Subject: Core/SSL Having issue with Lets encrypt certificate
Posted by Xemuth on Fri, 10 Apr 2020 21:40:52 GMT
View Forum Message <> Reply to Message

Hello,

I have a fresh and valide certificate from LetsEncrypt with is private key, to test Upp compatibility, I have launch the package References : Https

```
...
 for(;;) {
  TcpSocket socket;
  LOG("============================================================ Waiting...");
  if(socket.Accept(server)) {
   LOG("Connection accepted");
   socket.SSLCertificate(LoadFile(GetDataFile("C:\\Users\\Xemuth\\Documents\\ssl\\cert.pem")),
                         LoadFile(GetDataFile("C:\\Users\\Xemuth\\Documents\\ssl\\privkey.pem")),
                         false);
   if(!socket.StartSSL()) {
    LOG("Failed to start SSL: " << socket.GetErrorDesc());
    continue;
   }
   while(socket.SSLHandshake());
   if(socket.IsError()) {
    LOG("SSL handshake failed: " << socket.GetErrorDesc());
    continue;
   }
   LOG("SSL established");
...
```

Any one have an idea ?

Thanks in advance.
Best regards

Subject: Re: Core/SSL Having issue with Lets encrypt certificate
Posted by mirek on Mon, 13 Apr 2020 08:34:51 GMT
View Forum Message <> Reply to Message

I suspect there should be 'true' for asn1 parameter (I believe .pem files are in that format).

Mirek

Subject: Re: Core/SSL Having issue with Lets encrypt certificate
Posted by Xemuth on Mon, 13 Apr 2020 13:30:47 GMT
View Forum Message <> Reply to Message

Hello Mirek, Thanks for your help, I have try but with or without the result is the same, I have tried on my Raspberry (wich carry the server my certificate is for) and the result is slightly different :

Seems like it's working but not totally !

EDIT : Result is the same with cert and pkey provided by Https Example

Subject: Re: Core/SSL Having issue with Lets encrypt certificate
Posted by Xemuth on Mon, 13 Apr 2020 14:56:09 GMT
View Forum Message <> Reply to Message

According to https://tls.mbed.org/kb/cryptography/asn1-key-structures-in- der-and-pem

Pem are Base64 encoded, maybe I should do something like that :

```
socket.SSLCertificate(LoadFile(Base64Decode(GetDataFile("C:\\Users\\Xemuth\\Documents\\ssl\\
chain.pem"))),
	LoadFile(Base64Decode( GetDataFile("C:\\Users\\Xemuth\\Documents\\ssl\\privkey.pem"))),
	true);
```

It don't work, I will try to find other way of decoding it

EDIT : I have try to decode my certificate using this website : https://lapo.it/asn1js/ and it work : This page contains a JavaScript generic ASN.1 parser that can decode any valid ASN.1 DER or BER structure whether Base64-encoded (raw base64, PEM armoring and begin-base64 are recognized) or Hex-encoded.

Do Upp ASN1 parser is able to reconize and decode multiple structure of pem ?