

## Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2003-11/0254.html>

---

*From:* Bernard ([qbernard\\_at\\_hotmail.com](mailto:qbernard_at_hotmail.com))

*Date:* 11/12/03

Date: Thu, 13 Nov 2003 03:47:41 +0800

Sergio missing in action ?

I just enable this thread trace flags.. will keep monitoring :)

sorry, I'm out on this one .

--

Regards,

Bernard Cheah

<http://support.microsoft.com/>

Please respond to newsgroups only ...

"Ohaya" <[ohaya@NO\\_SPAM.cox.net](mailto:ohaya@NO_SPAM.cox.net)> wrote in message  
news:3FAEA65F.196E6003@NO\_SPAM.cox.net...

> Bernard,

>

> NONE so far :(....

>

>

>

>

> Bernard wrote:

> >

> > and what's the outcome ??

> >

> > --

> > Regards,

> > Bernard Cheah

> > <http://support.microsoft.com/>

> > Please respond to newsgroups only ...

> >

> > "Ohaya" <[ohaya@NO\\_SPAM.cox.net](mailto:ohaya@NO_SPAM.cox.net)> wrote in message

> > news:3FA1922B.C74AD692@NO\_SPAM.cox.net...

> > > Sergio,

> > >

> > > Thanks for the followup. Believe me, I am MORE than happy to provide

> > > whatever information that I can on this. I'll try to respond to all  
of

> > > your questions (interspersed below), and hope that I don't miss

> > > anything...

> > >

> > >

> > >

> > > "Sergio Dutra [MS]" wrote:

## microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > >
> > > > Could you specify how you generated the Root CA and SSL server
> > certificates
> > > (enough details so I can reproduce it)?
> > >
> > > The certificate for the root CA (the one that is being used by the MS
> > > Certificate Server) was created when I installed MS Certificate
Server.
> > >
> > > When I installed the system (Win2K Advanced Server), I think that the
> > > steps that I went through were:
> > >
> > > 1) Install Windows 2K Advanced Server SP3 (MS Cert Server not selected
> > > during installation) and IIS from CD.
> > >
> > > 2) Using the popup program that starts up automatically after Windows
> > > installation, configured machine as the first DC (i.e., installed AD).
> > > Did not install DNS Server as part of this.
> > >
> > > 3) Installed MS Certificate Server.
> > >
> > > At this point, the root CA certificate now existed in the system.
> > >
> > > I then used Windows Update to bring IE to 6.0 and Windows to SP4.
> > >
> > > I then imaged my hard drive. I did this so that I could restore the
> > > system back to this point for subsequent system, i.e., so I could use
> > > this configuration as my test baseline.
> > >
> > > I then used IIS Server Certificate wizard to create a cert request for
> > > the server.
> > >
> > > The next day, when I got the server cert back from the 3rd-party CA, I
> > > imported the root CA cert and the sub-CA cert from my 3rd-party
> > > CA/sub-CA into the Local Machine Trusted and Intermediate stores,
> > > respectively.
> > >
> > > I then used IIS Server Certificate wizard to process the server
> > > certificate that I had received from my 3rd-party CA.
> > >
> > > Note that at this point, I had:
> > >
> > > - the root CA cert for MS Certificate Server installed on the machine
> > > - the certs for the root CA and sub-CA for my 3rd-party CA installed
> > > - the server cert issued by my 3rd-party CA imported into Windows, and
> > > installed in IIS
> > >
> > > I did not have a server cert issued by my MS Certificate Server (I had
> > > not issued any yet). As I alluded to in my previous post, I kind of
am
> > > guessing that this is the "root" of this "bug" (sorry for the pun
:)!).
> > >
> > > [Please DON'T FLAME me for the following! This is all just GUESSING
on
> > > my part, trying to imagine what kind of mistake I might have made if I
> > > was coding this stuff myself that would result in the behavior that I
am
> > > actually witnessing.]:
> > >
> > > I think what's going on is a kind of "boundary" problem, i.e.,
something
```

## microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > like this: The code in either IIS or CryptoAPI (I can't determine
> > > which) *assume* that there is more than one certificate created by
> > > Certificate Server already in the system. So, during the SSL
handshake,
> > > when it (either IIS or CryptoAPI) starts enumerating through these
certs
> > > to build the SSL CertificateRequest message, it starts checking from
the
> > > 2nd cert, rather than the 1st (the MS Certificate Server CA cert), and
> > > as a result, it skips checking the "Client Authentication" purpose in
> > > the first (the MS Certificate Server root cert) cert.
> > >
> > >
> > >
> > >
> > > > The list you specify for the root CA, is that from the Details pane
or
> > > the
> > > > General pane of the certificate UI?
> > >
> > > The list was from the Details tab, displayed in the lower pane of the
> > > certificate UI when I clicked on Enhanced Key Usage in the upper pane.
> > >
> > >
> > > > Also, are you attempting to perform client authentication from the
same
> > > > machine as the root CA?
> > >
> > > I think that you're asking if the client machine that I'm testing with
> > > is the same as the machine that is running the MS Certificate Server?
> > >
> > > If that is an accurate interpretation of your question, then the
answer
> > > is "no".
> > >
> > > As I explained in detail in the 1st post in this thread I am using two
> > > machines in these tests:
> > >
> > > Server: Win2K Advanced Server SP4, updated on Friday (10/24/03)
> > >         Server is the DC (i.e., ActiveDirectory is installed)
> > >         MS Certificate Server is installed
> > >         IIS5
> > >
> > > Client: Win2K Pro SP4, updated same date as server
> > >         IE 6.0.2800.1106
> > >
> > >
> > >
> > > If so, the root CA may have a copy in another store
> > > > (usually, "MY" store), and that copy may not have a property
restricting
> > > the
> > > > usages, so that IE would pick the SSL certificate issued by that
root.
> > >
> > > Again, that (client machine = server machine) is not the configuration
> > > that I have. The client machine (running Win2K Pro) is a physically
> > > separate machine from the server (running Win2K Advanced Server).
> > >
> > >
> > >
> > > >
