Subject: How can I use CORE/SSL to sign something or check signatures?
Posted by Alboni on Tue, 02 Mar 2021 18:56:46 GMT
View Forum Message <> Reply to Message

I am implementing communication with a pay terminal. It uses a soap connection over the internet. I figured out how to do that, it is just a http put with a specific xml, but one of the fields in the xml requires signing the SHA256 of all the other fields with a private certificate and adding it as base64 to the xml.
I also need to verify all the info coming back by checking it with their public certificate.
I have all the certificates and the protocol description.

What I can't figure out is how to do the signing using upp or the actual checking of their signature.

Subject: Re: How can I use CORE/SSL to sign something or check signatures?
Posted by mirek on Wed, 03 Mar 2021 08:58:54 GMT
View Forum Message <> Reply to Message

Alboni wrote on Tue, 02 March 2021 19:56I am implementing communication with a pay terminal. It uses a soap connection over the internet. I figured out how to do that, it is just a http put with a specific xml, but one of the fields in the xml requires signing the SHA256 of all the other fields with a private certificate and adding it as base64 to the xml.
I also need to verify all the info coming back by checking it with their public certificate.
I have all the certificates and the protocol description.

What I can't figure out is how to do the signing using upp or the actual checking of their signature.

I am not 100% sure it applies in your code, but there is some signing code in PdfDraw:

String p7s = HexString(GetP7Signature(data, sign->cert, sign->pkey));

(please share your progress - can be useful for others...)