

Re: PKI and Relying Parties

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-03/0600.html>

From: Paul Rubin (phr-n2002a@nightsong.com)

Date: 03/27/02

From: Paul Rubin <phr-n2002a@nightsong.com>

Date: 27 Mar 2002 10:35:52 -0800

Anne & Lynn Wheeler <lynn@garlic.com> writes:

- > *some number of financial institutions have gone to "relying party*
- > *only" certificates ... i.e. certificates issued by the institution and*
- > *only useful by that institution. what they found out was that they were*
- > *interested in public key authentication ... which (apparently when*
- > *they started) they thought was equivalent to PKI, CAs, certificates,*
- > *etc.*
- >
- > *What they started to find out was that the transactions & operations*
- > *were accessing the same infrastructure that effectively was used for*
- > *issuing the certificates ... including real time status information.*
- >
- > *It was then trivially possible to show that the actual issuance of a*
- > *certificate as redundant and superfluous.*

Yeah, that's what the whole private CA biz seems to be about (Verisign OnSite, etc.)

- **Next message:** [Richard E. Silverman: "Re: Agent forwarding between OpenSSH and ssh.com servers"](#)
- **Previous message:** [Lars Kellogg-Stedman: "Agent forwarding between OpenSSH and ssh.com servers"](#)
- **In reply to:** [Anne & Lynn Wheeler: "Re: PKI and Relying Parties"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)