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > --
> > > This posting is provided "AS IS" with no warranties, and confers no
> > rights.
> > > Use of included script samples are subject to the terms specified at
> > > http://www.microsoft.com/info/cpyright.htm
> > >
> > >
> > >
> > > "Ohaya" <ohaya@NO_SPAM.cox.net> wrote in message
> > > news:3FA142DC.4DFC1230@NO_SPAM.cox.net...
> > > > Sergio,
> > > >
> > > > Sorry, I messed up typing out the list of Extended Key Usage (the
cert
> > > > is on a different machine than I use to post, so I had to manually
key
> > > > everything into the post). The list should have been:
> > > >
> > > > File Recover
> > > > Digital Rights
> > > > Smart Card Logon
> > > > License Server Verification
> > > > Key Pack Licenses
> > > > Embedded Windows System...
> > > > OEM Windows...
> > > > Windows System Component Verification
> > > > Windows Hardware Driver Verification
> > > > Encrypting File System
> > > > IP Security User
> > > > IP Security tunnel termination
> > > > IP Security end system
> > > > Microsoft Time Stamping
> > > > Microsoft Trust List Signing
> > > > Time Stamping
> > > > Secure email
> > > > Code Signing
> > > > Client Authentication
> > > > Server Authentication
> > > >
> > > >
> > > > And, yes, I can confirm that that list was from the root
certificate
> > > > used for MS Certificate Server.
> > > >
> > > > So, I think that, based on what you described below, I should be
able
> > > to
> > > > control whether this CA gets sent out by IIS in the SSL
> > > > CertificateRequest message by enabling/disabling the "Client
> > > > Authentication" purpose in the root CA cert, but as I indicated,
this
> > > > does not seem to be working.
> > > >
> > > > IIS is including this CA name in the CertificateRequest regardless
of
> > > > the setting of the "Client Authentication" purpose in the
Certificate
> > > > Server/root CA certificate, and as I've indicated in a previous
post,
> > > > I've confirmed this using OpenSSL's s_client.
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > >
> > > > One thing that I noticed when testing with OpenSSL s_client is
that if
> > > > the "Client Authentication" purpose is disabled, the MS
Certificate
> > > > Server CA name is always the first in the list of CAs that IIS
sends
> > in
> > > > the CertificateRequest message.
> > > >
> > > > I'm thinking that this "bug" is related to some kind of indexing
> > problem
> > > > in either IIS or maybe in CryptoAPI when it enumerates the CAs
from
> > the
> > > > Trusted Root store. In other words, maybe since my MS Certificate
> > > > Server's root CA cert is #0, there's a bug in either IIS or
CryptoAPI
> > > > where it's skipping the checking of the "Client Authentication"
> > purpose.
> > > >
> > > > As I've also posted, I've sent an email to MS, and posted on the
> > website
> > > > as a possible bug, but I haven't heard anything back (I didn't
expect
> > > > that anyway :)), so I hope that since you're with MS, you might
bring
> > > > this up to the appropriate people.
> > > >
> > > > If someone was malicious, and depending on how you look at it,
this
> > > > could be regarded as a semi-serious security vulnerability, akin
to a
> > > > "hijacking a CA" exploit.
> > > >
> > > >
> > > >
> > > >
> > > >
> > > > "Sergio Dutra [MS]" wrote:
> > > > >
> > > > > The way certificate properties work is by restricting the usages
> > allowed
> > > > by
> > > > > the certificate. Hence, for a certificate that has no EKU
extension
> > > > (meaning
> > > > > it's good for anything) or for a certificate that has multiple
> > usages
> > > > > (including Client Auth) specified in the EKU extension, enabling
the
> > > > Client
> > > > > Auth property restricts the certificate to being good only for
> > client
> > > > > authentication.
> > > > >
> > > > >
> > > > > If the certificate does have the EKU extension but it does not
have
> > the
> > > > > Client Auth usage, enabling the Client Auth property makes the
> > > > certificate
> > > > > valid for nothing, since the intersection of the EKU extension
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > usages
> > > > and
> > > > > the property usages is nil.
> > > > >
> > > > > Typically, the EKU property is set on the root certificate and
not
> > on
> > > > end
> > > > > certificates. I assume that the MS Certificate Server cert you
> > listed
> > > > the
> > > > > usages for is the root certificate, and not the end certificate
> > issued
> > > > by it
> > > > > that is actually used by SSL.
> > > > >
> > > > > In your case, the MS Certificate Server CA cert does seem to
have
> > the
> > > > EKU
> > > > > extension and it has several usages in it, but I do not see the
> > Client
> > > > Auth
> > > > > usage in the list below. If this is the case, then you should
not be
> > > > able to
