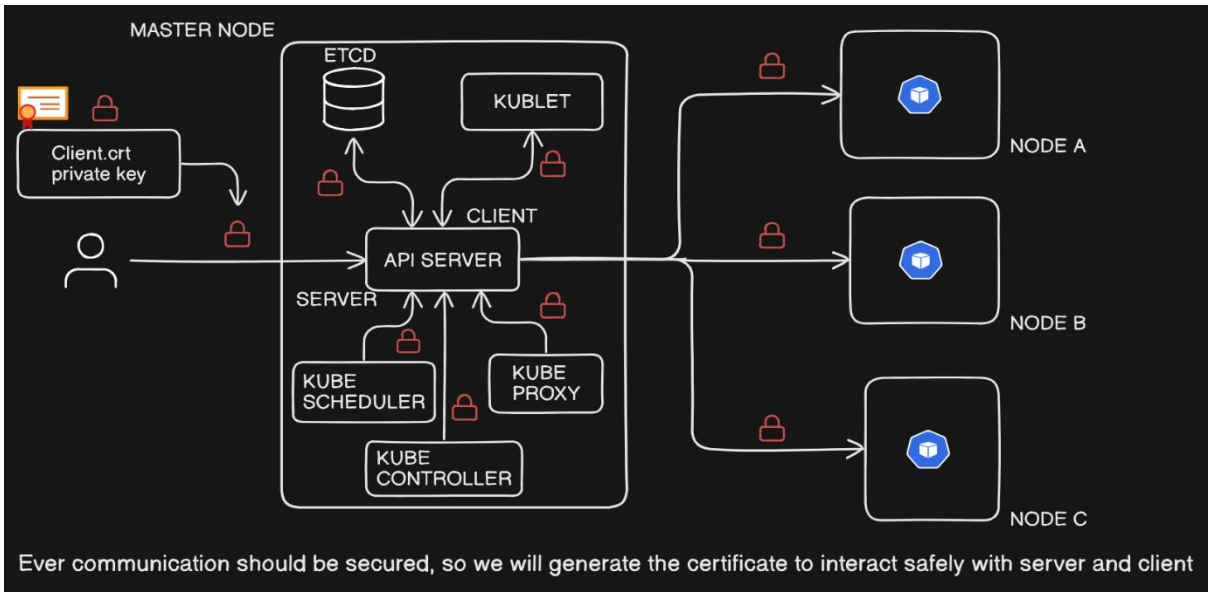
SSL AND TLS CERTIFICATE IN KUBERNETES

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) certificates play a critical role in securing communications between components by encrypting data and verifying identities.

SSL and TLS Certificates in Kubernetes

- **SSL/TLS certificates** are digital certificates that provide authentication and encryption for secure data exchange over a network. They ensure the confidentiality and integrity of data transmitted between clients (like a user's web browser or service) and servers.
- In Kubernetes, TLS is primarily used for securing:
  - **API server** communication: Protects data exchanged between the Kubernetes API server and clients, such as kubectl.
  - **Intra-cluster communication**: Encrypts traffic between pods or services.
  - **Ingress traffic**: Secures external traffic entering the cluster via an Ingress Controller.



We Need SSL/TLS Certificates in Kubernetes

- **Security**: TLS certificates provide end-to-end encryption, preventing data from being intercepted by unauthorized parties.
- **Authentication**: Certificates validate the identity of clients and servers, reducing the risk of man-in-the-middle attacks.
- **Compliance**: Many regulations require data encryption, especially for sensitive or personal information.

