

Re: PKI in multi sites/domains environment

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-12/msg00054.html>

- *From:* "Brian Komar" <brian.komar@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 11 Dec 2007 22:27:30 -0600
-

Sorry, not a lot of time to respond this evening (writing the 2nd edition of my PKI book :-S)

"BZP" <p.audonnet@xxxxxxxx> wrote in message
news:3d50de26-c005-4db1-aae6-c7f53791c759@xx

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 ?)

It may send responses to each CA, but only stops when it receives a certificate from a CA. Not really a roll back, but similar

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

No problem

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 ?

This is another way, but could lead to a lot of configuration headaches. I would not recommend it, even though I wrote the whitepaper.

Re: PKI in multi sites/domains environment

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 ?

Not quite. The certificates are published to the Configuration naming context. The autoenrollment process ensures that these are plumbed to the AD clients running win2k or higher

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

See RFC 3647 and look for assurance levels. this is a rudimentary implementation and most companies do custom assurance levels.

Thanks.

Regards,

—

P.J.A.