

## Re: 2003 PKI Design Question

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-02/0409.html>

---

**From:** Paul Adare ([padare\\_at\\_newsguy.com](mailto:padare_at_newsguy.com))

**Date:** 02/25/05

Date: Fri, 25 Feb 2005 02:41:52 -0500

In article <uI621arGFHA.2752@TK2MSFTNGP12.phx.gbl>, in the microsoft.public.windows.server.security news group, Mark Gamache <mark.gamache@css-security.com.nospam> says...

> *Your two basic options are to create your own root and deal with the issues*  
> *of it not being trusted by other parties, or you can have your CA signed by*  
> *a trusted root and be subject to their terms and conditions.*  
>

Actually there is a third option that is probably a better way to go and that is to use a combination of the two options.

For certificates that need to be trusted externally, chain an issuing CA (there's really no point in having an offline subordinate policy CA here as you will be restricted by the external CA's CPS) to an external trusted root CA. This would issue S/MIME certs, and possibly code signing certs if the code signing certs need to be externally trusted.

For certificates that only need to be (and should only be) trusted internally, deploy an internal PKI (2 or 3 tier depending on your needs). This would issue EFS and smart card logon certs (and anything else that needed only internal trust such as IPSec, 802.1x, etc.).

--

Paul Adare

"On two occasions, I have been asked [by members of Parliament], 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' I am not able to rightly apprehend the kind of confusion of ideas that could provoke such a question."

-- Charles Babbage (1791-1871)