

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices.enhancements/2005-09/>

- *From:* "William Stacey [MVP]" <staceyw@xxxxxxxx>
 - *Date:* Thu, 22 Sep 2005 14:57:30 -0400
-

If you use SCT (recommended) it goes something like this:

- 1) Session key exchange using Certs to exchange and verify identities. I think you can demand client also has cert.
- 2) Both sides now have a SecurityContextToken which includes the SKey and the SCT ID and expire datetime.
- 3) Server caches the SCT using SCTID is unique id.
- 4) Client signs/encrypts future messages with the SCT.
- 5) Server receives message and looks up SCT via ID and verifies the message signature using the SKey it knows for that SCTID. If bad, exception.
- 6) Client can continue to use SCT without handshake until SCT expires. Then needs to do SCT exchange again.

—

William Stacey [MVP]

<jason.chen@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:O13W2X6vFHA.3000@xxxxxxxxxxxxxxxxxxxxxxxx

- > Hi Steven,
- > usually in a server to server scenario, once response is received, the
- > *client* who sends the request will close down the connection. I think
- > that's the difference comparing to browser to server scenario? I know the
- > SSL handshake is an expensive operation, if I choose to use SSL to access
- > the webservice, that'll mean everytime I send a request to the webservice,
- > a
- > new connection is established, and SSL handshake will be done, then we
- > lose
- > the benefit of re-using the same session key, is it correct?
- >
- > thanks,
- > -Jason
- >
- > "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message
- > news:2sOVJa0vFHA.1616@xxxxxxxxxxxxxxxxxxxxxxxx
- >> Hi Jason,
- >>
- >> Of course the sessionkey will be expired and regenerated after connection
- >> closed and new connection established. Also, during a live connection's

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>> lifecycle, the SessionKey will also expire and be regenerated according
>> to
>> the timespan is has across so as to ensure the channel's secure. In
>> addition, for SSL between server to server, I think it's the same with
>> client to server, in fact when a server use HTTPS to call webservice at
>> another server protected by SSL/TLS, the server which send the request is
>> just the "CLIENT", so server/client is a logic concept.
>>
>> Thanks,
>>
>> Steven Cheng
>> Microsoft Online Support
>>
>> Get Secure! www.microsoft.com/security
>> (This posting is provided "AS IS", with no warranties, and confers no
>> rights.)
>>
>> -----
>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>> References: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <NRnDAzcuFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <uK1wLCguFHA.596@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <dIKkV7luFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <uKVnDInuFHA.3500@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <gRqUmbouFHA.1080@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <Oxmu91IvFHA.3452@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <gGB5JtLvFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <eqSVtJgvFHA.2076@xxxxxxxxxxxxxxxxxxxxxxxx>
>> <M10VK0ovFHA.580@xxxxxxxxxxxxxxxxxxxxxxxx>
>> Subject: Re: FOLLOW UP – Re: what certificate to buy from Verisign ?
>> Date: Wed, 21 Sep 2005 12:58:55 -0400
>> Lines: 388
>> X-Priority: 3
>> X-MSMail-Priority: Normal
>> X-Newsreader: Microsoft Outlook Express 6.00.3790.326
>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>> Message-ID: <ei#DE3svFHA.908@xxxxxxxxxxxxxxxxxxxxxxxx>
>> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements
>> NNTP-Posting-Host: a7cebc03.cst.lightpath.net 167.206.188.3
>> Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!tk2msftngp13.phx.gbl
>> Xref: TK2MSFTNGXA01.phx.gbl
>> microsoft.public.dotnet.framework.webservices.enhancements:4946
>> X-Tomcat-NG: microsoft.public.dotnet.framework.webservices.enhancements
>>
>> Hi Steven,
>> thanks for getting back to me. SSL is possible in my scenario, but I
>> have some doubts about using SSL in a server to server scenario, let me
>> explain:
>>
>> in a typical scenario of Browser talking to server through SSL, a SSL
>> handshake is done, and a session key is established, session key is

