ExtPascal Advanced Configuration *

By Luiz Eneas Costa Junior

*This text was translated from the original in Brazilian Portuguese.
*Some parts was translated by Google Translator®

Any corrections and suggestions, tell me at eneascostajr@gmail.com

SUMMARY

1 Windows + Apache 2.2

1.01 Installation of Apache

1) Download the version 2.2.X of the Apache for Win32 and run the setup application. By opening the first screen click **[Next]**

2) Check the item "I accept the terms ..." and click **[Next]**

3) Read the text if you want and click **[Next]**

4) Enter the domain name, the server name and e-mail from the server administrator, if any. Otherwise just put "localhost" in the name of the server and "localdomain" in the field, and your e-mail as an e-mail the Administrator. Select, also an option "for All Users ..." and click **[Next]**

5) To choose "Custom" and click **[Next]**

6) Click **[Change]**

7) In "Folder name" type "C:\Apache\" and click **[Ok]**

8) Click **[Next]**

9) Click **[Install]**

10) Click **[Finish]**

1.02 FastCGI Module

1) Download the FastCGI module at:

```
http://www.fastcgi.com/dist/mod_fastcgi-2.4.6-AP22.dll
```

2) Rename library "mod_fastcgi-2.4.6-AP22.dll" to "mod_fastcgi.so" and copy to the folder of the Apache modules (c:\apache\modules)

3) Insert the line below in the session LoadModule httpd.conf

```
LoadModule fastcgi_module modules/mod_fastcgi.so
```

4) Declare FastCGI server as external

5) Anywhere in the httpd.conf (preferably at the end), include the line:

```
fastcgiexternalserver <work folder/SrvExtPascal> -host <host name
or ip address>:2014 -idle-timeout 3000
```

6) <work folder> should be the full path to the file in the format supported by Apache or an alias created in the appropriate session. Eg

```
"C:/Apache/htdocs/FastCGI/SrvExtPascal" or /FastCGI/ which is an
alias to the folder above
```

7) SrvExtPascal is a file used only to refer to the application and redirect the call to the real server. Must be an empty file created in the work folder. The relationship between the Apache server and the FastCGI service will be via external socket on the understanding that the application is already active in their respective server.

8) The parameter "-host" specifies the server that hosts the service FastCGI. If it is the same host where webserver resides declare it localhost. If it is in another host enter the FQDN of the host or its IP address.

9) The TCP port used by default will be 2014. If not available, any other unused port can be configured.

10) If you prefer to use Alias instead of full name of a folder entry in the session Alias <IfModule alias_module> should be established, as example below:

```
alias /FastCGI/ "C:/Apache/htdocs/FastCGI/"
```

11) If the folder is created outside of the folder declared in the entry "DocumentsRoot", the creation of the "Alias" is mandatory for it to be referenced by browsers in the address bar. That alias can be used anywhere where they reference the full name of the folder . Even the entry <Directory>

12) <Directory> entries must be created, as example below, for each folder you created for Web service to allow users access to avoiding errors "403 Forbidden".

```
<Directory /fastcgi/>
AllowOverride None
Options None
Order allow, deny
Allow from all
</Directory>
```

13) To change the configuration of apache between with-SSL and without-SSL observer the line "fastcgiexternalserver" to point respectively to the secured or not secured folders. E.g.: "ssl-htdocs" or "htdocs"

14) The line "ScriptAlias /cgi-bin/" ditto

1.03 Framework ExtJS

1) Download the package ExtJS 2.2 version at:

```
http://www.extjs.com/products/extjs/download.php?dl=extjs22
```

2) Extract the contents of the Ext-2.2.zip package in the root folder of your site's default web server on the same level of folders cgi-bin and FastCGI. Eg

On the server apache

```
C:\Apache\htdocs-ssl\ext
```

Or

```
C:\Apache\htdocs\ext
```

3) Create an alias file in httpd.conf

```
 Alias /ext/ "C:/Apache/ssl-htdocs/ext/"
```

1.04 Installation of ExtPascal

1) Copy the executable FastCGI (ExtPascalSamples) to the folder 'C:\Program Files\extpascal\" or anywhere else you wish. It must be compiled with the declaration {$DEFINE SERVICE}

2) to install ExtPascal server as service run this in command line:

```
C:\Program Files\ExtPascal> extpascalsamples /install
```

3) To uninstall it run:

```
C:\Program Files\ExtPascal> extpascalsamples /uninstall
```

4) To start service proceed like with any other service:

- Run management console (point to “My Computer” and right-click “Manage”)
- Choose service manager
- Find ExtPascal service entry
- Change the options you need (initialization: automatic, manual or disabled)
- Start the service

1.05 Installation of Gateway CGI (if applicable)

Copy the file CGIGateway.exe to the folder cgi-bin located in the root folder of your Web server where the website will be hosted.

1.06 Traffic Compression

1) Uncomment the line referring to the module "Deflate"

```
LoadModule deflate_module modules/mod_deflate.so
```

2) Include the block below before the declaration of fastcgiexternalserver:

```
# ---- HTTP COMPRESSION CONFIGURATION ----
<IfModule deflate_module>
# <Location />
# Insert filter
SetOutputFilter DEFLATE
SetInputFilter DEFLATE

AddOutputFilterByType DEFLATE text/html text/plain text/xml text/css
application/x-javascript text/javascript

# Netscape 4.x has some problems ...
BrowserMatch ^Mozilla/4 gzip-only-text/html
```

```
# Netscape 4.06-4.08 have some more problems
BrowserMatch ^Mozilla/4\.0[678] no-gzip

# MSIE masquerades as Netscape, but it is fine
# BrowserMatch \bMSIE !no-gzip !gzip-only-text/html

BrowserMatch \bMSI[E] !no-gzip !gzip-only-text/html

# Do not compress images
SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary

# Do not compress binaries
SetEnvIfNoCase Request_URI \.(?:exe|t?gz|zip|bz2|rar)$ no-gzip dont-vary


# Other configuration options

DeflateBufferSize 65535
DeflateCompressionLevel 9
DeflateFilterNote input instream
DeflateFilterNote output outstream
DeflateFilterNote ratio ratio

# LogFormat Basic
#  LogFormat '"%r" In:%{instream}n  Out: %{outstream}n Comp.:%{ratio}n%%'
deflate

# LogFormat Full
  LogFormat '%t | Cliente:%h(%a) | %>s | %B | "%r" | In:%{instream}n Out:
%{outstream}n Comp:%{ratio}n%% Tempo:%D/%T' deflate

# Log file to be generated
CustomLog logs/deflate.log deflate

# DeflateMemLevel Value
# How much memory should be used by zlib compression is. Value
between 1 and 9
# Default: DeflateMemLevel 9

# DeflateWindowSize Value
# Zlib compression window size. Value between 1 and 15
# Default: DeflateWindowSize 15
# </Location>
</IfModule>
# ---- End of HTTP COMPRESSION CONFIGURATION -----
```

1.07 Installing OpenSSL (optional)

1) Download the Windows version of OpenSSL (http://www.slproweb.com/download/Win32OpenSSL-v0.9.8.exe)

2) To install OpenSSL, double-click on the file *"Win32OpenSSL-v0.9.8.exe"* and follow the steps below:

3) Welcome screen of the program's installation OpenSSL. Click **[Next]** to go to the screen with a license to use the OpenSSL.

