



Standard Operating Procedure (SOP) Managing External (GlobalSign) SSL Certificate Generation/ Renewal

Introduction

This SOP describes the complete lifecycle management of SSL/TLS certificates issued by GlobalSign: creating a Certificate Signing Request (CSR), decoding/validating it, submitting the request through ServiceNow, retrieving the issued certificates, optionally converting to PFX, and revoking certificates when required. Following this procedure ensures secure encrypted communication and maintains compliance with security policies.

1. Prerequisites – OpenSSL Installation

Before generating an SSL certificate, ensure OpenSSL is installed. It is required to create a CSR and the private key.

1.1 Check if OpenSSL is installed

Run the following command in the terminal:

```
openssl version
```

If OpenSSL is installed, the version will be displayed. If not, proceed to install it.

1.2 Install OpenSSL (Linux/Red Hat)

Install OpenSSL using:

```
sudo yum update
sudo yum install openssl
```

1.3 Verify OpenSSL Installation

After installation, confirm with:

```
openssl version
```

2. Generate CSR and Private Key

To generate a Certificate Signing Request (CSR) and private key using OpenSSL (for both Windows and Linux certificates), run the command below on any Linux server with OpenSSL installed:

```
openssl req -new -newkey rsa:2048 -nodes -keyout <common_name>.key -out <common name>.csr
```

When prompted, provide the details listed in the table below.

```
[d41315188@cgl-jusp00am01 ~]$ openssl req -new -newkey rsa:2048 -nodes -keyout common_name.key -out common_name.csr
Generating a RSA private key
 writing new private key to 'common_name.key'
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) [XX]:US
State or Province Name (full name) []:illinois
Locality Name (eg, city) [Default City]:chicago
Organization Name (eg, company) [Default Company Ltd]:adtalem
Organizational Unit Name (eg, section) []:IT

Common Name (eg, your name or your server's hostname) []:common_name

Email Address []:
Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Fig: CSR creation

CSR Field Details

Field	Example / Description
Country (C)	(e.g., US)
State / Province (ST)	(e.g., Illinois)
Locality / City (L)	(e.g., Chicago)
Organization (O)	(e.g., Adtalem/Walden)
Organizational Unit (OU)	(e.g., IT)
Common Name (CN) / FQDN	(e.g., app.example.com)

Note: You may refer to an existing RITM as a reference. Decoding the CSR will also help you retrieve the necessary information. For new certificates, confirm the university/organization (e.g., Adtalem, Walden) and populate the details accordingly.

3. View and Copy CSR & Private Key

To view the contents of the CSR and key:

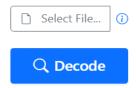
```
cat <common_name>.csr
cat <common_name>.key
```

Important: Verify the details by decoding the CSR before requesting approval via ServiceNow. You can use any online CSR decoder (e.g., "CSR Decoder and Certificate Decoder").

Decoder Hyperlink: CSR Decoder and Certificate Decoder

Q CSR and Certificate Decoder ①

----BEGIN CERTIFICATE REQUEST----MIICwTCCAakCAQAwfDELMAkGA1UEBhMCVVMxETAPBgNVBAgMCElsbGlub2lzMRAw DgYDVQQHDAdDaGljYWdvMSUwIwYDVQQKDBxBZHRhbGVtIEdsb2JhbCBFZHVjYXRp b24gSW5jMQswCQYDVQQLDAJJVDEUMBIGA1UEAwwLY29tbW9uX25hbWUwggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCqpdFwWNUiuegZPb99n+XWrbWk/9k0 yoo2HD0nFKMmJE06DwGeVBaXZ7dtd9aYgjqvqgIk9C73uIvVIQ0LPbSCfVZabnU7 Fpqh+OyRtbl0yrWMxA745Y24DZ+cPgYZy2bCxHpUlA6dXEQofw4lc9BOrMNOXKow Ul5+wVvv1hKJZclPVCEH4n+8WQWQsxLXYlcKql3Kd6H5eLFFHZQs1ztqxJkGf0GE 1KtnbOpqHbKKjB4uA5V/xZ0wD50BoaqKEnID20N7W5fjJ9T0FThBufy7wmo10n0l NaJLPhq1fFyjf8Nozx9hqaTQHD5/fZSN+K0v0TrwX5lUaO+lG1v61DEJAgMBAAGg ADANBgkqhkiG9w0BAQsFAAOCAQEAJbEI9h2KzPR20rz53A/hbI6MWS8xXqWbrfFO RZsUIVFUnH/7DcoAcF11jFpZlSZ68v9Li7l2ax36WTq8g29rA1Kqux1BrMXhpHPb FQ3WznCZR1u8dcXSCffUZ5b8+kxLpxarIgYKkL/rZgPH+6mODIDly42Qha7ZflOM 4yrgvPbaKVm/pv/ghXRoTgQetEHlbSyAVhzFLm3bFjnSIItlDV/lKqeZT9j+Y36K QsDV5h8mx0It/KX+CG54F+nYAfPXLn3mx3G57v2G59tbyfxhZKQN7j4fHXAXZ61F V3C8Sbv8svumnWOF3zdER4fuJlBQjNHsH66w3Ecp+mJgVmrRRw== ----FND CERTTETCATE REQUEST----



CSR Subject	
Common Name (CN)	common_name
Organizational Unit (OU)	IT
Organization (O)	Adtalem Global Education Inc
Locality (L)	Chicago
State or Province (ST)	Illinois
Country (C)	US

Fig: CSR Decoder

4. Request for SSL Certificate via ServiceNow

Step-by-step instructions:

Hyperlink: HYPERLINK "https://atge.service-

now.com/nav to.do?uri=%2Fcom.glideapp.servicecatalog cat item view.do%3Fv%3D1%26sysparm id %3Df02955311bd4f9502c29a683b24bcb2f"Create TLS Certificate

And COVERNIA State of the Control State of the Cont

1) In ServiceNow, navigate to the TLS Certificate request page (e.g., "Create TLS Certificate").

Fig: TLS Request Creation

2) Fill out the form:

- Requested For: Your name
- Application Owners: Add at least three names (e.g., Shane Ingram, Adam Spickler, your teammate)
- CSR: Paste the full contents of your .csr file
- SAN DNS: Usually the same as your CNAME. If multiple SANs, separate by commas
- Note: Avoid adding extra spaces while inserting these details

3) Click "Order Now" to submit your request. A request number (RITM) will be generated.

4.1 Certificate Approval and Retrieval

Once the request is approved, you will receive Main, Intermediate, and Root certificate files via email from GlobalSign. You can also download these from ServiceNow (All Certificates).

Download from: ServiceNow >> All certificates

Hyperlink: View certificates in ServiceNow

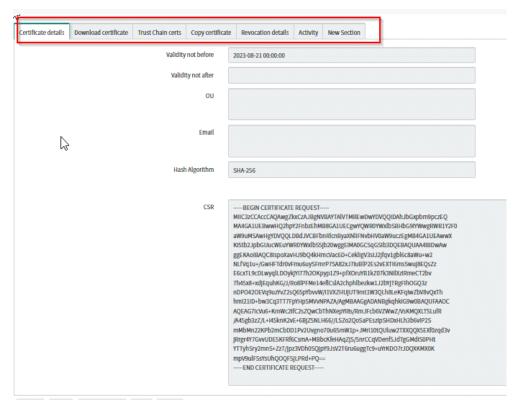


Fig: View Certificates

5. Certificate Installation

Installation steps vary based on the environment:

- Windows Server / IIS
- Load Balancer

Identify the responsible person/team for installation and share the following files with them:

- .key file (private key)
- Certificate files: main, intermediate, root

6. Convert Certificate to PFX Format (Optional)

To use the certificate in platforms like Windows or certain applications, you may need to create a .pfx file. You will need the <common_name>.crt and <common_name>.key files.

