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.

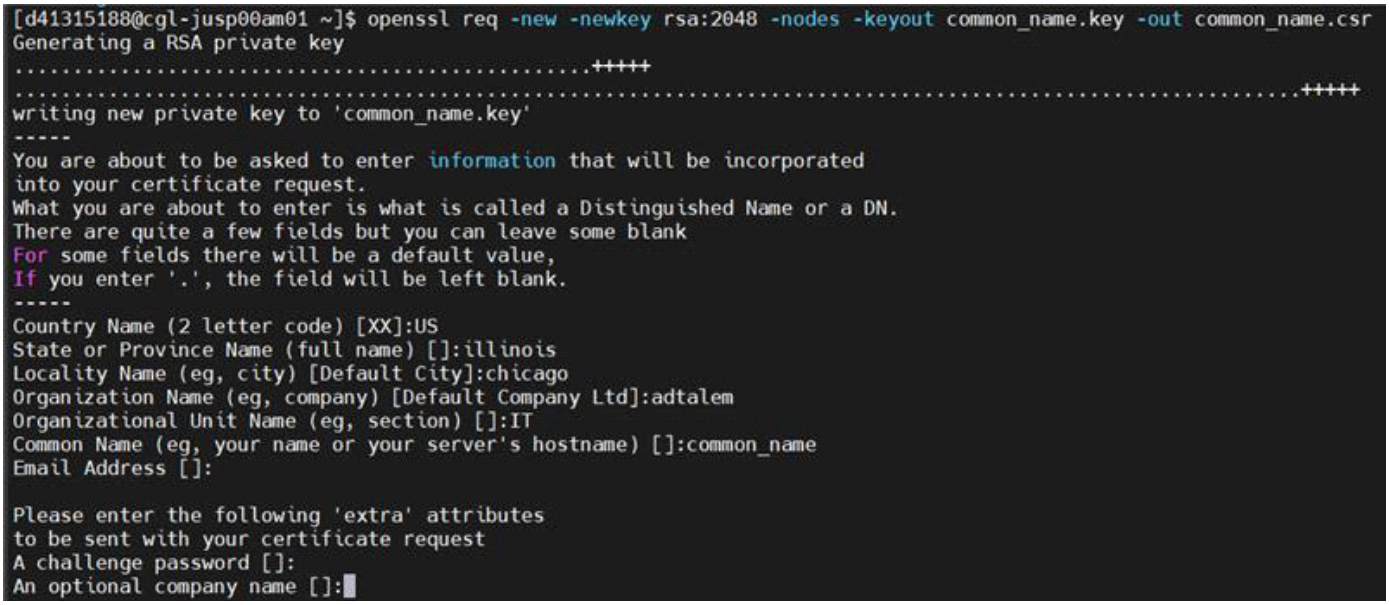

Fig: CSR creation

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

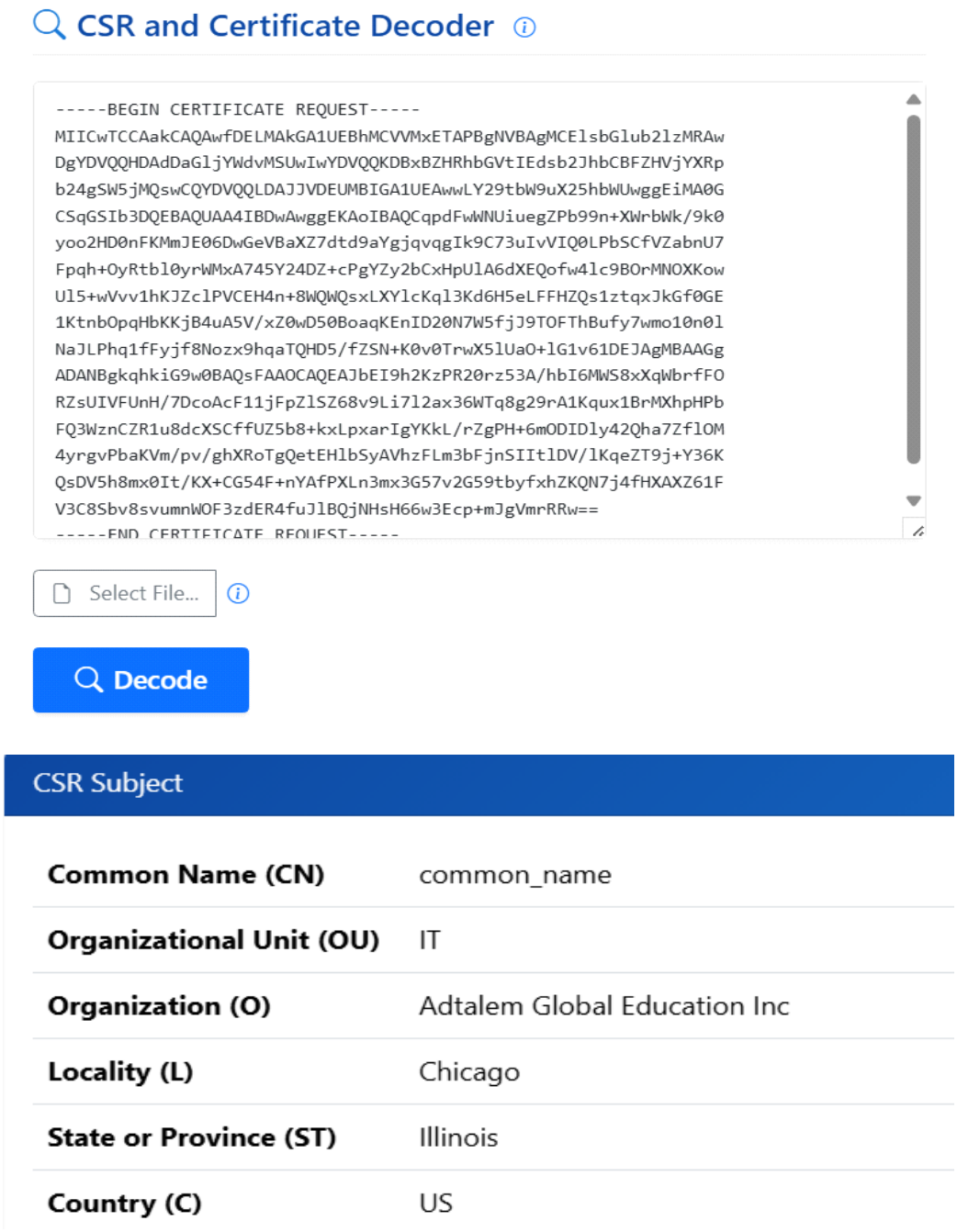