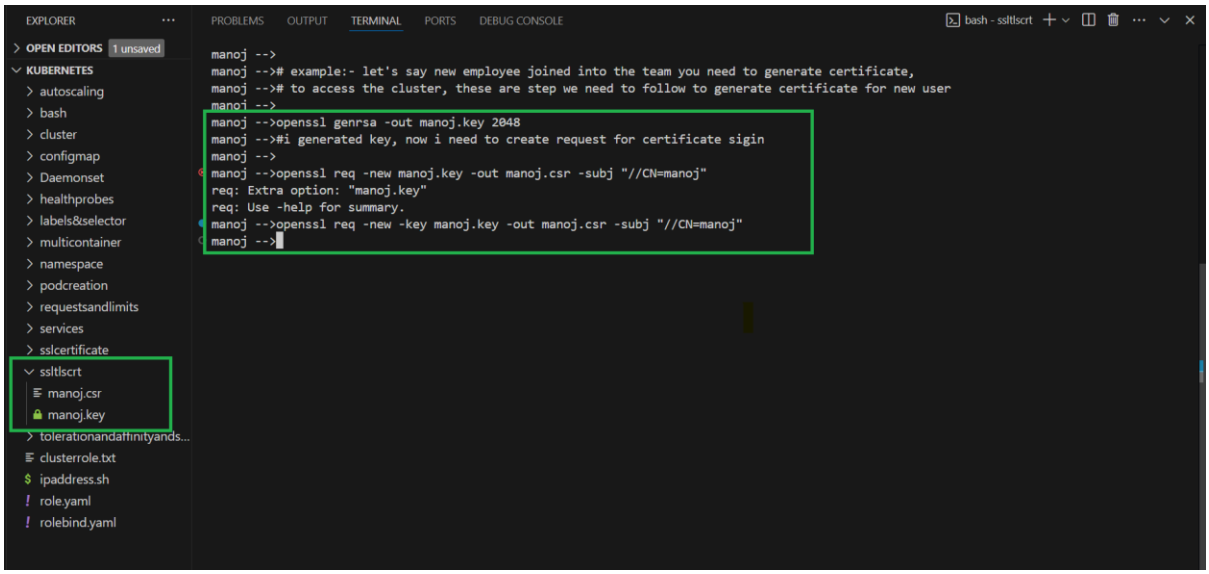
When to use SSL/TLS Certificates in Kubernetes

- **API Communication**: Kubernetes by default secures the API server with TLS to ensure secure access for kubectl and other clients.
- **Service Communication**: When sensitive data is transmitted between services or pods, encrypting intra-cluster communication adds another security layer.
- **Ingress Traffic**: When exposing services to the internet, TLS certificates secure user access, especially when handling personal or sensitive information.

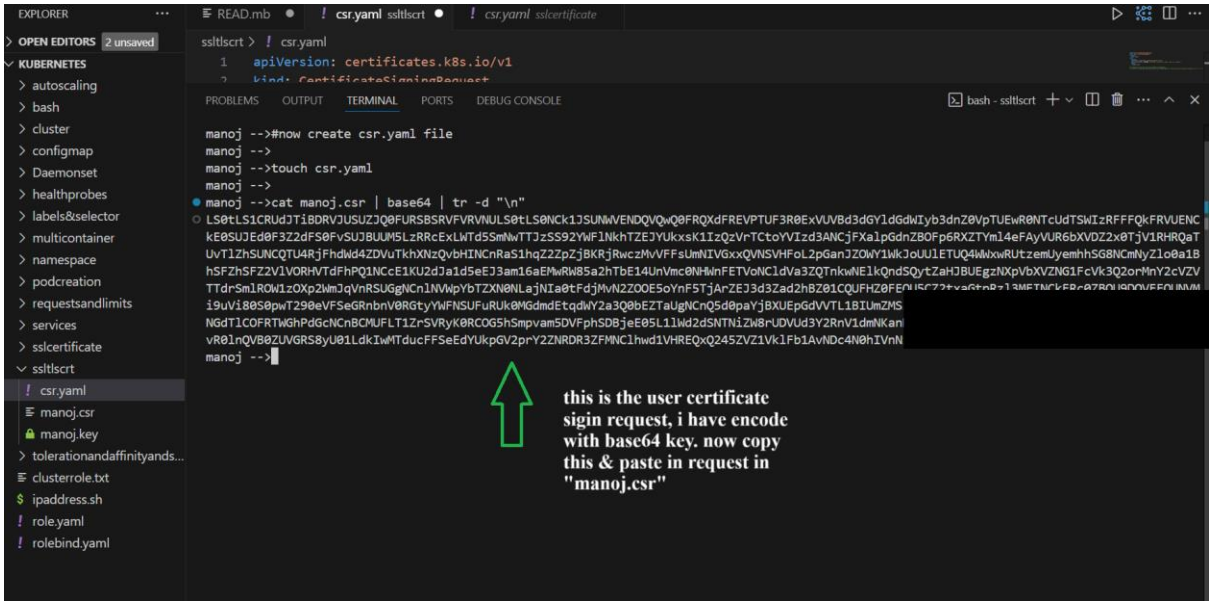
SSL AND TLS CERTIFICATE IN KUBERNETES

New employee joined inot the team I need to generate certificate to give access to the cluster.

