

Re: Question regarding PKI architecture with cross domain trusts.

Re: Question regarding PKI architecture with cross domain trusts.

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2007-09/msg00058.html>

- *From:* "Brian Komar" <brian.komar@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 17 Sep 2007 14:29:59 -0500
-

A couple of thoughts inline:

Brian

"Enrico" <nricko@xxxxxxxx> wrote in message
news:1190054916.239862.262090@xx

Hello all,

I have the following PKI architecture implemented in a dev environment

- 1 Office Root CA
- Root CA Certificate Properties:
 - CDP: ldap location on both DomainA and DomainB
 - AIA: ldap location on both DomainA and DomainB

In your environment, I would only use HTTP locations for the CDP and AIA, rather than LDAP. The reason is how the certificate validation engine works. For the users in the domain that is first in the list of LDAP URLs, everything is great. Fast responses to CRL validation downloads. For the other users.... well.... they..... have to wait..... for the first LDAP URL to fail
If you had a third domain to the mix, there is going to be a case where they now have to fail again.

- 2 Online Enterprise Issuing CAs
 - 1 in DomainA
 - 1 in DomainB

This is good. In fact, I would recommend having an HTTP URL first followed by an LDAP URL only containing the local domain's LDAP URLs.

There is also a cross-domain trust established between DomainA and DomainB.

Re: Question regarding PKI architecture with cross domain trusts.

As of now there seems to be no issue with certificate communication between a server on DomainA and a server on DomainB, but I am unsure as to how this communication would be affected when I introduce a new domain (DomainC) to the mix.

To add a new domain to this architecture I would do the following:

1. Bring the root CA online.
2. Update the CDP and AIA points to include the ldap location of DomainC.

I would update to only use HTTP URLs. In any kind of cross forest environment, I would only use HTTP URLs. Alternatively, you could introduce an ADAM server or other LDAP server, and use LDAP.

3. Publish that certificate to the new domain and create an issuing CA on that domain, similar as I did for DomainA and DomainB.

Yep

4. Establish a cross domain trust with Domain A and DomainC.

5. Re-new the DomainA and DomainB subCA certificates so that they only contain the HTTP URL in the SubCA certificate

Questions

-
1. Is the certificate communication between DomainA and DomainB servers dependent on the CDP and AIA lists or just the fact that they trust the Root Certificate signature?

Both. They must trust the root signature, but they also will need to download the CRL and CA certificate during chain validation.

2. Since the CDP and AIA points will change in the Root CA certificate, will DomainA and DomainC have a certificate communication issues since the updated Root CA certificate will be contained in DomainC, but not in DomainA (essentially uses certificate without updated CDP and AIA extensions)?

There will not really be any issues, but I would recommend changing to just an HTTP URL and renewing the

Re: Question regarding PKI architecture with cross domain trusts.

DomainA and DomainB certificates.

3. As a side note, does disabling the certificate revocation checks affect the validity of a certificate?

No. But if you are disabling revocation checks, you have real problems with your PKI and need to fix it. If you are not determining if a certificate is revoked, what use are the certificates...

Thank you