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>> transferred back to browser from server. and browser can use the
>> generated
>> session key to send request to the server as long as the browser remain
>> open. if browser closes down, session will be lost, if new browser
> instance
>> opens, new SSL handshake have to be done, new session key will be
> generated
>> and transferred back to browser.
>>
>> in a scenario of server talking to server through SSL, SSL handshake
>> will
>> be done when server tries to send request to the other server through
> https.
>> session key will be transferred back, and as long as the connection not
>> closed down, same session key will be used. the catch here is in most
> server
>> to server scenario, I think connections have to be closed once the
>> request
>> is done. or in this scenario, should we put the opened https connection
> into
>> a connection pool? I think I'm lost in this. also, will the session key
> ever
>> expire?
>>
>> thanks,
>> -jason
>>
>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:M10VK0ovFHA.580@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>> > Hi Jason,
>> >
>> > Thanks for your followup.
>> > The verisign guy's suggestion is reasonable from security perspective
>> since
>> > Asymmetric encryption is really more secure, but also more performance
>> > cost. Generally, we'll use asymmetric encryption to transfer
>> > sessionkey
>> > and then use that sessionkey to do symmetric encryption for all the
>> > sequential commuincation. That's also what SLL/TLS does.
>> >
>> > For HTTPS/SSL, of course I'd recommend you consider it if SSL/TLS is
>> really
>> > possible for your scenario. The SSL/TLS just provide a secuire point to
>> > point channel which ensure confidential, integrity And though
> WSE
>> > also priovde these features, the SSL/TLS's implementation is surely
>> > more
>> > robust and sophisticated. And the WSE's strong point is that it
>> > provide
>> > more flexible and wide applicaiton scenario, which is not limited to
>> > webserver scenario, (generally SSL/TLS require our server service be

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>> hosted
>>> in a sophisticated webserver like IIS/ Apache or other applicaiton
>>> server). While WSE application can be hosted in any .NET application.
>>>
>>> Thanks,
>>>
>>> Steven Cheng
>>> Microsoft Online Support
>>>
>>> Get Secure! www.microsoft.com/security
>>> (This posting is provided "AS IS", with no warranties, and confers no
>>> rights.)
>>> -----
>>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>>> References: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxx>
>>> <NRnDAzcuFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>> <uK1wLCguFHA.596@xxxxxxxxxxxxxxxxxxxx>
>>> <dIKkV7luFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>> <uKVnDInuFHA.3500@xxxxxxxxxxxxxxxxxxxx>
>>> <gRqUmbouFHA.1080@xxxxxxxxxxxxxxxxxxxx>
>>> <Oxmu91IvFHA.3452@xxxxxxxxxxxxxxxxxxxx>
>>> <gGB5JtLvFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>> Subject: FOLLOW UP – Re: what certificate to buy from Verisign ?
>>> Date: Tue, 20 Sep 2005 12:43:28 –0400
>>> Lines: 284
>>> X–Priority: 3
>>> X–MSMail–Priority: Normal
>>> X–Newsreader: Microsoft Outlook Express 6.00.3790.326
>>> X–MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>>> Message–ID: <eqSVtJgvFHA.2076@xxxxxxxxxxxxxxxxxxxx>
>>> Newsgroups: microsoft.public.dotnet.framework.webservices.enhancements
>>> NNTP–Posting–Host: a7cebc03.cst.lightpath.net 167.206.188.3
>>> Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP14.phx.gbl
>>> Xref: TK2MSFTNGXA01.phx.gbl
>>> microsoft.public.dotnet.framework.webservices.enhancements:4929
>>> X–Tomcat–NG: microsoft.public.dotnet.framework.webservices.enhancements
>>>
>>> HI Steven,
>>> this is an update on this thread, I just had a call with a Verisign
>>> senior engineer, and he had very strong opinions on using asymeric
>>> encryptions.
>>> first thing he said when I tried to explain to him WSE2 uses
>>> asymeric
>>> encryption is 'asymeric encryption is 1000 times slower than symetric
>>> encryption', then he recommended to use HTTPS protocol to protect the
>>> data
>>> on the transport level instead of using HTTP and protect the data on
>>> the
>>> application level. he also said by protecting data on application
>>> level,
>>> it'll be much slower and will be easier for brute force attack.