Fig: CSR Decoder

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

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

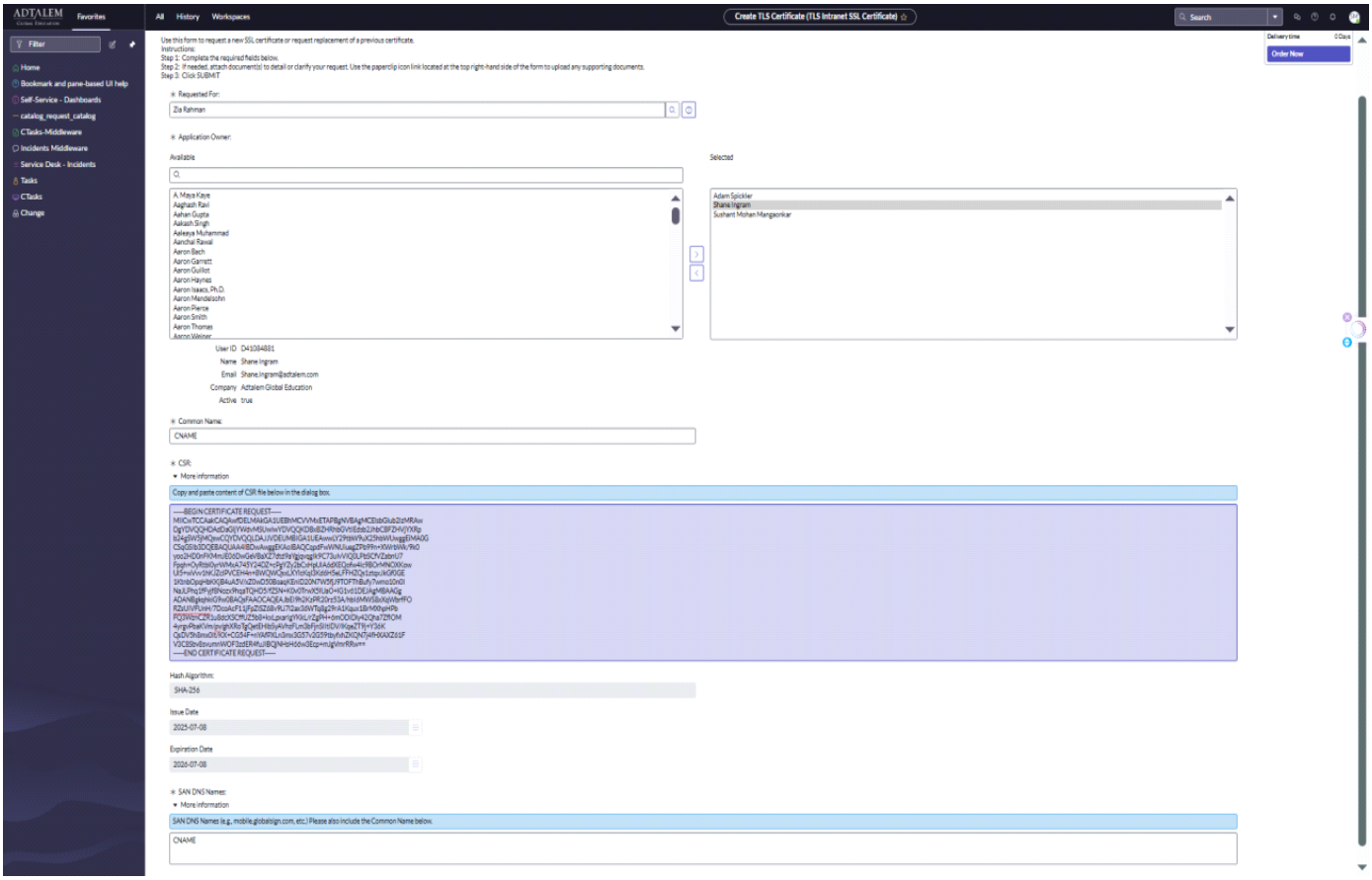

