Renewing an SSL Certificate Provided by a Certificate Authority (CA) on the BlueSecure Controller (BSC)

Date: July 2, 2010
Revision: 2.0

Introduction
This document explains how to renew an SSL Certificate Provided by a Certificate Authority (CA) such as Verisign or Godaddy on the BlueSecure Controller (BSC).

Requirements
Ensure that you meet these requirements before you attempt this configuration:
- Knowledge of how to configure the BSC, Access Point, and client for basic operation.

Components Used
The information in this document is based on these hardware and software versions:
- All supported hardware platforms running current software image/patches. Current software image/patches and release notes available at support.bluesocket.com for download.

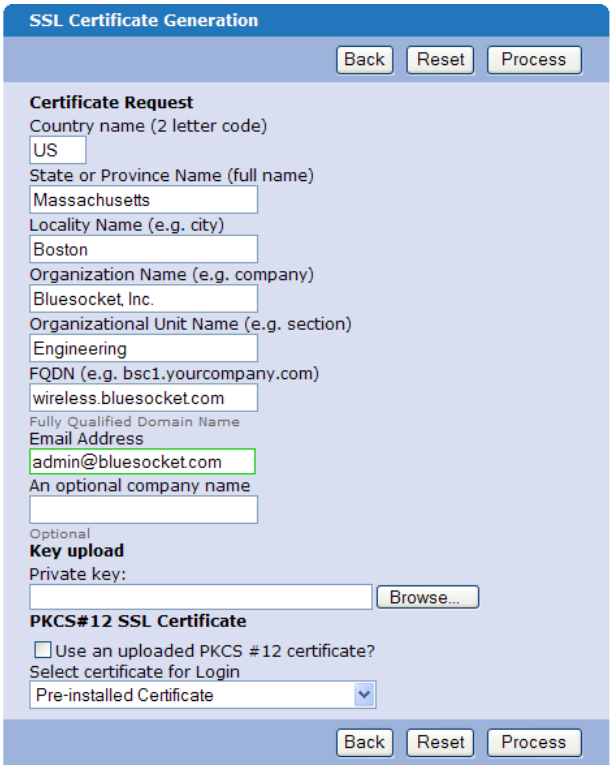
Background Information

An SSL Certificate provided by a Certificate Authority (CA) is only valid for a finite period of time. The BSC allows you to generate a Certificate Signing Request (CSR) for a certificate renewal on the renewal setup tab without deleting the current one. After uploading the new certificate to the BSC you can then switch to it without incurring any downtime.

These are the steps to follow:

1. Generate a new CSR on the renewal setup tab
2. Backup your private key
3. Submit the CSR to the CA
4. Retrieve the certificate that the CA Produces
5. Upload the certificate to the BSC
6. Switch to the new certificate