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>> what I'd like to find out from you is, do you have any performance
>>> matrix on how much performance overhead will be added by using x.509
>>> certificates to encrypt the sign the data comparing to not encrypting
> and
>>> sign the data?
>>> also, do you have any comment on using HTTPS vs. using HTTP + WSE2
>>> encryption and signing?
>>>
>>> thanks,
>>> –Jason
>>>
>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:gGB5JtLvFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx
>>>> You're welcome Jason,
>>>>
>>>> If there're any further things we can help later, please feel free to
>>> post
>>>> here.
>>>> Good luck!
>>>>
>>>> Steven Cheng
>>>> Microsoft Online Support
>>>>
>>>> Get Secure! www.microsoft.com/security
>>>> (This posting is provided "AS IS", with no warranties, and confers no
>>>> rights.)
>>>> -----
>>>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>>>> References: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxx>
>>>> <NRnDAzcuFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>>> <uK1wLCguFHA.596@xxxxxxxxxxxxxxxxxxxx>
>>>> <dIKkV7luFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>>> <uKVnDInuFHA.3500@xxxxxxxxxxxxxxxxxxxx>
>>>> <gRqUmbouFHA.1080@xxxxxxxxxxxxxxxxxxxx>
>>>> Subject: Re: what certificate to buy from Verisign ?
>>>> Date: Sun, 18 Sep 2005 16:13:51 –0400
>>>> Lines: 212
>>>> X–Priority: 3
>>>> X–MSMail–Priority: Normal
>>>> X–Newsreader: Microsoft Outlook Express 6.00.3790.326
>>>> X–MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>>>> Message–ID: <Oxmu91IvFHA.3452@xxxxxxxxxxxxxxxxxxxx>
>>>> Newsgroups:
>>>> microsoft.public.dotnet.framework.webservices.enhancements
>>>> NNTP–Posting–Host: a7cebc03.cst.lightpath.net 167.206.188.3
>>>> Path: TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP14.phx.gbl
>>>> Xref: TK2MSFTNGXA01.phx.gbl
>>>> microsoft.public.dotnet.framework.webservices.enhancements:4913
>>>> X–Tomcat–NG:
> microsoft.public.dotnet.framework.webservices.enhancements
>>>>

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>> thanks steven for following up, I guess I have to schedule a call
>>> with
>>> verisign to work this out then.
>>>
>>> –Jason
>>>
>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxx> wrote in message
>>> news:gRqUmbouFHA.1080@xxxxxxxxxxxxxxxxxxxxxxxx
>>>> Hi Jason,
>>>>
>>>> Server certificate is used by server service, and is not necessary
> for
>>>> client app. For client side, there has Client Authentication
>>> Certificate
>>>> respectively. In fact, you find a certain windows 2000 or 2003
> server
>>>> machine which can install the Microsoft Certificate Service, so
>>>> that
>> you
>>>> can create/send certificate request to it , from which you can see
>> those
>>>> most popular types of certificates. In addition, professional
>>> Authority
>>>> like Verisign will have much more types of certificates available,
> so
>> I
>>>> still think it better you consult them on your scenario.
>>>>
>>>> Thanks,
>>>>
>>>> Steven Cheng
>>>> Microsoft Online Support
>>>>
>>>> Get Secure! www.microsoft.com/security
>>>> (This posting is provided "AS IS", with no warranties, and confers
> no
>>>> rights.)
>>>>
>>>>
>>>>
>>>>
>>>> -----
>>>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>>>> References: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxx>
>>>> <NRnDAzcuFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>>> <uK1wLCguFHA.596@xxxxxxxxxxxxxxxxxxxx>
>>>> <dIKkV7luFHA.768@xxxxxxxxxxxxxxxxxxxx>
>>>> Subject: Re: what certificate to buy from Verisign ?
>>>> Date: Thu, 15 Sep 2005 23:52:07 –0400
>>>> Lines: 146
>>>> X–Priority: 3

