

## Re: Slightly OT: SSL certs – best practice?

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2006-05/msg00044.html>

---

- *From:* Ian G <[iang@xxxxxxxx](mailto:iang@xxxxxxxx)>
  - *Date:* Tue, 16 May 2006 10:51:51 +0200
- 

Hi all,

Clemens Renner wrote:

Hi James,

I would advise against using wildcard certificates. There certainly are situations where this might be adequate but I'm in favor of a single server certificate for each service that uses a different (virtual) host. Thus, I have created several certificates for Apache SSL hosts plus certificates for mail serving, etc.

An alternative to wildcard certificates is the SAN or SubjectAltName method documented here:

<http://wiki.cacert.org/wiki/VhostTaskForce>

It seems to work, I've used it (note that the primary CN should be duplicated in the SAN list).

PS – Once I've worked out how exactly I'm supposed to be doing this, I'll probably get some "officially" signed certs. I hear CACert are a good, free way of doing this. Anyone got any comments on that?

...

I'd say the same thing applies to certificates signed by a CA that does not do a "real" verification of the requesting person by which I mean that you probably don't need to go somewhere and show some official ID to prove that you are in fact you.

OK, just to clarify here – CACert's system of verification includes (in general) checking of identity documents in a person-to-person process.

Re: Slightly OT: SSL certs – best practice?

Once people have been verified to their standard – they call it their assurance process – the assured user can issue certs with names in them, using a "class 3" root; before that, users can only issue unnamed certs using an anon "class 1" root.

(Whether this works for you, all depends.)

iang

PS: I gather that the "class 3" and "class 1" convention comes from verisign.

---

freebsd-security@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"