties of your Certification Authority to  
>> include a different public URL where the CA Cert lives, then upload the  
>> CA Cert to that location. This still doesn't keep the process as  
>> streamlined as it normally should be – but you don't have to manually  
>> distribute the CA Cert either. The thing is that foreign users will not  
>> be able to install any certs you create until they trust you as a CA,  
>> which requires installing your CA Cert. So for example, if a foreign  
>> user browsed to an SSL-encrypted web site that was using an SSL Cert you  
>> created, they'd get a security warning indicating that the certificate  
>> was issued by a company they haven't chosen to trust. The user would  
>> have to view the certificate, then go to the certification path, select  
>> the CA (you) and view that certificate (which would open the CA Cert  
>> uploaded to the public URL). The foreign user could then install the CA  
>> Cert, adding you as a trusted CA, return to the SSL certificate and  
>> install the SSL cert, then continue to the encrypted page.  
>>  
>> And just think – for \$100 you could purchase a cert from a trusted root  
>> CA which means that no one would have to install anything – it's all  
>> verified in the background without any user intervention . . . Which  
>> makes for happy customers & partners :^)  
>>  
>> --  
>> Chad A. Gross [SBS-MVP]  
>>  
>> **SBS ROCKS!!!**  
>>  
>> "MCSEGURU" <mcseguhere@aol.com> wrote in message  
>> news:urwpmmbmDFHA.2824@tk2msftngp13.phx.gbl...  
>>> Additionally,  
>>>  
>>> Please correct me if I'm wrong, I don't claim to be the "be all end all"  
>>> expert on much of anything. Technology changes way too fast for me to  
>>> keep up in every market.  
>>>  
>>> You may have to publish your Cert SVR (ie. to the web) in order for it  
>>> to issue User Certs for each session on the fly. I think when using  
>>> certs for authentication the session verifies the user, and then creates  
>>> a session cert based upon successful authentication of the user combined  
>>> with the machine id (ie. user and the hardware or node) upon session

>>> negotiation. But, I could be way off here, I think there are multiple  
>>> ways of implementing certificates for encryption and authentication.  
>>>  
>>> Maybe others know more about other ways of implementing this.  
>>>  
>>>  
>>> "Chad A Gross [SBS-MVP]" <chad.gross@laytonflower.nospam.com> wrote in  
>>> message news:OhLiLpkDFHA.1936@TK2MSFTNGP14.phx.gbl...  
>>>> It doesn't cost – but if you don't purchase a root CA cert, it's going  
>>>> to be a PITA. You mention secure email as an example. In order to do  
>>>> this, you're going to have to distribute your self-created root CA cert  
>>>> to everyone in addition to any certs you create. The remote users can  
>>>> trust you (as a root CA) and the certs you issue, but it's not as  
>>>> straight-forward as it would be otherwise.  
>>>>  
>>>> Not to mention that most corporate use policies will prohibit trusting  
>>>> a self-created root CA cert . . . And certs are coming way down in  
>>>> price, which makes it harder to justify being your own CA and the  
>>>> support issues involved with it. One example:  
>>>>  
>>>> Cheap SSL Certificate:  
>>>> <http://www.digicert.com/digid.html>  
>>>>  
>>>> And I think I've even seen somewhere offering certs for under \$50 – but  
>>>> I can't remember where I saw it . . . :^)  
>>>>  
>>>> --  
>>>> Chad A. Gross [SBS-MVP]  
>>>>  
>>>> SBS ROCKS!!!  
>>>>  
>>>> "tester" <tester@testthis.net> wrote in message  
>>>> news:110i5g89vpgpf45@corp.supernews.com...  
>>>>> that's what I thought, so there is no real issue loading cert svcs on  
>>>>> the sbs then right?  
>>>>> I'm going untrusted for now. but in development we want to mess with  
>>>>> mapping users to certs for other applications, secure email using  
>>>>> certs, etc. since it would not cost us to implement this then it was  
>>>>> looked at as an alternative for now.  
>>>>>  
>>>>> "MCSEGURU" <mcseguruhere@aol.com> wrote in message  
>>>>> news:OEDix4gDFHA.3648@TK2MSFTNGP10.phx.gbl...  
>>>>>> Do you care if your certs are "trusted" by your remote computers? If  
>>>>>> so, do you intend on installing your root CA cert on their computers,  
>>>>>> or will you purchase a root CA cert from a trusted Root CA? If you  
>>>>>> are considering purchasing a root CA cert from a trusted Root CA, you  
>>>>>> might be better off (cost wise) to purchase a certificate solution  
>>>>>> from a provider. Trusted Root CA certificates can be expensive.  
>>>>>>  
>>>>>> If however, you take the no cost route, and have all your remote  
>>>>>> users install your "un-trusted" root CA on all their remote

>>>>> computers, you may be able to issue user certs for single sign on.  
>>>>>  
>>>>>  
>>>>>  
>>>>> "tester" <tester@testthis.net> wrote in message  
>>>>> news:110hvhltlhg5hf70@corp.supernews.com...  
>>>>> Thanks Mariana for the response,  
>>>>> I know that SBS creates it's own but it isn't just certs for SBS, I  
>>>>> want it (the CA) to issue certs for tother servers, for users, etc.  
>>>>> That is why I figured I'd load it on my main server. Since that is  
>>>>> an SBS box I thought I'd look for some more expert opinion.  
>>>>>  
>>>>> "Marina Roos [SBS-MVP]" <marina@roos.nodontwantspam.nl.com> wrote in  
>>>>> message news:%237KYsagDFHA.148@TK2MSFTNGP14.phx.gbl...  
>>>>>> Hi,  
>>>>>>  
>>>>>> SBS doesn't need the certificate services as it creates its own  
>>>>>> certificate.  
>>>>>> Just run the CEICW wizard.  
>>>>>>  
>>>>>> --  
>>>>>> Regards,  
>>>>>>  
>>>>>> Marina  
>>>>>> Microsoft SBS-MVP  
>>>>>> One of the Magical M&M's  
>>>>>>  
>>>>>> "tester" <tester@testthis.net> schreef in bericht  
>>>>>> news:110htlf4jds2u6b@corp.supernews.com...  
>>>>>>> I am thinking of loading certificate services on my sbs premium  
>>>>>>> server  
>>>>>>> (with  
>>>>>>> ISA on it and a HDW firewall in front of it) to issue my own certs  
>>>>>>> for  
>>>>>>> sharepoint single sign on and for Outlook as well as for some  
>>>>>>> other  
>>>>>>> internal  
>>>>>>> applications. Anything I need to look out for before? anyone have  
>>>>>>> a how  
>>>>>>> to  
>>>>>>> or is it simply add it then configure?  
>>>>>>>  
>>>>>>> I want to set it up as the top level ca for the  
>>>>>>> domain/organization. Am I  
>>>>>>> better off loading it on another server? I have a server that  
>>>>>>> will host  
>>>>>>> sharepoint portal and a few other web sites, internal and  
>>>>>>> external, as  
>>>>>>> well  
>>>>>>> as lcs 2005 so I guess I could put it there. Ideas? Opinions?  
>>>>>>> Never really had CS loaded so am just toying with the idea at the