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>>> X-MSMail-Priority: Normal
>>>> X-Newsreader: Microsoft Outlook Express 6.00.3790.326
>>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>>>> Message-ID: <uKVnDInuFHA.3500@xxxxxxxxxxxxxxxxxxxxxxxx>
>>>> Newsgroups:
> microsoft.public.dotnet.framework.webservices.enhancements
>>>> NNTP-Posting-Host: a7cebc02.cst.lightpath.net 167.206.188.2
>>>> Path:
> TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP09.phx.gbl
>>>> Xref: TK2MSFTNGXA01.phx.gbl
>>>> microsoft.public.dotnet.framework.webservices.enhancements:4897
>>>> X-Tomcat-NG:
>> microsoft.public.dotnet.framework.webservices.enhancements
>>>>
>>>> hi Steven,
>>>> I'd like X509 certificate to be used by both client and server,
>> you
>>>> mentioned the server side can use a regular SSL certificate, can
>> client
>>>> also
>>>> use a regular ssl certificate on client side?
>>>>
>>>> thanks,
>>>> –Jason
>>>>
>>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in
>>>> message
>>>> news:dlKkV7luFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx
>>>>> Thanks for your response Jason,
>>>>>
>>>>> As for the webservice client, it all depends on your
>>>>> application's
>>>>> security
>>>>> authentication design. If you server doesn't use some
> authentication
>>>> schema
>>>>> which require client certificates(x509 authentication based token
>>>>> authentication....) or the server doesn't require the client to
> use
>> a
>>>>> certain certificate to identify clientside, then client app do
> not
>>> need
>>>>> to
>>>>> have a own certificate. This is just like when we use SSL
> without
>>>>> requiring clientside certificate. Also, since you're using
>>>>> WSE,
>> if
>>>> you
>>>>> have used x509 certificate token to sign message at both

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>>> client/serverside,
>>>>> then, the clientside also must have its own certificate.
>>>>>
>>>>> Thanks,
>>>>>
>>>>> Steven Cheng
>>>>> Microsoft Online Support
>>>>>
>>>>> Get Secure! www.microsoft.com/security
>>>>> (This posting is provided "AS IS", with no warranties, and
>>>>> confers
>> no
>>>>> rights.)
>>>>>
>>>>>
>>>>> -----
>>>>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>>>>> References: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxxxxxx>
>>>>> <NRnDAZcuFHA.768@xxxxxxxxxxxxxxxxxxxxxxxx>
>>>>> Subject: Re: what certificate to buy from Verisign ?
>>>>> Date: Thu, 15 Sep 2005 10:19:53 -0400
>>>>> Lines: 83
>>>>> X-Priority: 3
>>>>> X-MSMail-Priority: Normal
>>>>> X-Newsreader: Microsoft Outlook Express 6.00.3790.326
>>>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>>>>> Message-ID: <uK1wLCguFHA.596@xxxxxxxxxxxxxxxxxxxxxxxx>
>>>>> Newsgroups:
>> microsoft.public.dotnet.framework.webservices.enhancements
>>>>> NNTP-Posting-Host: a7cebc03.cst.lightpath.net 167.206.188.3
>>>>> Path:
>> TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!TK2MSFTNGP12.phx.gbl
>>>>> Xref: TK2MSFTNGXA01.phx.gbl
>>>>> microsoft.public.dotnet.framework.webservices.enhancements:4884
>>>>> X-Tomcat-NG:
>>> microsoft.public.dotnet.framework.webservices.enhancements
>>>>>
>>>>>> thanks Steven, I guess the server side can just purchase the
> normal
>>>>>> webserver certificate, what about the client side who consumes
>>>>>> the
>>>>>> webservice? should they also get a normal webserver certificate
>>>>>> or
>>>>>> something
>>>>>> particular?
>>>>>>
>>>>>> many thanks,
>>>>>> -jason
>>>>>>
>>>>>> "Steven Cheng[MSFT]" <stcheng@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in
> message

