**SSL Certificate Renewal & Installation for SAN Subdomain on AWS EC2 (NGINX)**

**Overview:**

This document details the step-by-step process to rekey, download, and install a renewed SSL certificate for the SAN subdomain trueface.co.in, which is part of the main domain cstech.com, managed in GoDaddy. The application is hosted on an AWS EC2 Amazon Linux instance using NGINX as a reverse proxy for a Spring Boot backend.

**✅ 1. Verify Existing Certificate Expiry**

On the EC2 instance:

openssl x509 -in /etc/nginx/ssl/trueface.crt -noout -dates

To confirm the certificate is for the correct subdomain:

openssl x509 -in /etc/nginx/ssl/trueface.crt -text -noout | grep -A2 "Subject Alternative Name"

**🔧 2. Generate New Private Key and CSR**

Generate a new key and CSR on EC2:

sudo openssl req -new -newkey rsa:2048 -nodes \

-keyout /etc/nginx/ssl/trueface.key \

-out /etc/nginx/ssl/trueface.csr

When prompted, use:

* **Common Name:** cstech.com (main domain)
* Add other details as needed (State, Organization, Email, etc.)

**🌐 3. Rekey Certificate in GoDaddy**

1. Log in to [GoDaddy SSL Manager](https://godaddy.com/).
2. Go to **My Products** → SSL Certificates.
3. Click "Not Verified" or "Rekey" next to your main domain cstech.com.
4. Paste the contents of trueface.csr into the CSR input box:
5. cat /etc/nginx/ssl/trueface.csr
6. Submit and wait ~5–15 minutes for processing.

**📥 4. Download and Prepare Certificate**

1. After "Verified" status appears, click **Download ZIP**.
2. Select **Apache** as the server type.
3. Unzip the contents — you’ll get:
   * trueface.crt (domain certificate)
   * gd\_bundle-g2-g1.crt (intermediate chain)

Upload these to EC2:

scp trueface.crt gd\_bundle-g2-g1.crt ec2-user@<EC2-IP>:/tmp

Then move them to the NGINX SSL directory:

sudo mv /tmp/trueface.crt /etc/nginx/ssl/

sudo mv /tmp/gd\_bundle-g2-g1.crt /etc/nginx/ssl/

**🧩 5. Combine Certificates for NGINX**

NGINX requires a full chain certificate:

sudo cat /etc/nginx/ssl/trueface.crt /etc/nginx/ssl/gd\_bundle-g2-g1.crt > /etc/nginx/ssl/fullchain.crt

**⚙️ 6. Update NGINX Configuration**

Edit NGINX SSL server block (e.g., /etc/nginx/nginx.conf or /etc/nginx/conf.d/default.conf):

server {

listen 443 ssl;

server\_name trueface.co.in;

ssl\_certificate /etc/nginx/ssl/fullchain.crt;

ssl\_certificate\_key /etc/nginx/ssl/trueface.key;

location / {

proxy\_set\_header X-Forwarded-For $remote\_addr;

proxy\_set\_header Host $http\_host;

proxy\_pass http://127.0.0.1:8080;

client\_max\_body\_size 20m;

}

error\_page 404 /404.html;

location = /404.html { }

error\_page 500 502 503 504 /50x.html;

location = /50x.html { }

}

**🔄 7. Test & Reload NGINX**

Check config:

sudo nginx -t

Reload if successful:

sudo systemctl reload nginx

**🔍 8. Validate Setup**

1. Access https://trueface.co.in in a browser.
2. Check certificate info (padlock icon → "Certificate").
3. Confirm it’s valid, signed by GoDaddy, and includes SANs.

**✅ Confirmation**

* Rekey completed under main domain cstech.com.
* SAN subdomain trueface.co.in included and verified.
* SSL is now valid and secure.
* No impact to other SANs or main domain SSL.

**End of Document**