```
---BEGIN CERTIFICATE--
{\tt MIIGwTCCBamgAwIBAgIQAWq4fUYtMRrYBjyIVwMpvTANBgkqhkiG9w0BAQsFADBY}
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU21nbiBudi1zYTEuMCwGA1UE
DAWbdbWwkwTQSWjJTDHgzsqsqnsgmvabrRQHehrRP4Z04qPqv4hqbqNmjWn1jmOw
MfKKPSLY+50GqD4Hox2o32k8D8P05U0+X0MaDM+2zL8CAx7cbwwIwDcB58UmQ0q3
EjxVjUw=
  ---END CERTIFICATE----
----BEGIN CERTIFICATE----
MIIDXzCCAkegAwIBAgILBAAAAAABIVhTCKIwDQYJKoZIhvcNAQELBQAwTDEgMB4G
A1UECxMXR2xvYmFsU21nbiBSb290IENBIC0gUjMxEzARBgNVBAoTCkdsb2JhbFNp
Mx860yXShkD00yyGeMlhLxS67ttVb9+E7gUJTb0o2HL002JQZR7rkpeDMdmztcpH
WD9f
----END CERTIFICATE----
----BEGIN CERTIFICATE----
MIIEkDCCA3iqAwIBAqIRAIDlasfseKf/dqZyRkDleNEwDQYJKoZIhvcNAQELBQAw
TDEgMB4GA1UECxMXR2xvYmFsU21nbiBSb290IENBIC0gUjMxEzARBgNVBAoTCkds
qjoiDR4VwsK040olD0V3AbEZ11RTypM3v0OqPT2Jyj+otHTYL0ufjQpYJYzmqxNK
kv9Z/IpOTbw9yYnHXkPDNTmycuU=
  ---END CERTIFICATE----
----BEGIN PRIVATE KEY----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDFV97bapdqmlmN
nGqsYrfqkcPKkF6xviVX4Eqe+ajUexNlb3m7Ji0mIZqN2xdcbROj65kEyyVjI/BZ
b0Lm0kGpX1aip7bPLIbxwA6Jez5j8bLlNZs+Tz/m/qildh2iN5ykkWDnvN1JJCg8
XxachLplc5LWBrxSslqKo/4=
 ---END PRIVATE KEY----
```

Fig: Create .crt File

Create the .crt file:

```
vi <common name>.crt
```

Press 'i' to enter insert mode, then paste the Main, Root, Intermediate, and Key contents sequentially in the file. Save & exit with: Esc + :wq! + Enter.

Convert to .pfx:

```
openssl pkcs12 -export -out <common_name>.pfx -inkey <common_name>.key -in
<common name>.crt
```

Set a password when prompted and store it securely (ensure it is unique from any application passwords).

To view details of the .pfx file:

```
openssl pkcs12 -info -in <common_name>.pfx -nodes
```

Enter the password when prompted to display the file contents.

This creates a .pfx file you can import into Windows or other applications.