Fig: TLS Request Creation

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

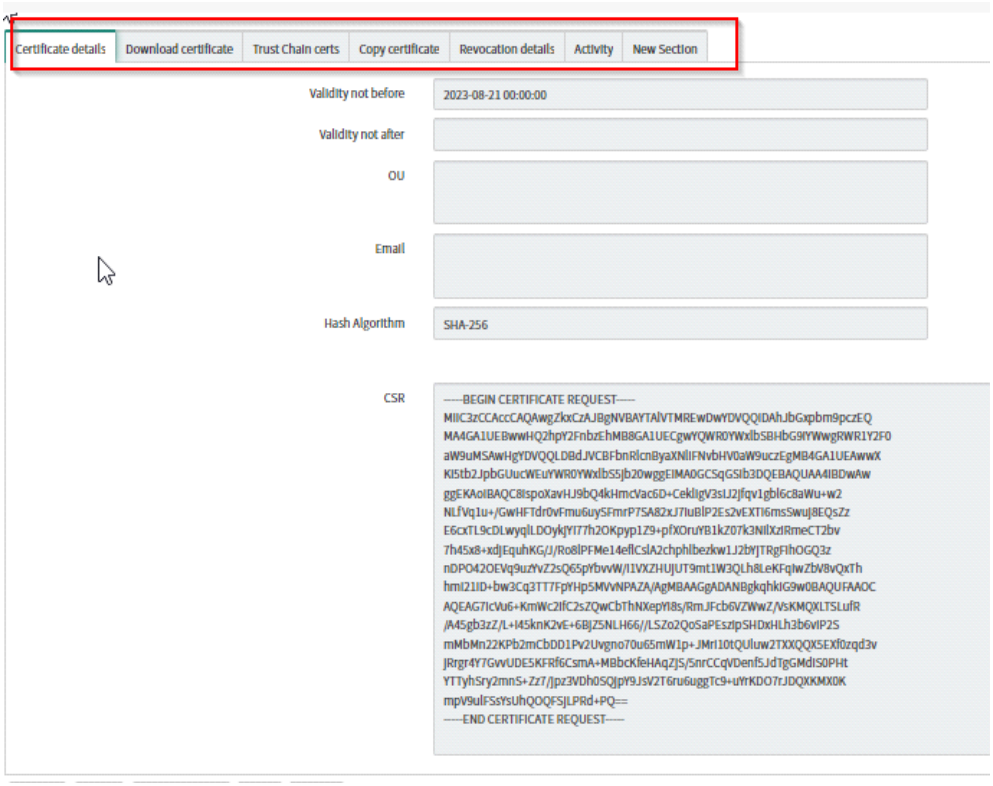

Fig: View Certificates

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.

