

Re: Which certificate do I have to deploy ? Root CA or Subordinate CA certificate ?

Re: Which certificate do I have to deploy ? Root CA or Subordinate CA certificate ?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2008-03/msg00084.html>

- *From:* "Brian Komar \ (MVP\)" <brian.komar.nospam@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 26 Mar 2008 06:37:17 -0500
-

If a subordinate chains to a trusted root CA, then it is also trusted.

Best bet is for your to read the certificate revocation and status checking whitepaper that describes how certificates are verified.

<http://technet.microsoft.com/en-us/library/bb457027.aspx>

PKI is based on root trust.

If you trust the root CA, you trust *ALL* subordinate CAs, no matter how deep the hierarchy (by default)

Brian

please

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxx> wrote in message

<news:mn.d2c77d834f67cee7.70874@xxxxxxxxxxxxxxxxxxxx>

Thank you for your answer.

In Microsoft website it is written :

"Only root CA certificates must be trusted and registered on client computers. Do not add subordinate CA certificates to the Group Policy trust, because intermediate and issuing CAs certificates may not be explicitly trusted."

Source :

<http://technet2.microsoft.com/windowsserver/en/library/e1f11ddb-759b-4f58-90b7-3d32f124d3bc1033.msp>

So I am not understanding that I have to trust the subordinate CA as you said.

Thanks

This is basic PKI. Trust is established at the root.

If the CA is a subordinate of a trusted root, you trust the CA.

I would recommend reading Polk and Housley

Brian

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxx> wrote in message

<news:mn.d2a87d837c712979.70874@xxxxxxxxxxxxxxxxxxxx>

Hi,

Re: Which certificate do I have to deploy ? Root CA or Subordinate CA certificate ?

we are planning to deploy a certificate hierarchy.

First, we will have a Root CA (standalone Offline) and a subordinate CA (enterprise online integrated to AD).

My question is which certificate should I have to deploy to my computer Trusted Root Certification Authorities Store ?
The Root CA or the Subordinate CA ?

I have read in Microsoft website that it should be the Root CA certificate (and not the Subordinate CA) but I dont understand why !

Indeed, imagine that in the future we decide to install a new subordinate Enterprise CA (child of the Root CA, so a brother of the first subordinate CA) for a new acquired company;

If we have installed the Root CA in our domain member computers, then they will trust every certificate delivered by the new subordinate Enterprise CA, am I right ?
This is not very nice as the new sub enterprise CA is not defined to trust computers for the "whole company" but just for the newly acquired company.

Please could you tell me what do you think about that ?

Thanks

-- Pascal

--
Pascal