

Re: PKI in multi sites/domains environment

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-12/msg00050.html>

- *From:* BZP <p.audonnet@xxxxxxxx>
 - *Date:* Tue, 11 Dec 2007 08:11:23 -0800 (PST)
-

Thanks !

As regards the isolation process (Americas users use only Americas CA), ok for the first way, via permissions. But I'm wondering something, it prevents users from getting certificates from a delocalized CA but it doesn't prevent users contacting the bad CA (does it?). For exemple, when a user need a certificate for encrypting his files. An automatic process will ask to a CA for a EFS certificates. And if the process use the bad CA, it rolls back to an other CA ? (Am I clear ?) or the process will use only CA where permissions are ok (how can it check this without contacting the CA ? permission are published in AD ? configuration context ?)

That's a great link (microsoft.com/pki) ! Thanks for this.

And what about X500 name constraints ? This function can be achieved by constraint extensions ? For exemple I configure a CA with constraint : issuing certificated only if subject CN match with "*,DC=AMERICAS,DC=LOCAL". Will this serve ?

For the point 3, you want to say that CA certificates are published in AD ? Is there a AD store like there is a User store in a computer ? How does it work ?

I can't get what the purpose of the Issuance Policies (Low, Medium, High). What is the interest ?

Thanks.

Regards,

—

P.J.A.

.