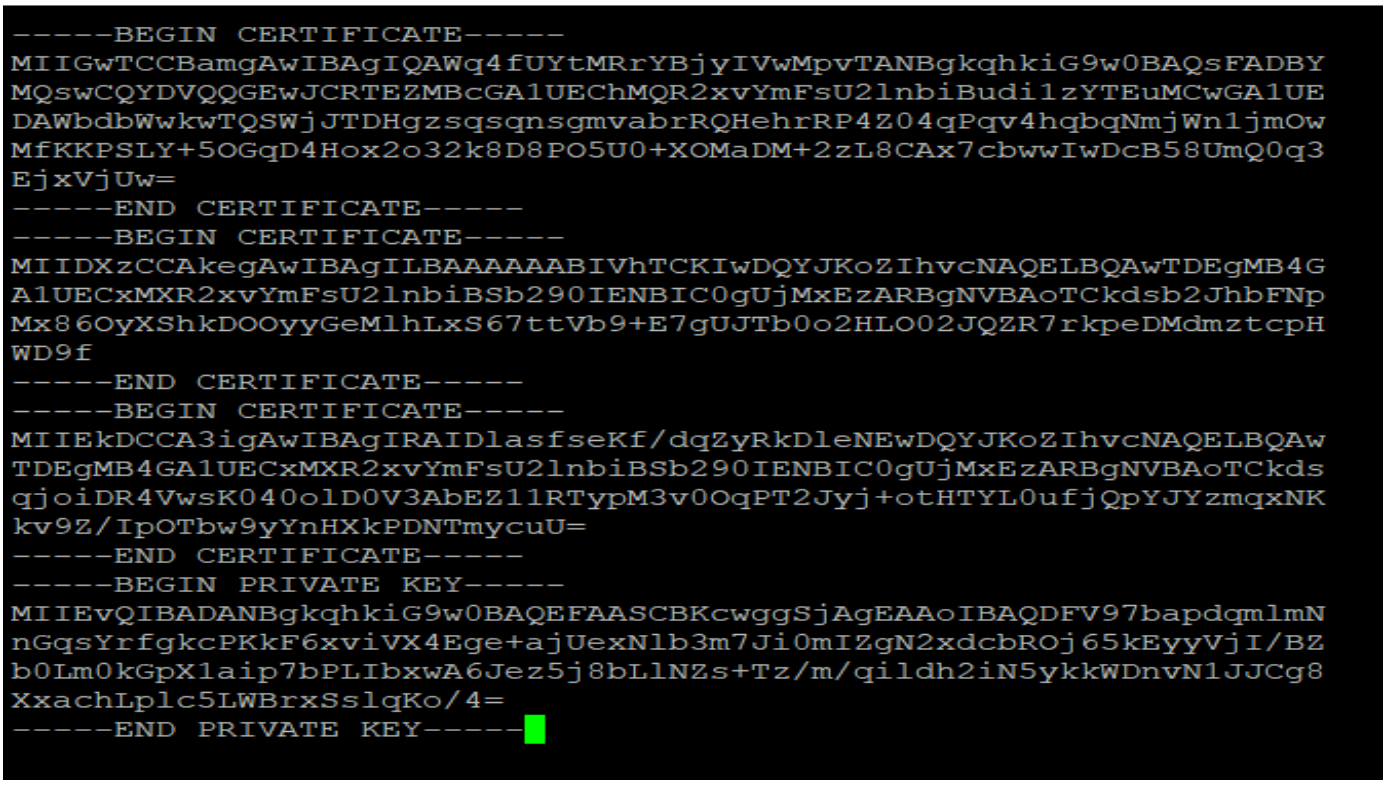

Fig: Create .crt File

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.