

Re: crypt32

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/0339.html

From: Wesley Vogel (123WVogel955_at_comcast.net)

Date: 02/03/04

Date: Tue, 03 Feb 2004 03:57:31 GMT

Drew;

<LOL>

The thing is, I haven't signed anything.
When I bought Enron stock it was good.

Seriously.

The only enabled purpose for VeriSign Time Stamping CA is time stamping.
I see that as an oxymoron. An expired certificate being used for time stamping.

I'm sorry but I see much humor here.

I guess since I have Update Root Certificates enabled I have to live with what it does.

[[keep it around for verifying past uses]] makes sense to me.

Thank you for your replies. I reckon I should read more about Certificates in MMC Help. :o)

Wes

In news:ONF7q7f6DHA.2560@TK2MSFTNGP09.phx.gbl,
Drew Cooper [MSFT] <dcoop@online.microsoft.com> hunted and pecked:

- > *Try this hypothetical scenario:*
- > – *Currently I have a signing cert (and priv key). The cert is good. The chain is good. Nothing expired.*
- > – *I sign file foo.exe with it and timestamp the file for good measure.*
- > – *2 years from now one of the certs in the chain expires. Chaining will fail.*
- >
- > *Should we still consider the signature good? We know that it was good when I signed foo.exe, so if we trusted the cert chain then, we trust that I was the one who actually signed foo.exe.*
- >
- > *Expiration *could* mean you don't trust anything that cert was used for.*
- > *Or it could mean "don't use that cert for any new operations, but keep it around for verifying past uses".*

Re: crypt32

>
> *I'm going to stop now before I confuse myself.*
> --
> *Drew Cooper [MSFT]*
> *This posting is provided "AS IS" with no warranties, and confers no*
> *rights.*
>
>
> *"Wesley Vogel" <123WVogel955@comcast.net> wrote in message*
> *news:udCTb.210314\$xy6.1081857@attbi_s02...*
>> *Drew;*
>> *Thank you for the reply.*
>>
>> *I don't understand. Before I delete the cert, it says it's*
>> *expired. Even if I couldn't figure out how a calendar*
>> *works. :o)*
>>
>> *If my drivers license expires I get a new*
>> *one and throw the expired one a way.*
>> *Same with food packages.*
>>
>> *If I want to keep an expired certificate why*
>> *wouldn't it be kept in*
>>
>> *Never mind. I see now that it's in the Untrusted Certificates*
>> *Certificates folder.*
>>
>> *Now that makes sense.*
>>
>>
>> *Wes*
>>
>> *In news:Oo5Wwke6DHA.3804@tk2msftngp13.phx.gbl,*
>> *Drew Cooper [MSFT] <dcoop@online.microsoft.com> hunted and pecked:*
>>> *That cert expired, but some of the certs issued from that root are*
>>> *probably still good. And we need the root cert to verify their*
>>> *chains. Actually even if it were revoked there could be circumstances*
>>> *in which we'd want to keep the cert around.*
>>> --
>>> *Drew Cooper [MSFT]*
>>> *This posting is provided "AS IS" with no warranties, and confers no*
>>> *rights.*
>>>
>>>
>>> *"Wesley Vogel" <123WVogel955@comcast.net> wrote in message*
>>> *news:J2FSb.147356\$sv6.821849@attbi_s52...*
>>>> *Howdy;*
>>>>
>>>> *Event Viewer.*
>>>> *=====*
>>>> *Event Type: Information*

>>>> *Event Source: crypt32*
>>>> *Event Category: None*
>>>> *Event ID: 7*
>>>> *Date: 1/30/2004*
>>>> *Time: 4:31:55 PM*
>>>> *User: N/A*
>>>> *Computer: MYPENTIUM450*
>>>> *Description:*
>>>> *Successful auto update retrieval of third-party root list sequence*
>>>> *number from:*
>>>>
>>>>
>>>>
>>>>
>>>>
>>>> <http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt>
>>>>
>>>> *For more information, see Help and Support Center at*
>>>> <http://go.microsoft.com/fwlink/events.asp>.
>>>> =====
>>>> *Event Type: Information*
>>>> *Event Source: crypt32*
>>>> *Event Category: None*
>>>> *Event ID: 2*
>>>> *Date: 1/30/2004*
>>>> *Time: 4:31:55 PM*
>>>> *User: N/A*
>>>> *Computer: MYPENTIUM450*
>>>> *Description:*
>>>> *Successful auto update retrieval of third-party root list cab from:*
>>>>
>>>>
>>>>
>>>>
>>>> <http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab>
>>>>
>>>> *For more information, see Help and Support Center at*
>>>> <http://go.microsoft.com/fwlink/events.asp>.
>>>> =====
>>>> *Event Type: Information*
>>>> *Event Source: crypt32*
>>>> *Event Category: None*
>>>> *Event ID: 1*
>>>> *Date: 1/30/2004*
>>>> *Time: 4:31:55 PM*
>>>> *User: N/A*
>>>> *Computer: MYPENTIUM450*
>>>> *Description:*
>>>> *Successful auto update of third-party root certificate.: Subject:*
>>>> *<OU="NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.", OU=VeriSign Time*

>>>> *Stamping Service Root, OU="VeriSign, Inc.", O=VeriSign Trust*
>>>> *Network> Sha1 thumbprint: <18F7C1FCC3090203FD5BAA2F861A754976C8DD25>*
>>>>
>>>> *For more information, see Help and Support Center at*
>>>> *<http://go.microsoft.com/fwlink/events.asp>.*
>>>> =====
>>>>
>>>> *I keep deleteing this expired Certificate and Cryptographic Services*
>>>> *keeps downloading it again. I tried to move it to the Untrusted*
>>>> *Certificates folder in Console1 | Certificates | but was unable to.*
>>>>
>>>> *The Expired Certificate is:*
>>>>
>>>> *VeriSign Time Stamping CA OU = NO LIABILITY ACCEPTED, (c)97*
>>>> *VeriSign, Inc. OU = VeriSign Time Stamping Service Root*
>>>> *OU = VeriSign, Inc.*
>>>> *O = VeriSign Trust Network*
>>>> *Valid to: Wednesday, January 07, 2004 4:59:59 PM*
>>>>
>>>> *This thing expired three weeks ago. What's the deal?? How come it*
>>>> *keeps coming back like a bad penny? Any insight would be*
>>>> *appreciated.*
>>>>
>>>> *Wes*