Verisign and Kafka - Separated at Birth?

Posted At : October 31, 2006 5:48 PM | Posted By : Mark Kruger
Related Categories: Hosting and Networking

So you want an SSL certificate and your customer insists on using Verisign eh? Here's something to watch out for - the "domain registrant". In case you needed another indicator that the whole SSL "authority" game is a **protection racket**, let me fill you in on my tail of woe. I have a customer who insisted on using Verisign for his SSL certificate. I dutifully went to Verisign and purchased the overpriced product and waited for my new cert to arrive. Shortly after the purchase I got a note from Verisign support. My customer in his wisdom had made the domain private. Because a "WHOIS" query identified the domain as private, Verisign couldn't verify that they "owned" the domain. Our first step was to make the information public. That turned out to be only the beginning of our trouble.

Next, it turned out that the domain registrant listed (let's say it was "acme company") did not match the information provided when we purchased the cert (like "acme co. Inc."). Close but no cigar. Verisign sent a helpful "pre-filled out" domain registrant verification letter with the following instructions.

1. Either Change the "WHOIS" information to reflect the Cert information

   ...or...

2. Sign and fax in the letter.

And what did we do?? To be extra helpful we did both. We faxed in the letter *and* we changed the WHOIS information - what could go wrong?

Now Verisign had a fax in hand that matched the *old* WHOIS information and WHOIS information that matched the cert. You would think they would just give us points for trying and send us the cert but nope. This discrepancy must be remedied. They sent another FAX for us to sign - this one matching the "new" WHOIS information. So here we sit twiddling our thumbs still without a cert. On the plus side we are getting certified in thumb-twiddling next Tuesday, and that will look nice on the old resume.