4) License to use the OpenSSL. Read the terms and select an option to accept or not the terms. If you do not accept the license terms, the installation program will be terminated. Click **[Next]**.

5) Choose the directory where the OpenSSL files will be installed. We recommend you use the default path as suggested by the installer. Click **[Next]**.

6) Select the name and location where the shortcuts in the start menu should be created. I advise you to use the default path as a suggestion offered by the installer. Click **[Next]**.

7) Review the options you chose earlier. When are all correct, click **[Install]**.

8) The installation program will copy all the files to your hard drive.
After completion of copying the files, click **[Finish]** to close the installation program.

1.08 Create test certificates

1) Open from "Command Prompt." Navigate to the directory "/bin" in your installation of OpenSSL.

2) Click "Start" and then "Run." The following screen will appear. Then run the command "CD C:\OpenSSL\bin".

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp..
C:\Documents and Settings\Administrator> cd C:\OpenSSL\bin
C:\OpenSSL\bin>
```

3) Log on to Windows as user "administrator".

4) Now let's create the test certificate to the server. In the "prompt" of command run the command "openssl openssl req-config. Cnf-new-out-my servidor.csr" and fill in the information that the program requires.

5) By default adopt the server name as the file name of certificates and keys. Ex: servername.csr, servername.key

```
C:\OpenSSL\bin> openssl req -config openssl.cnf -new -out my-
server.csr
Loading "screen" into random state - done


Generating to 1024 bit RSA private key
.++++++
.............++++++
writing new private key to "privkey.pem"
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
```

```
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter ".", The field will be left blank.
-----
Country Name (2 letter code) [AU]: BR
State or Province Name (full name) [Some-State]: Federal District
Locality Name (eg, city) []: Brasilia
Organization Name (eg, company) [Secretary of Finance of the DF]:
Organizational Unit Name (eg, section) [GESIS]:
Common Name (eg, YOUR name) []: www.lscalado.com
Email Address []: lscalado@blog.lscalado.com
Please enter the following "extra" attributes
to be sent with your certificate request
The challenge password []: secretpass
An optional company name []: secretpass

C:\OpenSSL\bin>
```

6) When you are prompted to fill in the "Common Name", give the exact name of the server it means that the certificate belongs to that server. The browser issue a warning when the name of the certificate and the name of the host web server does not match.

7) Run the command

```
#openssl rsa -in privkey.pem -out my-server.key
```

This removes the passphrase of the private key. You have to understand, this means that my-server. Key must only be readable by the Apache server and administrator. You MUST delete the file ".rnd" because it contains the information of "entropy" to create the key and could be used for attacks against your private key cryptography.

8) Now run the command

```
#openssl x509 -in my-server.csr -out my-server.cert -req -signkey-
my-server.key  -days 365
```

This command creates a signed certificate that you can use to get a certificate "real" of a certification authority. (This is optional: if you know your users tell you that you can install the certificate in their browsers).

9) Note that license expires in a year. You can increase this by changing the value after the "-days 365".

10) Create a new directory inside called "ssl" within the directory "Apache2 \ conf" and copy the files "my-server. Key" and "my-server.cert" for him.

1.09 Setup module in Apache mod_ssl

1) Module normally in the distribution of Apache. If not, download the http://modules.apache.org

2) You'll also need to download the file "ssl.conf" and put into the directory "C:\Apache2\conf."

3) Download your mod_ssl, if not with the Apache, and place in the "c:\apache2\modules".

4) Open the file "httpd.conf" you'll find in "Apache2\conf" and find the "LoadModule", uncheck the comment (#), if any, on the line that drives the cargo module of mod_ssl:

```
LoadModule ssl_module modules/mod_ssl.so
```

5) and add the following line, after the statements "LoadModule":

```
<IfModule Mod_ssl.c>
Include conf/ssl.conf
</IfModule>
```

6) After </IfModule> add:

```
SSLMutex default
SSLRandomSeed startup BUILTIN
SSLSessionCache none
```

7) Open the file ssl.conf and properly configure your domain and DocumentRoot (the place where you will serve your documents safe). Tip: next model of ssl.conf below:

```
#<IfDefine SSL>

Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl    .crl

#SSLPassPhraseDialog  builtin
#SSLSessionCache        none
#SSLSessionCache        shmht:logs/ssl_scache(512000)
#SSLSessionCache        shmcb:logs/ssl_scache(512000)
SSLSessionCache         dbm:logs/ssl-scache.log
SSLSessionCacheTimeout  300

#SSLMutex  file:logs/ssl_mutex.log
SSLMutex default

SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random  512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random  512
#SSLRandomSeed connect file:/dev/urandom 512

##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>

#  General setup for the virtual host
DocumentRoot "C:/Apache/ssl-htdocs"
ServerName <nomedoservidor>:443
ServerAdmin <administrator´s e-mail>
ErrorLog logs/error.log
TransferLog logs/access.log

SSLEngine on
```

```
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:
+SSLv2:+EXP:+eNULL
SSLCertificateFile "C:/Apache/conf/ssl/crt/Farm-Apache.cer"
SSLCertificateKeyFile "C:/Apache/conf/ssl/crt/Farm-Apache.key"
#SSLCertificateChainFile conf/ssl.crt/ca.crt
#SSLCACertificatePath conf/ssl.crt
#SSLCACertificateFile conf/ssl.crt/CACert.crt
SSLCACertificatePath "C:/Apache/conf/ssl/crt"
SSLCACertificateFile "C:/Apache/conf/ssl/crt/CACert.cer"
#SSLCARevocationPath conf/ssl.crl
#SSLCARevocationFile conf/ssl.crl/ca-bundle.crl
SSLVerifyClient optional_no_ca
SSLVerifyDepth  1

