

BUG?: Can't disable "Trusted" for Certificates Issued by MS Certificate Server

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2003-10/0448.html>

From: Ohaya (ohaya_at_NO_SPAM.cox.net)

Date: 10/27/03

Date: Mon, 27 Oct 2003 10:32:15 -0500

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 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 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 Certificate 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:

=====

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.