Generate ‘key’



Create the request for certification sigin



SSL AND TLS CERTIFICATE IN KUBERNETES

READ.mb ● | ! csr.yaml × | ! issusecrt.yaml ●

ssltlscrt > ! csr.yaml

```yaml
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: manoj
spec:
  # encode certificate request
  request: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0NCk1JSUNWVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFF
  signerName: kubernetes.io/kube-apiserver-client
  expirationSeconds: 4320000  # 50 days ,we can also give 1 year for validity
  usages:
  - client auth

#to decode the csr file use this command in powershell
# [Convert]::ToBase64String([System.IO.File]::ReadAllBytes("C:\Users\provide the path\[filename].csr")) | % { $_.Replace("`r`n", "") }
```

Created certificate signing request still in pending state

```
manoj -->
manoj -->kubectl get csr
NAME    AGE   SIGNERNAME                              REQUESTOR          REQUESTEDDURATION   CONDITION
manu    30m   kubernetes.io/kube-apiserver-client     kubernetes-admin   50d                 Approved,Issued
manoj -->kubectl apply -f csr.yaml
certificatesigningrequest.certificates.k8s.io/manoj created
manoj -->
manoj -->kubectl get csr
NAME    AGE   SIGNERNAME                              REQUESTOR          REQUESTEDDURATION   CONDITION
manoj   8s    kubernetes.io/kube-apiserver-client     kubernetes-admin   50d                 Pending
manu    30m   kubernetes.io/kube-apiserver-client     kubernetes-admin   50d                 Approved,Issued
manoj -->
```

we still didn't approved yet. this certificate should be approved by authorized CA (certificate authority) this is for the internal k8's cluster

```
manoj -->
manoj -->kubectl get csr
NAME    AGE     SIGNERNAME                              REQUESTOR          REQUESTEDDURATION   CONDITION
manoj   4m38s   kubernetes.io/kube-apiserver-client     kubernetes-admin   50d                 Pending
manu    35m     kubernetes.io/kube-apiserver-client     kubernetes-admin   50d                 Approved,Issued
manoj -->kubectl describe csr manoj
Name:         manoj
Labels:       <none>
Annotations:  kubectl.kubernetes.io/last-applied-configuration={"apiVersion":"certificates.k8s.io/v1","kind":"CertificateSigningRequest",
"metadata":{"annotations":{},"name":"manoj"},"spec":{"expirationSeconds":4320000,"request":"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tL
S0NCk1JSUNWVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUENCkE0SUJEd0F3Z2dFS0FvSUJBUUM5LzRRcExLWTd5SmNwTT
JzSS92YWFlNkhTZEJYUkxsK1IzQzVrTCtoYVIzd3ANCjFXalpGdnZBOFp6RXZTYml4eFAyVUR6bXVDZ2x0TjV1RHRQaTUvTlZhSUNCQTU4RjFhdWd4ZDVuTkhXNzQvbHINCnRaS1h
qZ2ZpZjBKRjRwczMvVFFsUmNIVGxxQVNSVHFoL2pGanJZOWY1WkJoUUlETUQ4WWxwRUtzemUyemhhSG8NCmNyZlo0a1BhSFZhSFZ2VlVORHVTdFhPQ1NCcE1KU2dJa1d5eEJ3am16
aEMwRW85a2hTbE14UnVmc0NHWnFETVoNCldVa3ZQTnkwNElkQndSQytZaHJBUEgzNXpVbXVZNG1FcVk3Q2orMnY2cVZVTTdrSmlROW1zOXp2WmJqVnRSUGgNCnlNVWpYbTZXN0NLa
jNIa0tFdjMvN2ZOOE5oYnF5TjArZEJ3d3Zad2hBZ01CQUFHZ0FEQU5CZ2txaGtpRzl3MEINCkFRc0ZBQU9DQVFFQUNVMi9uVi80S0pwT2S
dmdEtqdWY2a3Q0bEZTaUgNCnQ5d0paYjBXUEpGdVVTL1BIUmZMSldzczFqMWJCUGlFS3A4MHNlUUZsQVdVRkNSam15YUNGdTlCOFRTWGhI
vam5DVFphSDBjeE05L1lWd2dSNTNiZW8rUDVUd3Y2RnV1dmNKanNoRm1UWm8NCng4N3dwcWQ2SnlwcXhxSitLeE9idGovR0lnQVB0ZUVGI
Y2ZNRDR3ZFMNClhwd1VHREQxQ245ZVZ1VklFb1AvNDc4N0hIVnNzaEZiZDBVeFZHWFowRlFCRnk4U010VWFwQ1R0YW01dXRSamENClVkYI
ml1YlJOblE9PQ0KLS0tLS1FTkQgQ0VSVElGSUNBVEUgUkVRVUVTVC0tLS0tDQo=","signerName":"kubernetes.io/kube-apiserv
h"]}}

Creationtimestamp:   Wed, 30 Oct 2024 13:02:59 +0530
Requesting User:     kubernetes-admin
Signer:              kubernetes.io/kube-apiserver-client
Requested Duration:  50d
Status:              Pending
Subject:
         Common Name:    manoj
         Serial Number:
Events:  <none>
manoj -->
```