1. Generating a new Certificate Signing Request (CSR) on the BSC using the renewal setup tab



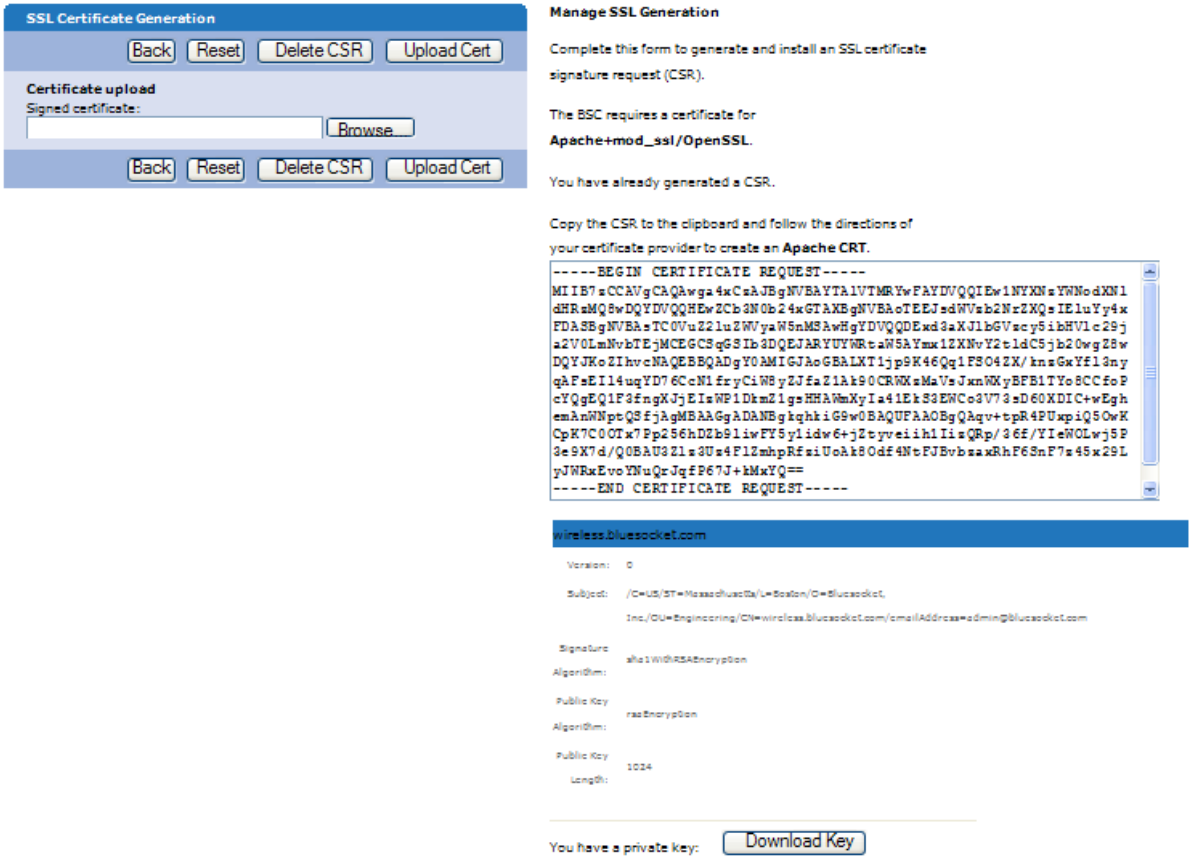
- Go to Web Logins>SSL Certificate>Renewal Setup>Fill out the Certificate Request form>click Process to create the CSR.
- If the renewal setup tab indicates you have already generated a CSR or you have already uploaded a certificate from a previous renewal attempt, click delete CSR or delete cert respectively.

- **Country Name**: Use the two-letter code without punctuation for country, for example: US or CA.
- **State or Province**: Spell out the state completely; do not abbreviate the state or province name, for example: Massachusetts
- **Locality Name**: The Locality field is the city or town name, for example: Boston.
- **Company**: If your company or department has an &, @, or any other symbol using the shift key in its name, It is

recommended you spell out the symbol or omit it. Example: Bluesocket, Inc.

- **Organizational Unit:** This field can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request.
- **FQDN (Fully Qualified Domain name):** This is equal to the **Common Name.** The Common Name is the Host + Domain Name. For example if the hostname of the BSC is wireless (Network>Protected>Hostname) and your domain name is Bluesocket.com. You should enter wireless.bluesocket.com.
- **Email Address:** Enter the email address of the administrator. The email address field is not part of the certificate. The CA may use it to contact you if it finds a problem. Example: admin@bluesocket.com
- **Optional Company Name:** This is an optional attribute.
- **Key Bit Length:** Select 1024 or 2048

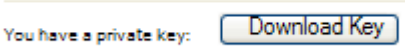
A new public/private key pair has now been created. The private key is stored locally on the BSC. The public key, in the form of a Certificate Signing Request (CSR) will be used for certificate renewal. The CSR will be displayed on the right hand side of the page in text format. A link to download the private key will also be displayed on the right hand side of the page.



2. **Backup your private key**

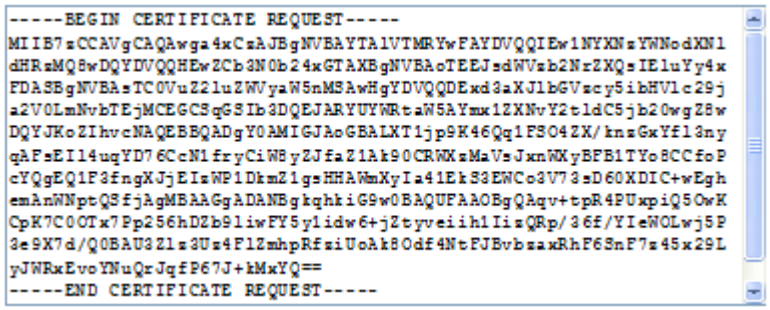
If the private key is lost or corrupted for any reason, the certificate will no longer work. For that reason, it is good practice to download the private key to a safe and secure place.

