HowTo - PxPlus SSL

This page contains the information/instructions on SSL Certificates for use with PxPlus Secure TCP/IP-based applications such as the PxPlus Web Server, the PxPlus Application Server and/or any services that developers may write which use the Secure TCP/IP Sockets interface in PxPlus. Included are instructions on Generating a Certificate Signing Request, obtaining your SSL Certificate and Installing & Using your Certificate.

Generating a CSR (Certificate Signing Request) The following contains information and instructions on generating a Certificate Signing Request (CSR) which you are required to send to a Certificate Authority (CA) to obtain an SSL certificate for your server(s).

Download the appropriate file from http://www.openssl.org/related/binaries.html to the version of PxPlus you are running.

Extract the files to the directory where pxplus.exe is located. After downloading and extracting the files, get to a DOS prompt and enter the command:

`> cd \pvxplus\...` (ie. change to the directory where openssl.exe now resides)

`>copy openssl.cfg openssl.conf` (use the example configuration to create a new configuration)

1. **Generate the Private Key**
   The first step will be to generate a 2048 bit RSA Private Key for Certificate use.
   This command requires no interaction.
   ```
   > openssl genrsa -out privkey.pem 2048
   ```

   It is highly recommended that you back up this key to several locations. If lost the SSL will no longer function and you may have difficulties renewing your SSL Certificate in future.

   IMPORTANT! Never share your Private Key with anyone - doing so will allow your SSL-secured TCP/IP network traffic to be intercepted and decrypted!

2. **Generate the CSR** This will generate the certificate CSR. Enter the following command:
   ```
   > openssl req -new -key privkey.pem -out pvxplus.csr -config
   openssl.conf
   ```

   You will be now be prompted to enter information that will be incorporated into your certificate request.

   What you about to enter is what is called a Distinguished Name (DN). There are quite a few fields but you can leave some blank; for some fields there is a default value. If you enter '.' the field will be left blank.

Please note: entries below are examples only; please enter your own information and not those shown.

Country Name (2-letter code)	[]:CA
State or Province Name (full name)	[]:Ontario
Locality Name (e.g. City)	[]:Richmond Hill
Organization Name (e.g. Company)	[]:PVX Plus Technologies Ltd.
Organizational Unit Name (e.g. Section)	[]:PxPlus
Common Name (e.g. Your Name)	[]:*.pvxplus.com
Email Address	[]:myaddress@pvxplus.com
Please enter the following 'extra' attributes to be sent with your certificate request:	
A Challenge Password	[]:
An Optional Company Name	[]:

Note: Common Name (CN) is not 'your name', it is the name of your server. For example, if you are creating a certificate for use only on your webserver, enter as the Common Name: www.mydomain.com where mydomain.com is your domain name, e.g. www.pvxplus.com.

The example above shows '*.pvxplus.com' which is a wildcard certificate. The certificate would be valid on any machine in the pvxplus.com domain. This is a special certificate which requires you to place your order with a CA (Certificate Authority) for a wildcard certificate. Since a wildcard certificate may be used on any machine in your domain, you may have to purchase "Rights to Use" from the CA for the number of different servers you wish to use the certificate on.

A wildcard certificate is used most often when a single machine has several different names with which to provide different services. For example at our office, a machine named 'inet.pvxplus.com' provides web, ftp and mail services. These services are provided by using the correct name such as www.pvxplus.com, ftp.pvxplus.com or mail.pvxplus.com. To use one certificate on this server which has three different names, a wildcard certificate is required.

3. You will now have 2 text files in your directory:
   privkey.pem
   This is your Private key

   pvxplus.csr
   This is the "Certificate Signing Request" and is the file you send to a CA (Certificate Authority) when you want to purchase an SSL Certificate from them. Do not send your Private Key file to the CA; only send the CSR.

Obtaining your SSL Certificate

When submitting your CSR to a CA, they often want to know what software you are using so that they may generate a certificate in the correct format, and provide you instructions on how to install your certificate into your software. Most CA's have never heard of PxPlus (hard to imagine, yes?) however they have all heard of OpenSSL, which is the toolkit used within PxPlus to provide SSL socket support. OpenSSL is also used by the Apache Web Server for its secured sockets, so if they provide you with an "OpenSSL" option then select that; if not select "Apache". NOTE: Select the openssl Apache, not the mod_ssl Apache.

When the CA approves and validates your Business / Personal Information, they will send you your completed SSL certificate. You may receive one or more certificate files, most often in ending in ".crt" for certificate. These are in binary format and are not very useful with PxPlus.

PxPlus requires the certificates in ASCII text, base64-encoded form. Your CA will either provide you a link or will put the ASCII base64 encoded certificate in the message body of the email they sent you which had your binary form certificates attached. If they do not send you the ASCII base64-encoded form of your certificate, you may either request it from them or import your binary certificate into a Microsoft Windows machine, and then export it from the Digital Certificate Store in an ASCII base64 format.

