

Python and SSL

Source: <http://coding.derkeiler.com/Archive/Python/comp.lang.python/2007-04/msg02528.html>

- *From:* "billiejoex" <gnewsg@xxxxxxxxx>
 - *Date:* 16 Apr 2007 08:24:18 -0700
-

Hi,

I developed an ftp-server library and now I would like to add support for SSL/TLS as described in RFC 2228: <http://tools.ietf.org/html/rfc2228>
Currently I'm searching for documentation about this subject and I would like to start to ask some questions:

– I noticed that socket module provides an SSL class (socket.ssl) but even if documentation reports that it does not do any certificate verification a lot of stdlib modules (imaplib, poplib, smtplib, httplib and urllib2) provides SSL extension classes wherein socket.ssl is used. What does it mean?

– On top of that why such extension classes [examples: 1, 2, 3] accepts key-files and cert-files as optional arguments if no certificate verification occurs?

- [1] poplib.POP3_SSL(host[, port[, keyfile[, certfile]])
- [2] imaplib.IMAP4_SSL([host[, port[, keyfile[, certfile]])])
- [3] smtplib.starttls([keyfile[, certfile]])

– By searching through the web I found some daemons supporting SSL such as this one:

<http://aspn.activestate.com/ASPN/Cookbook/Python/Recipe/442473>

By looking at the code I notice that pyopenssl package is used and that a certificate file is required. Why do I need to use pyopenssl and how do I generate the cert file?

Could someone point me in the right direction?

Thanks in advance.

.