we can see the creation of time and duration till it is valid

SSL AND TLS CERTIFICATE IN KUBERNETES

After checking very details then I need to approve the request

```
manoj -->kubectl describe csr manoj
Name:         manoj
Labels:       <none>
Annotations:  kubectl.kubernetes.io/last-applied-configuration={"apiVersion":"certificates.k8s.io/v1","kind":"CertificateSigningRequest",
"metadata":{"annotations":{},"name":"manoj"},"spec":{"expirationSeconds":4320000,"request":"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tL
S0NCk1JSUNWVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUENCkE0SUJEd0F3Z2dFS0FvSUJBUUM5LzRRcExLWTd5SmNwTT
JzSS92YWFlNkhTZEJYUkxsK1IzQzVrTCtoYVIzd3ANCjFXalpGdnZBOFp6RXZTYml4eFAyVUR6bXVDZ2x0TjV1RHRQaTUvTlZhSUNCQTU4RjFhdWd4ZDVuTkhXNzQvbHINCnRaS1h
qZ2ZpZjBKRjRwczMvVFFsUmNIVGxxQVNSVHFoL2pGanJZOWY1WkJoUUlETUQ4WWxwRUtzemUyemhhSG8NCmNyZlo0a1BhSFZhSFZ2VlVORHVTdFhPO1NCcE1KU2dJa1d5eEJ3am16
aEMwRW85a2hTbE14UnVmc0NHWnFETVoNCldVa3ZQTnkwNElkQndSQytZaHJBUEgzNXpVbXVZNG1FcVk3Q2orMnY2cVZVTTdrSml
jNIa0tFdjMvN2ZOOE5oYnF5TjArZEJ3d3Zad2hBZ01CQUFHZ0FEQU5CZ2txaGtpRzl3MEINCkFRc0ZBQU9DQVFFQUNVMi9uVi80
dmdEtqdWY2a3Q0bEZTaUgNCnQ5d0paYjBXUEpGdVVTL1BIUmZMSldzczFqMWJCUGlFS3A4MHNlUUZsQVdVRkNSam15YUNGdTlCO
vam5DVFphSDBjeE05L1lWd2dSNTNiZW8rUDVUd3Y2RnV1dmNKanNoRm1UWm8NCng4N3dwcWQ2SnlwcXhxSitLeE9idGovR0lnQV
Y2ZNRDR3ZFMNClhwd1VHREQxQ245ZVZ1VklFb1AvNDc4N0hIVnNzaEZiZDBVeFZHWFowRlFCRnk4U010VWFwQ1R0YW01dXRSamE
ml1YlJOblE9PQ0KLS0tLS1FTkQgQ0VSVElGSUNBVEUgUkVRVUVTVC0tLS0tDQo=","signerName":"kubernetes.io/kube-a
h"]}}

CreationTimestamp:   Wed, 30 Oct 2024 13:02:59 +0530
Requesting User:     kubernetes-admin
Signer:              kubernetes.io/kube-apiserver-client
Requested Duration:  50d
Status:              Approved,Issued
Subject:
         Common Name:    manoj
         Serial Number:
Events:  <none>
manoj -->
manoj -->
```

