

Questions about new PKI infrastructure

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-05/msg00152.html>

- *From:* Rasmus Rask <RasmusRask@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 2 May 2007 17:05:00 -0700
-

I'm about to implement a PKI infrastructure in my company, but am a complete n00b when it comes to PKI. I have read a lot of whitepapers, pages on MS TechNet, posts in MS newsgroups lately and feel like I m beginning to grasp the concept. I have a fairly good idea of the setup I think will suit us the best, but not having managed a PKI infrastructure before and think I could really use a sanity check and someone to help fill out the blanks.

OUR SETUP

We have an AD running in Windows 2003 native mode, have DCs in multiple sites and roughly 500 clients running Windows XP (a few running 2000). Most of our ~ 50 member servers run Windows Server 2003 and a few (maybe a handful) run Windows 2000 Server. Servers, clients, network and applications are managed by three administrators at our HQ and one in the US. Our manager is quite technical and helps out when needed. Administrative overhead is a major concern for us.

USAGE

We currently need PKI in order to support Office Communication Server 2007, EFS and SSL encryption for websites. In near future I imagine we will also use digital signing and encryption of e-mails and authentication of wireless network clients.

PROPOSED SETUP

A two-tier setup, both CA s running Windows 2003 Enterprise.

Root CA:

- Type: Offline stand-alone
- Certificate validity: 10 years
- Certificate key length: 4.096 bits
- CRL publishing interval: full: 6 months, delta: disabled
- CRL publishing properties: local: 1, LDAP: 10, HTTP: 10
- AIA publishing properties: local: , LDAP: , HTTP:
- CRL and AIA publication order: local, LDAP then HTTP
- CRL and AIA are manually published through LDAP and to a web server on our DMZ, the latter accessible both internally and externally for OCS clients to do certificate revocation and trust chain checking.

Sub-ordinate CA:

Questions about new PKI infrastructure

- Type: Online enterprise issuing
- Certificate validity: 5 years
- Certificate key length: 2.048 bits
- CRL publishing interval: full: 1 week, delta: 1 day
- CRL publishing properties: local: 65, LDAP: 77 or 79 (?), HTTP: 77 or 79 (?)
- AIA publishing properties: local: , LDAP: , HTTP:
- CRL and AIA publication order: local, LDAP then HTTP
- CRL and AIA are manually published through LDAP and to a web server on our DMZ, the latter accessible both internally and externally for OCS clients to do certificate revocation and trust chain checking.

Values for CRL publication properties taken from

<http://technet2.microsoft.com/windowsserver/en/library/073732b5-80f0-4cf0-bc8e-d8e055ce26491033.msp?mfr=tr>

values for AIA publication properties taken from

<http://technet2.microsoft.com/windowsserver/en/library/a624c39d-3e66-4c7c-9ef1-42d400a1c7f11033.msp?mfr=tr>

Questions:

- First of all: Does the above suggestion make sense? Any obvious weak points or thing I have missed completely?
- What should and should not be specified in the CAPolicy.inf for the root and sub respectively? Do I only have to worry about CDP, AIA, key length and validity?
- Can AIA publishing interval be defined?
- For the sub CA, should I use 77 or 79 as the CRL publishing option?
- I seem to recall that the root CA certificate should not have CPD and AIA defined. On the other hand, the process of generating and manually publishing the CRL and AIA is described several places. Am I getting things mixed here?

I know there s a lot of questions and suggestions to consider, sorry for that. Any help and hints will be greatly appreciated. My manager is very eager to get this thing flying as soon as humanly possible :-).

THANKS!

Best regards,
Rasmus Rask

.