

Re: Question about PKI and Trust model

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-07/1422.html>

From: Andrew Swallow (am.swallow_at_eatspam.btinternet.com)

Date: 07/30/04

Date: Fri, 30 Jul 2004 15:32:51 +0000 (UTC)

"ohaya" <ohaya@cox.net> wrote in message news:410A4D58.7A90E131@cox.net...
[snip]

- > *In other words, this is kind of the opposite to the normal "higher level*
- > *CA is higher trust" paradigm.*
- >
- >
- > *The reason THAT question is coming up is that we're kind of debating*
- > *whether or not these "special privileges" or "special*
- > *constraints/checks" and the enforcement should, or even can, be embedded*
- > *into and enforced by the PKI infrastructure mechanism, or whether they*
- > *should be done at the application-level (e.g., by the servers).*

It is normal to separate the access right system from the CA. Before trying to merge the two systems check that you have physical control of all of the CAs and sub CAs.

Andrew Swallow