certificate approved, valid till 50days. after the we can renew it. if we want

```
manoj -->
manoj -->kubectl get csr
NAME    AGE     SIGNERNAME                            REQUESTOR          REQUESTEDDURATION   CONDITION
manoj   7m55s   kubernetes.io/kube-apiserver-client   kubernetes-admin   50d                 Pending
manu    38m     kubernetes.io/kube-apiserver-client   kubernetes-admin   50d                 Approved,Issued
manoj -->
manoj -->#let approve the certificate
manoj -->
manoj --># if everything is good you can approve the request
manoj -->
manoj -->kubectl certificate approve manoj
certificatesigningrequest.certificates.k8s.io/manoj approved
manoj -->
manoj -->kubectl get csr
NAME    AGE     SIGNERNAME                            REQUESTOR          REQUESTEDDURATION   CONDITION
manoj   8m54s   kubernetes.io/kube-apiserver-client   kubernetes-admin   50d                 Approved,Issued
manu    39m     kubernetes.io/kube-apiserver-client   kubernetes-admin   50d                 Approved,Issued
manoj -->
manoj -->
```

after checking everything is good then only approve the certificate

```
manoj -->
manoj -->#now i want to share this certificate with user
manoj -->
manoj -->kubectl get csr manoj -o yaml > issusecrt.yaml
manoj -->
manoj -->
```

SSL AND TLS CERTIFICATE IN KUBERNETES

```
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"certificates.k8s.io/v1","kind":"CertificateSigningRequest","metadata":{"annotations":{},"name":"manoj"},"spec":{"expirationSeconds":4320000,"request":"LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFV
  creationTimestamp: "2024-10-30T07:32:59Z"
  name: manoj
  resourceVersion: "105207"
  uid: 82a6934e-fb13-4a03-b231-317f46e0e54f
spec:
  expirationSeconds: 4320000
  groups:
  - kubeadm:cluster-admins
  - system:authenticated
  request: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0NCk1JSUNWVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUENCkE0SUJEd0F3Z2dFS0FvSUJBUUM5LzRRcExlWTd5SmNwTTJzSS92YWFlNkhT
  signerName: kubernetes.io/kube-apiserver-client
  usages:
  - client auth
  username: kubernetes-admin
status:
  certificate: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUM5akNDQWQ2Z0F3SUJBZ01SQUtja3E2emdNTmZSMHVBOVllUW5xbU13RFFZSktvWklodmNOQVFFTEJRQXcKRlRFVE1CRUdBMVVFQXhNS2EzVm1aWEp1WlhSbGN6QWVGdzB5TkRFd016QXdOek0yTkRo
  conditions:
  - lastTransitionTime: "2024-10-30T07:41:48Z"
    lastUpdateTime: "2024-10-30T07:41:48Z"
    message: This CSR was approved by kubectl certificate approve.
    reason: KubectlApprove
    status: "True"
    type: Approved
```

```
manoj -->
manoj -->#in this file "request" is in encode formated we need to decode
manoj -->#copy the request from file
manoj -->
manoj --># echo "<past-request>" | base64 -d     ---> now decoded
manoj -->
manoj -->echo "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0NCk1JSUNWVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUENCkE0SUJEd0F3
Z2dFS0FvSUJBUUM5LzRRcExlWTd5SmNwTTJzSS92YWFlNkhTZEJYUkxsK1IzQzVrTCtoYVIzd3ANCjFXalpGdnZBOFp6RXZTYml4eFAyVUR6bXVDZ2x0TjV1RHRQaTUvTlZhSUNCQTU4RjFhdWd4ZDVuTkhXNzQvbHI
NCnRaS1hqZ2ZpZjBKRjRwczMvVFFsUmNIVGxxQVNSVHFoL2pGanJZOWY1WkJoUUlETUQ4WWxwRUtzemUyemhhSG8NCmNyZlo0a1BhSFZhSFZ2VlVORHVTdFhPQ1NCcE1KU2dJa1c
Vmc0NHWnFETVoNCldVa3ZQTnkwNElkQndSQytZaHJBUEgzNXpVbXVZNG1FcVk3Q2orMnY2cVZVTTdrSmlROW1zOXp2WmJqVnRSUGgNCnlNVWpYbTZXN0NLajNIa0tFdjMvN2ZOOE
UFHZ0FEQU5CZ2txaGtpRzl3MEINCkFRc0ZBQU9DQVFFQUNVMi9uVi80S0pwT290eVFSeGRnbnV0RGtyYWFNSUFuRUk0MGdmdEtqdWY2a3Q0bEZTaUgNCnQ5d0paYjBXUEpGdVVTL
MHNlUUZsQVdVRkNSam15YUNGdTlCOFRTWGhPdGcNCnBCMUFLT1ZrSVRyK0RCOG5hSmpvam5DVFphSDBjeE05L1lWd2dSNTNiZW8rUDVUd3Y2RnV1dmNKanNoRm1UWm8NCng4N3dw
nQVB0ZUVGRS8yU01LdkIwMTducFFSeEdYUkpGV2prY2ZNRDR3ZFMNClhwd1VHRE5QxQ245ZVZ1VklFb1AvNDc4N0hIVnNzaEZiZDBVeFZHWFowRlFCRnk4U010VWFwQ1R0YW01dXF
NNVGsrL1BBSVh6bm11YlJOblE9PQ0KLS0tLS1FTkQgQ0VSVElGSUNBVEUgUkVRVUVTVC0tLS0tDQo=" | base64 -d
-----BEGIN CERTIFICATE REQUEST-----
MIICVTCCAT0CAQAwEDEOMAwGA1UEAwwFbWFub2owggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQC9/4QpLKY7yJcpM2sI/vaae6HSdBXRLl+R3C5kL+haR3wp
1WjZFvvA8ZzEvSbixxP2UDzmuCgltN5uDtPi5/NVaICBA58F1augxd5nNHW74/lr
tZKXjgfif0JF4ps3/TQlRcHTlqASRTqh/jFjrY9f5ZBhQIDMD8YlpEKsze2zhaHo
crfZ4kPaHVaHVvVUNDuStXOCSBpMJSgIkWyxBwjmzhC0Eo9khSlMxRufsCGZqDMZ
WUkvPNy04IdBwRC+YhrAPH35zUmuY4mEqY7Cj+2v6qVUM7kJiQ9ms9zvZbjVtRPh
yMUjXm6W7CKj3HkKEv3/7fN8NhbqyN0+dBwwvZwhAgMBAAGgADANBgkqhkiG9w0B
AQsFAAOCAQEACU2/nV/4KJpOotyQRxdgnutDkraaMIAnEI40gftKjuf6kt4lFSiH
t9wJZb0WPJFuUS/PHRfLJ
pB1AKOVkITr+DB8naJjoj
x87wpqd6JypqxqJ+KxObt
XpwUGDD1Cn9eVuVIEoP/4
UdbCnQ6Y51HBkhtSMTk+/
-----END CERTIFICATE REQUEST-----
manoj -->
```