> > > > > enable the Client Auth property since the certificate does not
> > contain
> > > > that
> > > > > usage already.
> > > > > --
> > > > > This posting is provided "AS IS" with no warranties, and confers
no
> > > > rights.
> > > > > Use of included script samples are subject to the terms
specified at
> > > > > http://www.microsoft.com/info/copyright.htm
> > > > > "Ohaya" <ohaya@cox.net> wrote in message
> > > > news:3F9EAE9A.4C769D45@cox.net...
> > > > > Sergio,
> > > > >
> > > > > > There are no intermediate CAs or intermediate CA certs for the
MS
> > > > > > Certificate Server CA chain. MS Certificate Server was
installed
> > with
> > > > > > all the normal defaults.
> > > > > >
> > > > > > When I look at the MS Certificate Server CA cert under
> > > > Details->Enhanced
> > > > > > Key Usage extension, it lists:
> > > > > >
> > > > > > File Recover
> > > > > > Digital Rights
> > > > > > Smart Card Logon
> > > > > > License Server Verification
> > > > > > Key Pack Licenses
> > > > > > Embedded Windows System...
> > > > > > OEM Windows...
> > > > > > Windows System Component Verification
> > > > > > Windows Hardware Driver Verification
> > > > > > Encrypting File System
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > > > IP Security User
> > > > > IP Security tunnel termination
> > > > > IP Security end system
> > > > > Microsoft Time Stamping
> > > > > Microsoft Trust List Signing
> > > > > Time Stamping
> > > > > Secure email
> > > > > Code Signing
> > > > > Server Authentication
> > > > >
> > > > > Under Edit Properties:
> > > > >
> > > > > No matter whether I choose "Enable All", "Disable All", or
"Enable
> > > > > Only"
> > > > > and uncheck all boxes, IIS sends out the MS Cert Server in the
> > > > > acceptable CA list.
> > > > >
> > > > > Some of my subsequent posts showed up in the NGs, some didn't,
but
> > > > > FYI,
> > > > > I have used OpenSSL to confirm the above, and I have an image
of a
> > > > > clean
> > > > > Win2K/IIS/Cert Server install, and this problem is repeatable.
> > > > >
> > > > >
> > > > > "Sergio Dutra [MS]" wrote:
> > > > >
> > > > > > What usages does the root certificate of your MS Certificate
> > Server
> > > > > have
> > > > > > (from the Enhanced Key Usage extension)? Are there any
> > intermediate
> > > > > certs
> > > > > > and, if so, what are their usages?
> > > > > >
> > > > > > --
> > > > > > This posting is provided "AS IS" with no warranties, and
confers
> > no
> > > > > > rights.
> > > > > > Use of included script samples are subject to the terms
> > specified at
> > > > > > http://www.microsoft.com/info/copyright.htm
> > > > > > "Ohaya" <ohaya@NO_SPAM.cox.net> wrote in message
> > > > > > news:3F9D3A7F.7294A454@NO_SPAM.cox.net...
> > > > > > > Hi,
> > > > > > >
> > > > > > > I think that I have encountered a somewhat serious "bug"
> > > > > > > somewhere. I
> > > > > > > > can't tell if it's a CryptoAPI bug, an IIS bug, or
whatever,
> > so
> > > > > I'm
> > > > > > > cross-posting this to several newsgroups. This seems like
(to
> > me)
> > > > > a
> > > > > > > rather serious problem, and I'll try to describe what's
> > happening
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > > as
> > > > > > > best I can, and also provide a somewhat kludgy workaround.
> > > > > > >
> > > > > > >
> > > > > > > Background:
> > > > > > > =====
> > > > > > > Server: Win2K Advanced Server SP4, updated on Friday
> > (10/24/03)
> > > > > > > Server is the DC (i.e., ActiveDirectory is
installed)
> > > > > > > MS Certificate Server is installed
> > > > > > > IIS5
> > > > > > >
> > > > > > > Client: Win2K Pro SP4, updated same date as server
> > > > > > > IE 6.0.2800.1106
> > > > > > >
> > > > > > > I have been preparing to configure the above server for
SSL
> > with
> > > > > > server
> > > > > > > and client authentication for awhile.
> > > > > > >
> > > > > > > Before I did that, in order to do some pre-testing, I
issued a
> > > > server
> > > > > > > cert for IIS with MS Certificate Server, and several
client
> > certs.
> > > > > > >
> > > > > > > I got all of this (SSL with client and server
authentication)
> > > > working,
> > > > > > > including IE would display the client certs that were
issued
> > by MS
> > > > > > > Certificate Server whenever I tried to connect from IE to
IIS.
> > > > > > >
> > > > > > > Then, using the IIS server certificate wizard, I deleted
the
> > > > original
> > > > > > MS
> > > > > > > Certificate Server-issued server cert, then created a new
> > server
> > > > > > > certificate request, which I then sent to my commercial CA
one
> > > > night.
> > > > > > > The next morning, I received the new server cert from my
> > > > commercial
> > > > > > CA,
> > > > > > > along with a set of test client certificates.
> > > > > > >
> > > > > > > I then installed the root cert from my commercial CA on
the
> > > > server,
> > > > > > and
