

## Re: SSL/TLS – am I doing it right?

---

*Source:* <http://coding.derkeiler.com/Archive/Python/comp.lang.python/2006-03/msg02676.html>

---

- *From:* Sybren Stuvel <[sybrenUSE@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:sybrenUSE@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 15 Mar 2006 12:31:22 +0100
- 

Paul Rubin enlightened us with:

The client cert approach isn't strictly necessary but it means that the SSL stack takes care of stuff that your application would otherwise have to take care of at both the client and the server side.

Indeed. I always try to take the route of the least wheels I have to invent. If a group of security specialists have already looked at such a mechanism, why should I reinvent another?

If you don't generate a certificate, you have to generate a username and password instead, and manage that. There's still secret authenticating info on the client, so you haven't really decreased the client's responsibility.

And on top of that, using passwords the secret information is sent over the network.

Sybren

—

The problem with the world is stupidity. Not saying there should be a capital punishment for stupidity, but why don't we just take the safety labels off of everything and let the problem solve itself?

Frank Zappa

.