

Re: What's up with Skype in Germany?

## Re: What's up with Skype in Germany?

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2008-01/msg01409.html>

---

- *From:* Peter Pearson <[ppearson@xxxxxxxxxxxxxxxxx](mailto:ppearson@xxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 27 Jan 2008 22:47:02 -0000
- 

On Sun, 27 Jan 2008 22:22:10 +0100, Sebastian G. <[seppi@xxxxxxxxx](mailto:seppi@xxxxxxxxx)> wrote:

Peter Pearson wrote:

As I understand it, my assurance that I am talking with you depends only upon (1) the validity of our two respective copies of the Skype Certificate Authority's public key, (2) the secrecy of the Skype CA's private key, and (3) the secrecy of our two private keys, stored in our two computers. If your understanding differs, or if you see a connection between any of these points and the Skype login server, please elaborate.

Simply said, the Skype login server is the one who authenticates users against each other.

Are you claiming that my computer performs no authentication? Checks no certificate? Doesn't use your public key? I'm getting my information from Tom Berson's report at <http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf> . Have you found a clearer description of the authentication process? (If we weren't in "simply said" mode, would actual facts emerge? After all, if I only wanted condescending and laconic conclusory assertions, I'd go to Usenet. Oh, wait; I'm there.)

Considering under which jurisdiction this server exists, and the history of the company that provides Skype, it's very likely that this actually happens quite often.

It would greatly facilitate communications if you said something specific about that jurisdiction and that history.

Re: What's up with Skype in Germany?

Well, obviously the Skype login server is on soil of USA,

Is that obvious? I thought their engineering was in Tallinn, and their business office in London. Skype's "About" page says that they are based in Luxembourg. When I run the Skype software, within seconds messages are exchanged with IP addresses all over the globe.

--

To email me, substitute nowhere->spamcop, invalid->net.

.