- Click Download Key to backup your private key



3. Submit the CSR to the CA

- Highlight the entire text of the CSR and copy and paste it into the appropriate space on your certificate provider's renewal form.



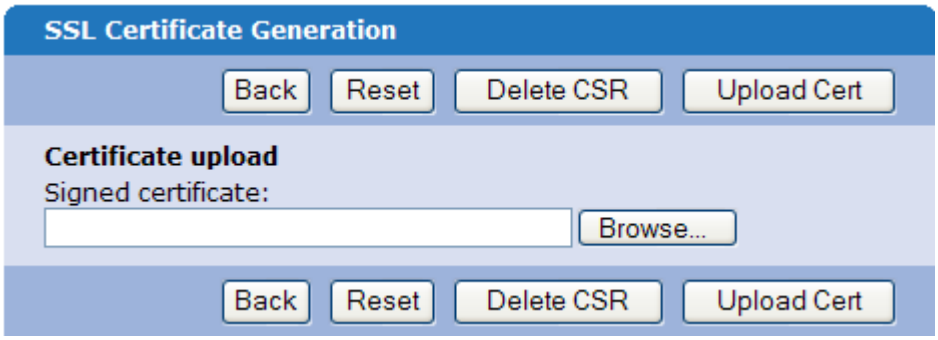
- Select apache as the server platform on your certificate provider's enrollment form.
- Complete any remaining steps required by the certificate provider.

4. Retrieve the certificate that the CA Produces

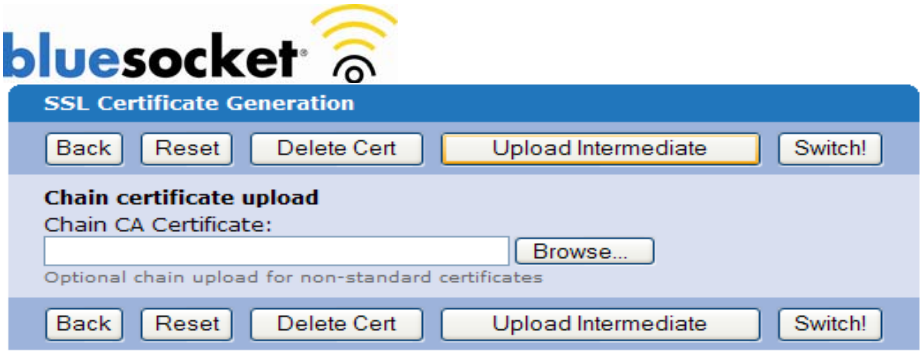
- The certificate provider will send you the certificate or instructions on how to obtain the certificate when authentication and processing is complete.
- Some certificate authorities may send the certificate in text. If so, copy and paste the text into a text editor such as notepad and save as a .cer file.

5. Upload the certificate to the BSC

- Upon receipt of the certificate go back to the Web Logins>SSL Certificate>Renewal Setup tab in the BSC.
- In the certificate upload box click browse.
- Browse for the certificate file (.cer) then click upload cert.

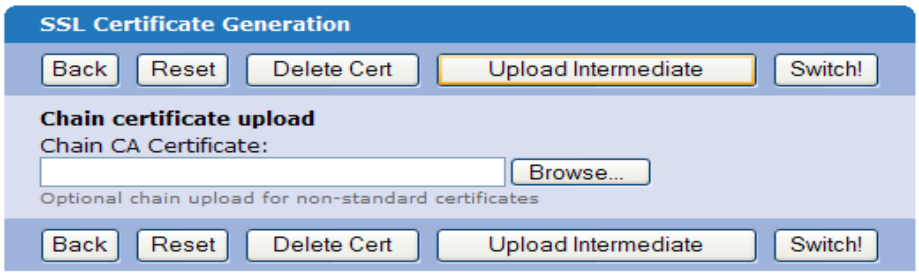


- If you also have an optional chain (intermediate) certificate, upload it next. (Some CAs use a chain of certificates rather than just one root certificate).



6. Switch to the new certificate

- Click the Switch! button to activate the new certificate
- You will be prompted to "click here" to have changes take effect. When you "click here"the BSC's web server will restart. You may lose access to the BSC's administrative gui momentarily but users will not be affected.



Verify

The next time that a client connects to the secure user login page or an administrator connects to the secure administrative login page using either IE7 or Firefox click the lock icon / in the address/navigation bar to view the certificate details. Make sure the certificate is valid for the appropriate period.