#   Access Control:
#   With SSLRequire you can do per-directory access control based
#   on arbitrary complex boolean expressions containing server
#   variable checks and other lookup directives.  The syntax is a
#   mixture between C and Perl.  See the mod_ssl documentation
#   for more details.
#<Location>
#SSLRequire (    %{SSL_CIPHER} !~ m/^(EXP|NULL)/ \
#            and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd." \
#            and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"} \
#            and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5 \
#            and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20       ) \
#           or %{REMOTE_ADDR} =~ m/^192\.76\.162\.[0-9]+$/
#</Location>

#SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars
+StrictRequire
SSLOptions +StdEnvVars

<Files ~ "\.(cgi|shtml|phtml|php3?)$">
 SSLOptions +StdEnvVars
</Files>

<Directory "C:/Apache/ssl-htdocs">
   Options Indexes FollowSymLinks
   AllowOverride None
   Order allow,deny
   Allow from all
   SSLOptions +StdEnvVars +ExportCertData
</Directory>

#   "force-response-1.0" for this.
SetEnvIf User-Agent ".*MSIE.*" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0

#   Per-Server Logging:
#   The home of a custom SSL log file. Use this when you want a
#   compact non-error SSL logfile on a virtual host basis.
CustomLog logs/ssl_request_log \
       "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
#</IfDefine>
```

+ StdEnvVars: Includes environmental variables on the SSL client and server unless their certificates coded

+ ExportCertData: Optionally, you can include two environmental variables containing the certificates of client and server.

8) Restart Apache and visit https://localhost to see you locally that everything is correct and then to the domain that you have configured for example http://servername/extpascal/srvextpascal

1.10 Environmental variables generated by Apache

Variable Name:	Value Type:	Description:
HTTPS	flag	HTTPS is being used.
SSL_PROTOCOL	string	The SSL protocol version (SSLv2, SSLv3, TLSv1)
SSL_SESSION_ID	string	The hex-encoded SSL session id
SSL_CIPHER	string	The cipher specification name
SSL_CIPHER_EXPORT	string	true if cipher is an export cipher
SSL_CIPHER_USEKEYSIZE	number	Number of cipher bits (actually used)
SSL_CIPHER_ALGKEYSIZE	number	Number of cipher bits (possible)
SSL_VERSION_INTERFACE	string	The program version mod_ssl
SSL_VERSION_LIBRARY	string	The OpenSSL program version
SSL_CLIENT_M_VERSION	string	The version of the client certificate
SSL_CLIENT_M_SERIAL	string	The serial of the client certificate
SSL_CLIENT_S_DN	string	Subject DN in client's certificate
SSL_CLIENT_S_DN_ *x509*	string	Component of client's Subject DN
SSL_CLIENT_I_DN	string	Issuer DN of client's certificate
SSL_CLIENT_I_DN_ *x509*	string	Component of client's Issuer DN
SSL_CLIENT_V_START	string	Validity of client's certificate (start time)
SSL_CLIENT_V_END	string	Validity of client's certificate (end time)
SSL_CLIENT_A_SIG	string	Algorithm used for the signature of client's certificate
SSL_CLIENT_A_KEY	string	Algorithm used for the public key of client's certificate

SSL_CLIENT_CERT	string	PEM-encoded client certificate
SSL_CLIENT_CERT_CHAIN *n*	string	PEM-encoded client certificates in certificate chain
SSL_CLIENT_VERIFY	string	NONE, SUCCESS, Generous or FAILED: *reason*
SSL_SERVER_M_VERSION	string	The version of the server certificate
SSL_SERVER_M_SERIAL	string	The serial of the server certificate
SSL_SERVER_S_DN	string	Subject DN in server's certificate
SSL_SERVER_S_DN_ *x509*	string	Component of server's Subject DN
SSL_SERVER_I_DN	string	Issuer DN of server's certificate
SSL_SERVER_I_DN_ *x509*	string	Component of server's Issuer DN
SSL_SERVER_V_START	string	Validity of server's certificate (start time)
SSL_SERVER_V_END	string	Validity of server's certificate (end time)
SSL_SERVER_A_SIG	string	Algorithm used for the signature of server's certificate
SSL_SERVER_A_KEY	string	Algorithm used for the public key of server's certificate
SSL_SERVER_CERT	string	PEM-encoded server certificate
[Where *x509* is a component of the X.509 C,ST,L,O,OU,CN,T,I,G,S,D,UID,Email C, C,ST,L,O,OU,CN,T,I,G,S,D,UID,Email		

2 Windows + IIS

2.01 Installing and configuring IIS 6.0

1) To install IIS, click on Start> Control Panel> Add or Remove Programs> Add or Remove Windows Components> select Application Server and Certificate Server> click Next. Click OK. Follow the instructions to continue the installation
2) To begin configuring IIS, click on Start> Control Panel> Administrative Tools> click Internet Information Service (IIS) Manager
3) Create the folders Ext, Extpascal, CGI-BIN, and ExtPascalSamples.exe Place CGIGateway.exe as indicated in the procedure for setting up the Apache environment.
4) In the TCP Port field, leave as is (80) and the SSL_Port: leave blank to generate certificates and configure the SSL mode. Click Next.
   Note: Although, by default, IIS create the folder /inetpub in the primary partition (C: drive) to house the archives of the site there, suggest its installation in a partition of data other than the system partition for the sake of security and ease of maintenance .
5) The next screen asks the permissions that will be implemented in the folder used to store the files on your site. It is advisable to leave only the options Read and Run scripts enabled. Click Next to finish the installation.
6) Now that you've built your site, we set it up! Double-click Web Sites> click with the right mouse button on the site created> Properties. When opening a new window, you will have the following options:
   Description: contains the generic name of the site
   IP Address: indicates the site's IP
   TCP: It is the port used to access the site: 80
   SSL port: used only when there is need for encryption, 443 being the default.
   Connection Timeout: time as the server waits until a user disconnects inactive
   Enable the HTTP Keep-Alive: it allows the connection is kept open rather than open it to each connection held
   Enable logging: allows you to create log files for access to the server (something important for audit)
7) Click on Properties to configure the logs:

   Click Daily (order to create a log file per day), click Use local time for file naming and overlapping so that the date/time of the log is the same server (using the time of the W3C, which is the same as Greenwich).

   In Directory of the log file, type the folder where you saved the log files.

   Compaction of the contents of the folder of log

   To enable compression, click on Start> My Computer> double-click on the partition where the log files are located>-click the right mouse in the folder where the log files are located> Properties> Advanced> click Compress the contents to save disk space> click OK> click Apply changes to this folder, sub-

folders and files and click OK.
The lower the number of files there, the faster the job is finalized. After compression, the portfolio will be with the color blue, indicating that there are compressed data.

The compression of the log folder does not influence the way the remarkable performance of the server.

8) Security directory: allows you to configure the type of authentication and access control, the IP restrictions and field (so you stop access to your site) and communications security (certificates for secure communication channel and security SSL).

9) Enabling HTTP Compression IIS 6
To enable compression (which is in the kernel and does not influence the performance of the server), you must click with the right mouse button on Web Sites> Services tab. Click on Options Compact Compact and application files of static files. In the maximum size of the temporary directory, leave at Unlimited. Click OK.

2.02 Framework ExtJS

2.02.1 Installation

1) Download the package ExtJS in version 2.1:

```
http://www.extjs.com/products/extjs/download.php?dl=extjs21
```

2) Extract the contents of the package Ext-2.1.zip in the root folder of your site's default web server on the same level of folders cgi-bin and FastCGI. On the server IIS:

```
C:\inetpub\wwwroot\ext
```

2.03 Installation of Gateway CGI (if applicable)

Copy the file to the folder CGIGateway.exe cgi-bin located in the root folder of your Web server (c:\inetpub\wwwroot\cgi-bin\) which will be hosted the secure website (SSL)

2.04 Traffic Compression

1) Start Internet Information Services, where he still is not running.
Expand the name of the web server

2) Right-click the mouse **in** the **"Web Sites"** and then click Properties.

3) Click the **"Service".**

4) In the panel **"HTTP Compression"** check the option **"Compress Application Files" and "Static Compress Files."** ***Click*** **[Ok]** ***to*** accept the changes.

2.05 Installing CA Service

1) To install IIS, click on Start> Control Panel> Add or Remove Programs> Add or Remove Windows Components> select Certificate Server> click Yes in the notice that appears> click Next.
2) On page "CA Type" select the "Stand-alone root CA." Click **[Next]**.
3) On page "CA Identifying Information", fill the "Common Name" with the following: "root CA <servername>." "Distinguish Name" is optional and in "Validity Period" choose the time you want and click **[Next]**.
4) On the "Certificate Database Settings" leave as is or adjust if necessary and click **[Next]**.
5) It will display a notice saying that temporarily stop the IIS service. Click **[Yes]**.
6) Please wait until the installation and click **[Finish]**.

2.06 Generate a Certificate Signing Request

1) Start the MMC snap-in (Microsoft Management Console) IIS.
2) Expand the server name and select the Web site you may want to install a certificate.
3) Right-click the mouse on the site and click on **"Properties".**
4) Click the **"Directory Security".**
5) Click on the **"Certificate Server"** under **"Secure Comunications"** to launch the Web Server Certificate Click **[Next]** to exit the dialogue of Welcome.
6) Choose **"Create a new certificate"** and click **[Next]*.***
7) The dialog has the following two options:
   a) ***"Prepare the request now, but send it later."***
   b) ***"Send the request immediately to an online certification authority."***
8) Click ***"Prepare the request now, but send it later"*** and click **[Next]*.***
9) Enter a descriptive name for the certificate in the Name field, for example "IIS server - <Server name>", choose " 1024 " for the length in bits for the key field size bit**.** The wizard uses the name of the current site as a default name. He is not used in the certificate, but appears in the "friendly name" and serves as a friendly name to help administrators to identify the certificate. Click **[Next]*.***
10) Enter the name of an organization want (Department of Finance of the Federal District) in the Organization and enter an organizational unit (GESIS) in the organizational unit and click **[Next]*.***
    In the Common Name field, type the server name and click **[Next]**.
    Important: The common name is one of the most significant information ending the certificate. It is the DNS name of the site (ie, the name that users

enter when navigating the site). If the name of the certificate does not match the name of the site, you reported an issue of certificate when users browse the site.
If the site is the Web and is named www.contoso.com, is what must be specified for a common name.
If the site is internal and users browse by computer name, enter the DNS or NetBIOS name of the computer.

11) Enter the appropriate information in the fields **Country/Region, State/Province and City/locality** and click **[Next].**

12) Enter a file name for the certificate request. Preferably the server name ***Click* [Next].** The wizard displays a summary of the information contained in the request for the certificate.

13) ***Click* [Next] *and*** click **[Finish]** to complete the inquiry.
The request for the certificate can now be sent to a certification authority for purposes of verification and processing. After receiving a response on the certificate of the certifying authority, you can continue to install the certificate on the Web server, again using the IIS Certificate Wizard.

2.07 Submit a request for a certificate of service

1) Use Notepad to open the certificate generated in the previous procedure and copy all its contents to the clipboard.

2) Start Internet Explorer and browse to http://hostname/CertSrv, where hostname is the name of the computer running Microsoft Certified Services.

3) Click on **"Request a certificate"** and ***click* [Next].**

4) Request a Certificate page**,** click on **"Advanced Certificate Request" and *click* [Next].**

5) On the **"Advanced Certificate Request"**, click on **"Submit a certificate request by using the base-64-encoded ..."**. Submit a certificate request file using a base64 encoded PKCS # 10 and click Next.

6) On the **"Submit a Request or Certificate Renewal** Request," click on the text box **"Saved Request"** Base-64-encoded certificate request (PKCS # 10 or # 7) and press CTRL + V to paste the certificate request copied earlier in clipboard, (item 1). Click **[Next].**

7) Note the number of identification of its request (Request ID) informed and move to the next step: to issue the certificate.

2.08 Issue the certificate of service

1) Start the Certification Authority tool in the Administrative Tools program group.

2) Expand the newly created CA with the name given by Common Name the item certification authority and select the Pending Requests folder.

3) Open the folder **"Pending Requests"** and select the application for a certificate you just send.

4) On the menu **"Action"** point to **"All Tasks"** and click **"Issue."**

5) Confirm that the certificate is displayed in the **"Issued Certificates"** and double-click it to exhibit it.

6) On the **"Details",** click **"Copy to file"** and save the certificate as an X.509 certificate Base-64 encoded. Tip of name "servername-cs-iis" (cs = certificate server for IIS) to differentiate the certificate generated by OpenSSL for Apache. Click **[Next].**

7) Click **[Finish].** Quit the application

2.09 Installing the certificate on the web server

1) Start Internet Information Services, where he still is not running.
Expand the server name and select the site you may want to install a certificate.

2) Right-click the mouse on the site and click Properties.

3) Click the **"Directory Security".**

4) Click on the **"Certificate Server"** under **"Secure Comunications"** to launch the Web Server Certificate Click **[Next]** to exit the dialogue of Welcome.

5) Select **"Process the pending request and install the certificate"** and click **[Next]**.

6) Enter the path and file name that contains the server certificate generated before or navigate to it by clicking **[Browse]** and click **[Next].**

7) Set the port 443 in **"SSL Port this web site should use"** and click **[Next].**

8) Examine the overview of the certificate, click **[Next]** and click **[Finish].**

9) A certificate is now installed on the server Web

2.10 Set resources to require access to SSL

1) Start Internet Information Services, where he still is not running.

2) Expand the server name and site whose certificate has been installed in the previous item.

3) Right-click the mouse on the Default Web Site and click **"Properties".**

4) Click the Directory Security tab.

5) In **"Secure Comunications"** click **"Edit".**

6) Check **"Require Secure Channel (SSL)."**
In the navigation to this virtual directory, you must now use HTTPS.

7) In the panel **"client certificates"** to choose appropriate to its needs, knowing that:
Ignore Client Certificates: Do not require licenses for access to the site
Accept Client Certificates: enables users to access the certificate of customers without requiring the certificate. Users with client certificate can be mapped; users without client certificate can use other authentication methods.

Require Client Certificates: Allows users to connect only with valid client certificate. Users without valid certificate does not have permission to access this site.

For testing purposes of certificate **select "Require ...",** which should also be an option used in production.

2.11 Request client certificate

1) Start Internet Explorer and browse to http://hostname/CertSrv, where hostname is the name of the computer running Microsoft Certified Services.
2) Click on **"Request a certificate"** and click **[Next].**
3) Request a Certificate page**,** click on **"Advanced Certificate Request."**