> > > > > > > then using IIS, used the IIS server certificate wizard to
> > install
> > > > the
> > > > > > > new server cert that I had just received from my
```

```
commercial
> > CA.
> > > > > > > >
> > > > > > > > I also installed one of the test client certificates from
my
> > > > > commercial
> > > > > > > > CA, and installed it on my client machine, and began
testing.
> > > > > > > >
> > > > > > > >
> > > > > > > > Problem:
> > > > > > > > =====
> > > > > > > > From some previous testing with an earlier similar (SSL
client
> > and
> > > > > > > > server authentication) setup, I found that I could control
> > which
> > > > > client
> > > > > > > > certificates that IE would display, when connecting to the
> > server,
> > > > by
> > > > > > > > enabling or disabling the "Client Authentication" Purpose
in
> > the
> > > > root
> > > > > CA
> > > > > > > > certificate Purposes for specific root CAs.
> > > > > > > >
> > > > > > > > In other words, if I disabled/unchecked the "Client
> > > > Authentication"
> > > > > > > > purpose for the root CA cert for "Whatever CA", then
client
> > > > > certificates
> > > > > > > > issued by "Whatever CA" would display in the IE popup when
I
> > tried
> > > > to
> > > > > > > > connect to the server. If I enabled/checked the "Client
> > > > > Authentication"
> > > > > > > > purpose for the root CA cert for "Whatever CA", then
client
> > > > > certificates
> > > > > > > > issued by "Whatever CA" would NOT display in the IE popup
when
> > I
> > > > tried
> > > > > > > > to connect to the server.
> > > > > > > >
> > > > > > > >
> > > > > > > > However, it appears that with the setup that I ended up
with
> > above
> > > > > > > > (install MS Cert Server server cert, uninstall server
cert,
> > > > install
> > > > > > new
> > > > > > > > commercial CA server cert), which I described above under
> > > > > "Background",
> > > > > > > > this (enabling/disabling "Client Authentication" purpose
for
> > the
> > > > root
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > > > CA
> > > > > > > > cert) does not appear to work for the client certs created
> > with MS
> > > > > > > > Certificate Server.
> > > > > > > > >
> > > > > > > > > Specifically, the client certificates that I created using
MS
> > > > > > > > > Certificate Server still get displayed by IE when
connecting
> > to
> > > > the
> > > > > > > > > server, regardless of how the "Client Authentication"
purpose
> > is
> > > > set
> > > > > > in
> > > > > > > > > the root CA certificate on the server-side, and there does
not
> > > > appear
> > > > > > to
> > > > > > > > > be any reasonable way to prevent these client certificates
> > from
> > > > being
> > > > > > > > > displayed by IE during a connection attempt.
> > > > > > > > >
> > > > > > > > > I'm guessing (I would HOPE) that deleting the root
certificate
> > for
> > > > my
> > > > > > MS
> > > > > > > > > Certifate Server on the SERVER might work, but then that
would
> > > > kill my
> > > > > > > > > MS Certificate Server installation, so that doesn't seem
like
> > a
> > > > > > > > > reasonable solution, and really, I'm kind of puzzled about
why
> > the
> > > > > > > > > "Client Authentication" purpose is "obeyed" for all client
> > > > > > > > > certificates
> > > > > > > > > except for the ones created by MS Certificate Server.
> > > > > > > > >
> > > > > > > > >
> > > > > > > > > Bottom line: It appears that if you install MS
Certificate
> > > > Server,
> > > > > > > > > issue a server cert and some client certs, then install a
> > server
> > > > cert
> > > > > > > > > from another CA, that there is no way way get IE browsers
that
> > had
> > > > > > > > > client certs from MS Certificate Server not to display
those
> > > > > > > > > previously
> > > > > > > > > issued client certs.
> > > > > > > > >
> > > > > > > > >
> > > > > > > > >
> > > > > > > > > Possible workaround:
```

microsoft.public.platformsdk.security: Re: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

```
> > > > > > > > =====
> > > > > > > > I haven't found a way, from the server-end, to cause IE
not to
> > > > display
> > > > > > > > those MS Certificate Server-issued client certs, but
> > > > > > > > > thankfully,
> > > > > > > > > with
> > > > > > > > > IIS at least, the CTL functionality still works properly.
> > > > > > > > > >
> > > > > > > > > In other words, if I set up a CTL with only the root cert
from
> > > my
> > > > > > > > > commercial CA, IE will STILL DISPLAY both the client certs
> > > > > > > > > from my
> > > > > > > > > commercial CA and the client certs that were issued by MS
> > > > > > > > > Certificate
> > > > > > > > > > Server, but at least the authentication/connection will
fail
> > > if
> > > > > > > > > someone
> > > > > > > > > > tries to connect using one of the client certs issued by
MS
> > > > > > > > > Certificate
> > > > > > > > > > Server.
```