

# Re: Multi-layered PKI implementation

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Debian/2006-05/msg00666.html>

---

- *From:* James Westby <[jw+debian@xxxxxxxxxxxxxxxxxx](mailto:jw+debian@xxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 5 May 2006 01:48:20 +0100
- 

On (04/05/06 19:16), Grant Thomas wrote:

Thanks for the explanations, they are rather more indepth than I was expecting for an idle curiosity.

Thanks for the verbosity and the need for clarification, they are always appreciated. As with many things, it is better to cut too long and adjust than to start short and really mess up.

I did figure that the access control wasn't built into the scheme and would take an external ACL implementation to do something like this.

In retrospect, I probably did have a slightly distorted impression of PKI, but the core I did understand.

To all, thanks for the responses, they were greatly interesting.

No problem.

So, one final question:

I would like to know more about encryption, the underlying infrastructures, etc. What would be, in the lists recommendation, a good place to start?

What sort of thing are you looking for? Are you just interested, or is it maybe something that will creep in to your work?

I'm always one for recommending books, so I'll just suggest a couple of things. If your just curious about the ideas behind some different schemes, and public vs private key, a bit of history, some anecdotes, then there are a couple of reasonable pop science type books around. I've read "The Code Book" by Simon Singh, and that was OK.

If you're interested say in the pros and cons of RSA vs El-Gamal, relative key sizes, attacks against them, factoring algorithms, then a

Re: Multi-layered PKI implementation

cryptography textbook might be a good idea. Either "Cryptography" by Nigel Smart, or "Practical Cryptography" by Bruce Schneier would be good.

If you're more interested in the issues surrounding cryptography and information security then there are again plenty of books out there. Again I would recommend Bruce Schneier.

If you dont fancy paper based material there are thousands of websites out there to trawl through, some of them are probably pretty good.

Maybe other people have different ideas.

Cheers,

James

--

James Westby  
jw+debian@xxxxxxxxxxxxxxxxx  
<http://jameswestby.net/>

--

To UNSUBSCRIBE, email to debian-user-REQUEST@xxxxxxxxxxxxxxxxx with a subject of "unsubscribe". Trouble? Contact listmaster@xxxxxxxxxxxxxxxxx