4) On the **"Advanced Certificate Request"** Click **"Create and submit a request to this CA"**
5) When they open the fields fill in the information group's **"Identifying Information." Select "Client Authentication Certificate"** from **"Type of Certificate Needed."** In **"Options key"** check **"Mark the key exportable."** Click **[Submit].**
6) Note the number of identification of its request (Request ID) informed and move to the next step: to issue the certificate.

2.12 Issue the client certificate

1) Start the Certification Authority tool in the Administrative Tools program group.
2) Expand the newly created CA with the name given by Common Name the item certification authority and select the Pending Requests folder.
3) Open the folder **"Pending Requests"** and **select** the application for a certificate you just send.
4) On the menu **"Action"** point to **"All Tasks"** and click **"Issue."**
5) Confirm that the certificate is displayed in the **"Issued Certificates"** and double-click it to exhibit it.
6) Click **[Finish].** Quit the application
7) Restart Internet Explorer and browse to http://hostname/CertSrv, where hostname is the name of the computer running Microsoft Certified Services, in the case http://servername/certsrv.
8) Click **"View the status of the Pending Certificate Request."**
9) On the next page click **"Client Certificate Authentication ...."** Check the date if the certificate is required
10) Then click **"Install this certificate"**
11) And the certificate is installed in the browser from which this procedure was performed. To use it in other browsers and other stations use the option of exporting from your browser and import the certificate generated in the browser destination.

2.13 Accepting third-party certificates

For the server accepted certificates issued by third-parties, certificates of each CA belonging to his chain of certification authorities should be installed. In the specific case of ICP-Brazil, the certificates of all CAs that composes. Can be downloaded from the site of the ITI (www.iti.gov.br).

2.14 Comments on certificates in IIS

When we tested the use of certifacate in a token issued by Brasilian Federal Revenue, IIS rejected the connections accusing errors 403.16, 403.13 in Internet Explorer and Firefox in error 403.7. The problem was this: even though the license has its hierarchy of certification authorities and all certificates of AC have been installed, IIS continued accusing the same mistakes. After some testing and research, it was found that IIS demand the list of licenses revoked the license customer, the URI described in the certificate called "the CRL Distribution Point" (in English: CDP). In IIS the recovery of the list of revoked certificates informed must be completed within 15 seconds, if not the application for certification is rejected. To circumvent this problem must be manually download the URI indicated in the field, the file containing the list and install it on the server. Note that this list should be specific. If you download any of the lists of the Certification Authority Web site operation is not complete.

2.15 Structure of folders

Below the folder corresponding to Default Web Site (c:\inetpub\wwwroot\) create a folder cgi-bin folder on the same level of the item 2.02.1 ext created that will contain the "gateway cgi" (cgigateway.cgi or any other name though you want to assign to the executable)

2.16 Environmental variables generated by IIS

Variable	Description
ALL_HTTP	List all the HTTP headers sent by the client browser to the server. Information such as: host home, the home page, the browser client features, among others.
ALL_RAW	Return all information sent by HTTP header of the page in its original state (Raw). The difference between ALL_RAW and ALL_HTTP is that ALL_HTTP poses a HTTP_ prefix before the name of the header and the name of the header always in all caps. In ALL_RAW the name of the header and value appear as they are sent by the client.
APP_POOL_ID	Returns the name of the application pool that is running in the IIS worker process that is handling the

IIS 5.1 and earlier: This server variable is not available.	request. There is also an APP_POOL_ID environment variable that is available to applications that are running in the IIS worker process.
APPL_MD_PATH	Return the logical path of the ASP file in question (the metabase path).
APPL_PHYSICAL_PATH	Physical path of the file to disk. This is the logical path of APPL_MD_PATH (metabase path of)
AUTH_PASSWORD	Password referring to the user logged on. This variable is only available in the basic mode of authentication (basic authentication). For this, you need to be done by the login dialog box to request the page.
AUTH_TYPE	Authentication method used by the server to validate users who request a script. It does not mean that the user was Authenticated if AUTH_TYPE contains the value and the authentication scheme is not Basic or integrated Windows authentication. The server allows authentication schemes it does not natively support because an ISAPI filter may be able to handle that particular scheme.
AUTH_USER	Username provided to the server in the event of did not allow anonymous access to the directory. This may be the name of a user domain or Windows user. The name of the user as it is derived from the authorization header sent by the client, before the user name is Mapped to a Windows account. This variable is no different from REMOTE_USER. If you have an authentication filter installed on your Web server that maps incoming users to accounts, use LOGON_USER to view the Mapped user name.
CACHE_URL IIS 5.1 and earlier: This server variable is not available.	For use in ISAPI applications only. Returns the unambiguous name for the current URL. It is necessary to use the Unicode version of this variable in conjunction with the kernel mode cache invalidation function to evict entries placed in the cache by HSE_REQ_VECTOR_SEND.

	Note: The server variable "UNICODE_CACHE_URL" is used in conjunction with the cache invalidation function retrieved by the HSE_REQ_GET_CACHE_INVALIDATION_CALLBACK function. This function invalidates cached in HTTP.SYS responses, whether those responses are produced by requests or by calling ISAPI HSE_REQ_VECTOR_SEND.
CERT_COOKIE	Unique identification of the customer's digital certificate Unique ID for the client certificate, returned as a string. This can be used as a signature for the whole client certificate.
CERT_FLAGS	Value of two bits: bit 0 equal to 1 indicates whether the client's certificate is present, bit 1 equals 1, indicates that the certifying authority of the client certificate is invalid. bit0 is September to 1 if the client certificate is present. bit1 is September to 1 if the certification authority of the client certificate is invalid (that is, it is not in the list of recognized certification authorities on the server). If bit 1 of CERT_FLAGS is September to 1, indicating that the certificate is invalid, IIS version 4.0 and later will reject the certificate. Earlier versions of IIS will not reject the certificate.
CERT_ISSUER	Issuer field of the certificate of the client (O = MS, OR = IAS, CN = user, C = USA)
CERT_KEYSIZE	Number of bits in key connection Secure Sockets Layer - SSL. Ex: 64, 128
CERT_SECRETKEYSIZE	Number of bits in the key of "Server certificate private" (private key). Ex: 1024
CERT_SERIALNUMBER	Serial Number field of digital certificate from the client
CERT_SERVER_ISSUER	Issuer field of the certificate server
CERT_SERVER_SUBJECT	Subject field of the server's SSL certificate

CERT_SUBJECT	Subject field of the certificate of client
CONTENT_LENGTH	Size in bytes, the contents of a request made by the client to server.
CONTENT_TYPE	Type of request sent to the server by the client. The data type of the content. Used with queries that have attached information, such as the HTTP queries GET, POST, and PUT.
GATEWAY_INTERFACE	Number of revision of the CGI specification used in the web server to handle the request (request). The format is CGI/Review
HEADER_ <HeaderName> IIS 5.1 and earlier: This server variable is not available.	The value stored in the header <HeaderName>. Any header other than those listed in this table must be preceded by "HEADER_" in order for the ServerVariables collection to retrieve its value. This is useful for Retrieving custom headers. Note: Unlike HTTP_ <HeaderName>, all characters in HEADER_ <HeaderName> are interpreted as-is. For example, if you specify HEADER_MY_HEADER, the server searches for a request header named MY_HEADER.
