Generate Server Private Key with Password Encryption

Introduction

As explained in Apache and SSL Certificates, passphrase encryption requires an administrator's intervention whenever the service is started.

As such, the current standard for Web Servers, is to **not** use password encryption and instead rely on the file system to protect the keys.

Having said that, in some cases the administrator may want to use password encryption.

Generating Server Private Key with Password Encryption

```
su bhitch # Use a sudo enabled account.
cd ~
mkdir private
sudo chmod 700 ./private
cd private
openssl genrsa -aes256 -out www.earth.com_server.key 2048
```

The openssl command reads,

- genrsa - generate asymmetric keys
- aes266- - protect the RSA key with a passphrase using CBC AES 256 symmetric key encyrption
- 2048 - make the RSA private key 2048 bit

> As of May 2011, most of the examples including the Apache 2.2 documentation use des3 and 1024. This was to accommodate older browsers. The standard has since changed to AES-256-CBC and 2048. Some CAs will no longer accept 1024.

Removing Password Encryption

To remove the password from the key file,

```
cp www.earth.com_server.key www.earth.com_server.key.bck # always good to
backup first
openssl rsa -in www.earth.com_server.key -out
www.earth.com_server.key.insecure
rm www.earth.com_server.key # delete the original file
mv www.earth.com_server.key.insecure www.earth.com_server.key
```