Wt - Bug #2916

SSL Certificate vs SSL Issuer Chain input file

04/08/2014 05:40 PM - Jesse Pepper

Status:	Feedback	**Start date:**	04/08/2014
Priority:	Normal	**Due date:**	
Assignee:	Koen Deforche	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.3.0		

Description

Hi There,

I'm trying to get SSL working with Wt app, and have specified the ---ssl-certificate command line argument. My certificate issuer however has provided me with both a .crt certificate file and a .ca-bundle "issuer chain". As I understand it, the issuer chain contains a chain of trusted certificates from a known trusted certificate body, to my own, via some intermediaries.

I tried to specify the .ca-bundle file in the ---ssl-certificate argument but received the following error from Wt at startup:

```
Error (asio): use_private_key_file: key values mismatch
```

When I use the .crt file itself, it runs fine, and works fine in chrome and safari, but some installations of firefox on windows don't trust the certificate, and the detail they give is as follows:

```
www.perth.surgerylink.com.au uses an invalid security certificate. The certificate is not trusted because no issuer chain was provided. (Error code: sec_error_unknown_issuer)
```

Is it possible to specify the certificate chain file for OpenSSL?

Apache allows the following 3 settings:

```
SSLCertificateFile /etc/ssl/crt/yourDOMAINNAME.crt
SSLCertificateKeyFile /etc/ssl/crt/private.key
SSLCertificateChainFile /etc/ssl/crt/yourSERVERNAME.ca-bundle ***
```

The SSLCertificateChainFile doesn't seem to be an option in Wt. Is this an oversight? Is it something that is intended to support?

Also, just checking you're aware of this, and 1.01g is supported.
http://www.pcworld.com/article/2140920/heartbleed-bug-in-openssl-puts-encrypted-communications-at-risk.html

History

#1 - 04/11/2014 09:16 PM - Peter K

Hi Jesse,

You can concatenate the certificate file and the bundle file into one, and give the name of the new file to Wt with ---ssl-certificate.

Regards,

Peter

#2 - 04/12/2014 11:20 AM - Koen Deforche

- Status changed from New to Feedback

- Assignee set to Koen Deforche

Hey,

I am not an expert on this, but I would also think that the certificate and issuer certificate chain is to be considered together, and thus goes into one file.

Could you confirm that that does work for you?

Regards,

koen

#3 - 04/12/2014 07:14 PM - Jesse Pepper

Yes, sorry for the delayed response, I wanted to confirm a few colleagues that were having trouble now saw my site as trusted. Concatenating the files together seems to work just fine. In case anyone else is having this issue, you keep the entire contents of each file and just merge them. I put the main key first and then the chain.

Thanks Peter

Jesse