If the CA sends you just one certificate that starts with -----BEGIN X509 CERTIFICATE----- then you do not need any other certificates.

If your CA sends you a certificate that begins with -----BEGIN CERTIFICATE----- then these are known as "Intermediate Certificates". These can only be used with ProvideX 5.12 or higher, and will require the CA's certificate as well as your own. The CA will provide instructions on how to install your certificate when using Apache which are not relevant to PxPlus; however they will also post a link to something they call a "bundle" file. This is a single ASCII text base64-encoded digital certificate containing both the Intermediate CA's digital certificate and their Root CA (Root Certificate Authority) digital certificate.

Once you have obtained your SSL certificate, in ASCII base64 form, and any additional digital certificates (such as individual or bundle certificates) for the CA who created your SSL certificate, you may install them by following the instructions in the next section, 'Using the Certificate'.

Using the certificate

1. You will need to create an ASCII text file to contain your Private Key and your ASCII base64 digital certificate(s). The name of this file does not need to be anything specific - you may use any name you wish.

   Copy and Paste your Private Key and your ASCII base64-encoded digital certificate(s) into the ASCII text file, examples below. Blank lines are premitted; comments of any kind may be included, provided you do not put anything between the -----BEGIN----- and -----END----- pairs, i.e. comments must be either above or below these paired entries.

-----BEGIN RSA PRIVATE KEY-----
<several lines worth of garbage-looking characters>
-----END RSA PRIVATE KEY-----

-----BEGIN X509 CERTIFICATE-----
<a bundle certificate of your local domain certificate and the root CA certificate>
-----END X509 CERTIFICATE-----

As of ProvideX v5.12, we are able to handle Intermediate (chained) SSL Certificates which are certificate files with two or three certificates (or more, up to 9) rather than just allowing a single master certificate.

Note: PxPlus requires the Private Key and Certificates to be in the SAME file. The order of certificates in the file is critical. The order is the highest certificate in the file is for the domain, then next would be for the Intermediate Certificate Authority, and the last certificate in the file would be the Root Certificate Authority:

Example - 3 Certificates
-----BEGIN RSA PRIVATE KEY-----
BASE64-ENCODEDCHARACTERS
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
YOUR LOCAL DOMAIN CERTIFICATE
-----END CERTIFICATE-----

----BEGIN CERTIFICATE-----
THE INTERMEDIATE CA CERTIFICATE
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
THE ROOT CA CERTIFICATE
-----END CERTIFICATE-----

Example - 2 Certificates
-----BEGIN RSA PRIVATE KEY-----
BASE64-ENCODEDCHARACTERS
-----END RSA PRIVATE KEY-----

----BEGIN CERTIFICATE-----
YOUR LOCAL DOMAIN CERTIFICATE
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
A BUNDLE CERTIFICATE OF BOTH
THE INTERMEDIATE CA CERTIFICATE
AND THE ROOT CA CERTIFICATE
-----END CERTIFICATE-----

Example - 1 Certificate

-----BEGIN RSA PRIVATE KEY-----
BASE64-ENCODEDCHARACTERS
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
A BUNDLE CERTIFICATE OF YOUR
LOCAL DOMAIN CERTIFICATE
AND THE ROOT CA CERTIFICATE
-----END CERTIFICATE-----

2. When you have finished creating the ASCII text file, you should test it from within PxPlus before you attempt to use it. Follow these instructions to test your SSL Certificate:

   Start an instance of PxPlus. At the prompt (->) enter (substituting your ASCII file name for MyCert.pem)
   ```
   ->OPEN (1)"[TCP];50000;Secure=c:\Pvxplus\MyCert.pem"
   ```
   If you get another (->) prompt, with no error then you have successfully obtained/created the necessary SSL Certificates and you are ready to use them.

   Errors:
   If PxPlus reports error #63, then your PxPlus is not activated for SSL support. To use SSL, you must have an eCommerce license or the SSL AddOn Package added to Base PxPlus. Please contact your dealer, distributor or OEM to obtain the required licenses.

   If error #12 is reported, then PxPlus is unable to find your SSL certificate.

   If you get err=0, then some other application is using socket 50000; try a different socket number and re-test.

   If error 13 is reported, then enter 'print msg(-1)' to get additional information. An err=13 typically occurs if the file named does not contain any Private Key or Digital Certificate. It may also occur if your Digital Certificates are not in the correct order within the file. The text reported by msg(-1) should give you a clue as to what is wrong. Check that the order of your certificates is as shown in the examples above; then exit PxPlus and restart a new instance of PxPlus before trying the test again. NOTE: SSL libraries in Open SSL do not seem to be able to load a valid certificate chain is an invalid one was previously loaded - this is why you need to restart PxPlus before trying the test again.

3. Specify the name of this file on the configuration for the PxPlus Webserver's SSL.