HTTP_ <HeaderName>	Value stored in the header specified. We can highlight the most common: HTTP_ACCEPT, HTTP_ACCEPT_ENCODING, HTTP_ACCEPT_LANGUAGE, HTTP_COOKIE, HTTP_USER_AGENT, HTTP_REFERER. The value stored in the header <HeaderName>. Any header other than those listed in this table must be preceded by "HTTP_" in order for the ServerVariables collection to retrieve its value. This is useful for Retrieving custom headers. Note: The server interprets any underscore (_) characters in the <HeaderName> dash in the current header. For example, if you specify HTTP_MY_HEADER, the server searches for a request header named MY-HEADER.
HTTP_ACCEPT	Returns the value of the Accept header that contains the list of accepted formats, for example, "image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,

	application/vnd.ms-excel." The values of the fields for the variable HTTP_ACCEPT are concatenated, and separated by a comma (,).
HTTP_ACCEPT_ENCODING	Returns the list of accepted encoding types, for example, "gzip, Deflate."
HTTP_ACCEPT_LANGUAGE	Returns the string Describing the language to use for displaying content.
HTTP_CONNECTION	Returns the string Describing the connection type, for example, "Keep-Alive".
HTTP_COOKIE	Returns the string cookie that was included with the request.
HTTP_HOST	Returns the name of the Web server. This may or may not be the same server_name depending on the type of name resolution you are using on your Web server (IP address, host header).
HTTP_METHOD	The method used to make the request (same as REQUEST_METHOD).
HTTP_REFERER	Returns the string that contains the URL of the page that referred the request to the current page using an HTML tag <A>. Note that the URL is the one that the user typed into the browser address bar, which may not include the name of the default document. If the page is redirected, HTTP_REFERER is empty. HTTP_REFERER is not a mandatory member of the HTTP specification.
HTTP_URL	Returns the raw, encoded URL, for example, "/vdi/default.asp? Querystring."
HTTP_USER_AGENT	Returns the string Describing the browser that sent the request.
HTTP_VERSION	The name and version of the protocol request (the raw form of SERVER_PROTOCOL).
HTTPS	Return to request an inquiry, saying that the channel is safe (ON) or unsafe (OFF). Returns on if the request came in through a secure channel (for example, SSL), or it returns OFF, if the request is for an insecure channel.
HTTPS_KEYSIZE	Number of bits in key connection Secure Sockets Layer

	- SSL.
HTTPS_SECRETKEYSIZE	Number of bits in the private key of the server certificate
HTTPS_SERVER_ISSUER	Issuer field of the certificate from the server.
HTTPS_SERVER_SUBJECT	Field subject of the certificate from the server.
INSTANCE_ID	ID, in text format, for instance of Internet Information Server (IIS). The ID for the IIS instance in textual format. If the instance ID is 1, it appears as a string. You can use this variable to retrieve the ID of the Web server instance (in the metabase) to which the request belongs.
INSTANCE_META_PATH	The metabase path for the instance of Internet Information Server (IIS) that responds to the request (request)
LOCAL_ADDR	Return the logical address of the server where the request was made (the address of the server where the file named). This is important on computers that may have multiple IP configured and wants to know which address the request was made.
LOGON_USER	The user account used to log into Windows. The Windows account that the user is impersonating while connected to your Web server. Use REMOTE_USER, UNMAPPED_REMOTE_USER, or AUTH_USER to view the raw user name that is contained in the request header. The only time LOGON_USER holds a different value than these other variables is if you have an authentication filter installed.
PATH_INFO	Virtual path of the file that held the requisition, starting from the root of the server. Eg /files/documento.asp Path information, those given by the client, for example, "/vdir/myisapi.dll/zip." If this information comes from a URL, it is decoded by the server before it is passed to the CGI script or ISAPI filter. If the AllowPathInfoForScriptMappings metabase property to Sept is true (to support exclusive functionality CGI), PATH_INFO will only contain "/zip" and ISAPI applications such as ASP will break.

PATH_TRANSLATED	Version of the variable PATH_INFO "turned into physical path. The physical path that maps to the virtual path in PATH_INFO, for example, "c: \ inetpub \ wwwroot \ vdir \ myisapi.dll." This variable is used by IIS during the processing of ISAPI applications. If the AllowPathInfoForScriptMappings metabase property to Sept is true (to support exclusive functionality CGI), PATH_INFO will only contain "/zip" and ISAPI applications such as ASP will break.

3 Fedora Linux 9 + Apache 2.2

3.01 Installing Linux Fedora 9

1) Install from the distribution Fedora-9-i386-dvd.iso;

2) Language: <your language>
   Keyboard: <your keyboard>

3) Network Devices - Edit - disable IPv6 support if necessary
   Name of the machine: set manually: <server name>

4) Various settings: none

5) Time zone: <your time zone>

6) Root password: <password>

7) Hard Disk Partitioning:
   "Remove Linux partition in selected disks and create default layout
   - Mark "review layout pattern"
   click **[Next]** - "save changes to disk"
   - Partitioning and give **[Next]**;
   - List of operating systems, click on the line of Fedora and click [Edit];
   - Label = Fedora 9, **[Next]**;

8) Selection of applications
   - Check all (Office and Productivity, Software Development and Web Server
   - In "additional repositories leave only" Fedora "marked
   - Mark "customize now" and **[Next]**;

9) Note:
   Items preceded by:
   "**O**" will have no subitens selected for installation.
   "**X**" will have subitens selected to be installed.are listed. Only those marked to be installed are listed

10) Working Environment:
   X - Gnome

11) Applications
   O - Authorship and Publication
   X - Editors
      Vim
   O - Engineering and Science
   O - Office and Productivity
   X - Graphics
      Image Magik
   O - Internet in GUI
   X - Internet in text mode
      Elinks
   O - Games and Entertainment
   O - Educational Software
   X - Sound & Video
      Alsa-plugins
      K3B

12) Development
X - Libraries Development
binutils
lib * - all
lockdev
openldap
openssl
pcsc-lite
O - WEB Development
O - Gnome Development
O - KDE Development
O - Legacy Development
O - X Development
O - Development XFCE
O - Java Development
O - packer Fedora
O - Fedora Eclipse
X - Development Tools
automake 17
elfutils
indent
ltrace
subversion
O - Ruby

13) Servers
- MySQL
O - PostGreSQL
O - Clustering
X - Configuration Tools
all
X - FTP Server
X - Web Server
pound
apachetop
awstat
crypto-utils
distcache
httpd-manual
Webalizer
X - Windows Server Files
system-config-samba
O - Email Server
O - DNS server
O - Server News
O - Network server legacy
O - Network server
X - Support for printing
samba-client
system-config-printer

14) Base System_
X - Base

acpid, cpuspeed, dhclient, dosfstools, eject, FTP, gpm, ipstate, irqbalance, l ftp, logwatch, man-pages, mtools, ntfs-3g, ntfsprogs, openssh-clients, openssh-server, rdist, redhat-lsb, rsync, setuptool, sudo, symlinks, sysreports, system-config-firewall, system-config-network, talk, tcpdump, time, tree, unzip, usbutils, wget, which, yum, yum-utils, zip

X - Administration Tools
authconfig-gtk
gnome-packagekit
system-config-date
system-config-firewall
system-config-keyboard
system-config-network
system-config-users

X - System Tools
fuse
ntfs-3g
samba-client
screen
vnc
yum-utils

O - Sources

X - Sources legacy
bitmap, xorg-x11-100dpi, xorg-x11-iso8859-1, xorg-x11-iso8859-9, xorg-x11-Type1, xorg-x11-fonts-misc

O - Java

O - Legacy Software Support

O - Hardware Support

O - Dialup Network Support

X - XWindows System
authconfig-gtk
gdm
gnome-packagekit
kerneloops
openssh-askpass
policycoreutils
rhgb
setroubleshoot
system-config-* (all)
vnc
xorg-x11-apps
xorg-x11-utils
xterm

15) Languages
X – Desired languages

16) After the 1st boot on the Welcome screen click **[Next]**

17) After reading the license terms, click **[Next]**

18) Create a user and **[Next]**

19) Set date and time and **[Finish]**

20) After the restart normal, log on as root (accuses error of kernel, then solve)

21) In some cases the network's may use Microsoft's proxy ISA and require authentication, and that authentication via NTLM be owned by Microsoft, initially the machine will not have access to external networks.
To access external networks and download packages is necessary first to configure Firefox, which is the only Linux application that recognizes the Microsoft´s authentication protocol.
Copy the package "tar" from Firefox to a temporary folder and run the commands below:

```
# tar xvjf firefox-xxx.bz2 -C /usr/lib/
# cd /usr/bin/
# ln -sf /usr/lib/firefox/firefox ./
```

22) Setting launch menu on the screen or on the desktop if you want pointing to the application in /usr/bin/firefox

23) Setting the standard proxy network.

24) Adjust video settings

25) If a proxy/firewall Microsoft ISA Server, install NTLMaps
download the latest version of NTLMaps at:
http://sourceforge.net/project/showfiles.php?group_id=69259
and run the following commands:

```
# tar xvzf ntlmaps-xxx.tar.gz -C /usr/local
# cd /usr/local/
# mv ntlmaps-xxx ntlmaps
# cd ntlmaps
```

where xxx is the version number of NTLMaps

create a copy of the file server.cfg and edit it. The following configurations needed:

```
LISTEN_PORT: 5865 (default)
PARENT_PROXY: 10.70.1.20
PARENT_PROXY_PORT: 80
NT_DOMAIN: <domain name>
USER: <user name>
PASSWORD: <password>
LM_PART: 0
NT_PART: 1
NTLM_FLAGS: 05820000
NTLM_TO_BASIC: 0
```

26) Note: the settings on the pattern of LM authentication or NT are LM_PART: 1, NT_PART: 0 and NTLM_FLAGS: 06820000 by default, but I decided change. I do not know but it makes a difference in the way the NT encryption is more secure through the doubts and opted for NT.

27) Add the following line to the end of /etc/rc.d/rc.local if you want the authentication server start automatically:

```
# python /usr/local/ntlmaps/main.py
```

28) As a rule the majority of Linux applications that allow the configuration of proxy accept the environmental variables:
"http_proxy", "ftp_proxy" in the formats:

export http_proxy = http:// <username>: <password> @ host: port, or
export http_proxy = http://host:port

29) If the application may not make use of variables, so they must be individually configured to use the proxy at the address 127.0.0.1, port 5865.

30) For Yum, for example, as an alternative to the use of environmental variables, can be changed /etc/yum.conf to contain the proxy settings.

In order to avoid exposing the password for authentication on the proxy it can be omitted in the server.cfg, but in this case the server asks for the password. If the service is activated in the background (&) will not be asked for the password and proxy not authenticate the connections.

The best solution is to omit the password for the file server.cfg, configuring the environmental variables "http_proxy" without the password, and the fire service manually (by a script for example), then the server when you request a password. Tip of script:

```
# python /usrs/local/ntlmaps/main.py
```

31) In the specific case of Firefox you can choose to keep ntlmaps configured the proxy or proxy's original network, since it makes the authentication via NTLM.

3.02 Installation of Apache

Note: If you installed Fedora with Apache, then the configuration of Apache is a little different from what we suggest. The configuration file "httpd.conf" is in /etc/ httpd/conf/, the binary of the Apache (httpd) is in /usr/sbin/. The tools are in /usr/bin/. The root folder of the Web (DocumentRoot) is in /var/www/html/. Consider these differences to make the installation of packages needed to ExtPascal, following the road map below.

1) Download the latest package in
http://httpd.apache.org/download.cgi.
In this case httpd-2.2.9.tar.bz2

2) Unpack as described below:

```
# tar xvjf http-2.2.9.tar.bz2
# cd httpd-2.2.9
#./configure
# make
# make install
```

3) To start the service Apache (httpd) during the boot copy the script apachectl to the folder /etc/rc.d/init.d.
- Create symbolic links K99httpd and S99httpd the folders /etc/rc.d/rc3.d, /etc/rc.d/rc4.d and /etc/rc.d/rc5.d that are initlevels where apache will be initialized:

```
# cp /usr/local/apache2/bin/apachectl /etc/rc.d/init.d/httpd
# cd / etc/rc.d/rc3.d
# ln - s ../init.d/httpd K99httpd
# ln - s ../init.d/httpd S99httpd
# cd ../rc4.d
# ln -s ../init.d/httpd K99httpd
```

```
# ln -s ../init.d/httpd S99httpd
# cd ../rc5.d
# ln -s ../init.d/httpd K99httpd
# ln -s ../init.d/httpd S99httpd
```

3.03 Installation of the module FastCGI

1) Download the version 2.4.6 of http://www.fastcgi.com/dist/mod_fastcgi-2.4.6.tar.gz

2) Unpack the package downloaded and compile it using the procedures described below:

```
# tar xvzf mod_fastcgi-2.4.6.tar.gz
# cd mod_fastcgi-2.4.6
# cp Makefile.AP2 Makefile
# make
# make install
```

3) After these procedures the module 'mod_fastcgi. So "will be created and placed in the folder /usr/local/apache2/modules

4) Changing the httpd.conf to support the FastCGI module:

```
LoadModule fastcgi_module modules/mod_fastcgi.so

fastcgiexternalserver/<folder name>/<application name>
     -host <name host>:<socket> -idle-timeout <n>
```

Where <folder name> is the full name of the folder where you set your application and web <application name> is the name of the file that will be created to be referenced by the FastCGI module. To be referenced the module connects to the host of <name host>, using the socket <socket>, and awaits a reply by the time <n>

3.04 Install the package ExtJS

1) Download the package of ExtJS http://www.extjs.com/ .....

2) Putting it in the root folder of web DocumentRoot set in the httpd.conf file and run the following commands:

```
# unzip ext-2.2.zip
# mv ext 2.2-ext
```

3.05 Installing ExtPascal as Daemon

1) Put the executable binary in your preferred folder, e.g.: /usr/local/extpascal/

2) copy the shell script bellow (extpascalsampled) to /etc/init.d.

```
#!/bin/bash
#
# Startup script for the ExtPascalSamples Server
#
# chkconfig: 35 80 20
# description: The ExtPascalSamples Server
```

```
# process name: extpascalsamplesd
#
#
#
#
### BEGIN INIT INFO
# Provides: extpascalsamplesd
# Required-Start: $local_fs $remote_fs $network $named
# Required-Stop: $local_fs $remote_fs $network
# Should-Start: distcache
# Short-Description: start and stop extpascalsamples server
# Description: The ExtPascalSamples is an MDA Development Tool
#  implementing the current HTTP standards.
### END INIT INFO

# Source function library.
. /etc/init.d/functions

# Name of binary file
daemonname=extpascalsamplesd

# Full path to the server binary.
extpascalsamplesd='/usr/local/extpascal/extpascalsamplesd'

start() {
   echo $"Starting $daemonname..."
   $extpascalsamplesd &
   echo
}

stop() {
   echo $"Stopping $daemonname..."
   kill -KILL `pidof $daemonname`
   echo
}

# See how we were called.
case "$1" in
  start)
   start
   ;;
  stop)
   stop
   ;;
  restart)
   start
   ;;
  *)
   echo $"Usage: $prog {start|stop|restart}"
esac

exit $RETVAL
```

The commented line:

```
#chkconfig 35 20 80
```

says that the random script should be started in levels 3 and 5, that its start priority should be 20, and that its stop priority should be 80.

3) edit the shell script to reflect the folder you put the binary

4) run the command below to add the daemon to the chkconfig database:

```
#chkconfig –add extpascalsamplesd
```

5) to change run levels, for example, to run ExtPascal daemon in levels 2, 3, 4 and 5 run:

```
#chkconfig --level 2345 extpascalsamplesd on
```

to disable the daemon to not run in any level, run:

```
#chkconfig --level 2345 extpascalsamplesd off
```

6) to check ExtPascal run levels configuration run:

```
#chkconfig –list extpascalsamplesd
```

7) to start stop or restart the daemon run:

```
# service extpascalsamplesd {start | stop | restart}
```