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>>>> news:NRnDAzcuFHA.768@xxxxxxxxxxxxxxxxxxxxxxxxxxxx
>>>>> Hi Jason,
>>>>>
>>>>> AS for the Certificate type you mentioned, for your scenario,
>> since
>>>> the
>>>>> certificate is mainly used to identify your server application
>> and
>>>> build
>>>>> a
>>>>>> secure communication channel between client/server, I think a
>> normal
>>>> web
>>>>>> server certificate is enough. Of course, there must has some
> guys
>>>> from
>>>>>> Verisign who will help you find the proper certificate for your
>>>>>> application.
>>>>>>
>>>>>> Thanks,
>>>>>>
>>>>>> Steven Cheng
>>>>>> Microsoft Online Support
>>>>>>
>>>>>> Get Secure! www.microsoft.com/security
>>>>>> (This posting is provided "AS IS", with no warranties, and
> confers
>>>> no
>>>>>>> rights.)
>>>>>>>
>>>>>>>
>>>>>>> -----
>>>>>>> From: <jason.chen@xxxxxxxxxxxxxxxxxxxx>
>>>>>>> Subject: what certificate to buy from Verisign ?
>>>>>>> Date: Wed, 14 Sep 2005 12:52:04 -0400
>>>>>>> Lines: 29
>>>>>>> X-Priority: 3
>>>>>>> X-MSMail-Priority: Normal
>>>>>>> X-Newsreader: Microsoft Outlook Express 6.00.3790.326
>>>>>>> X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.326
>>>>>>> Message-ID: <Oo3#jyUuFHA.3756@xxxxxxxxxxxxxxxxxxxxxxxx>
>>>>>>> Newsgroups:
>>> microsoft.public.dotnet.framework.webservices.enhancements
>>>>>>> NNTP-Posting-Host: a7cebc03.cst.lightpath.net 167.206.188.3
>>>>>>> Path:
>>> TK2MSFTNGXA01.phx.gbl!TK2MSFTNGP08.phx.gbl!tk2msftngp13.phx.gbl
>>>>>>> Xref: TK2MSFTNGXA01.phx.gbl
>>>>>>> microsoft.public.dotnet.framework.webservices.enhancements:4873
>>>>>>> X-Tomcat-NG:
>>>> microsoft.public.dotnet.framework.webservices.enhancements
>>>>>>>

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

>>>>> Hi, my company plans to use WSE2.0 sp3 to secure the webservice
>>>>> communication between us and the client. now that we are
>>>>> looking
>> at
>>>>> Verisign
>>>>> on what exactly to buy but the sales person at Verisign were
>>>>> not
>>> very
>>>>> helpful. and MSDN didn't provide any information on what exact
>>>> certificate
>>>>> to buy from Verisign either, all it says is get certificate
>>>>> from
> a
>>>>> trusted
>>>>>> CA, for example: Verisign.
>>>>>>
>>>>>> could someone point out which product to buy from verisign?
>>>>>>
>>>>>> some information on what I found so far:
>>>>>>
>>>>>> 1. after searched around, seems a lot of people are complaining
>>>> Verisign
>>>>>> sales have no idea what to buy to encrypt and sign web
>>>>>> services.
>>>>>>
>>>>>> 2. some people seem got regular SSL certificates working to
>> encrypt
>>>> and
>>>>>> sign web service request, but will there be performance issues?
> is
>>> it
>>>>>> recommened by Microsoft that an existing SSL certificate can be
>> used
>>>> for
>>>>>> encrypt and sign webservice requests?
>>>>>>
>>>>>> 3. some people in various newsgroups are talking about using
>>>>>> the
>>>> Digital
>>>>>> ID
>>>>>> product from Verisign to encrypt and sign webservice requests,
>>>>>>
>>>>>>
>>>>>
>>>>
>>>
>>>
>>>
>>>>>> (<http://www.verisign.com/products-services/security-services/pki/pki-applica>
>>>>>> tion/email-digital-id/index.html), this is a product from
> Verisign
>>> to

Re: FOLLOW UP – Re: what certificate to buy from Verisign ?

◇ *From:* jason.chen

◆ **Re: what certificate to buy from Verisign ?**

◇ *From:* Steven Cheng[MSFT]

◆ **FOLLOW UP – Re: what certificate to buy from Verisign ?**

◇ *From:* jason.chen

◆ **RE: FOLLOW UP – Re: what certificate to buy from Verisign ?**

◇ *From:* Steven Cheng[MSFT]

◆ **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**

◇ *From:* jason.chen

◆ **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**

◇ *From:* Steven Cheng[MSFT]

◆ **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**

◇ *From:* jason.chen

- Prev by Date: **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**
- Next by Date: **RE: SecurityToken assertion policy in WSE 2.0 SP3 Configuration Ed**
- Previous by thread: **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**
- Next by thread: **Re: FOLLOW UP – Re: what certificate to buy from Verisign ?**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**