Decode the request

Now I can add this certificate to kube-config and assign certain roles to it. So that user will have certain permissions and user can access the server using that certificate.

```
manoj -->
manoj --># now i can add this certificate to kube-config and assign certain roles to it. so that user will have certain permissions and
manoj --># user can access the server using that certification
manoj -->
manoj -->kubectl get csr -o yaml > manoj.crt
manoj -->
manoj -->
```

SSL AND TLS CERTIFICATE IN KUBERNETES


```yaml
apiVersion: v1
items:
- apiVersion: certificates.k8s.io/v1
  kind: CertificateSigningRequest
  metadata:
    annotations:
      kubectl.kubernetes.io/last-applied-configuration: |
        {"apiVersion":"certificates.k8s.io/v1","kind":"CertificateSigningRequest","metadata":{"annotations":{},"name":"manoj"},"spec":{"expirationSeconds":4320000,"reques
    creationTimestamp: "2024-10-30T07:32:59Z"
    name: manoj
    resourceVersion: "105207"
    uid: 82a6934e-fb13-4a03-b231-317f46e0e54f
  spec:
    expirationSeconds: 4320000
    groups:
    - kubeadm:cluster-admins
    - system:authenticated
    request: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0NCk1JSUNwVENDQVQwQ0FRQXdFREVPTUF3R0ExVUVBd3dGYldGdWIyb3dnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUENCkE0SUJEd0F3Z2dFS0FvS
    signerName: kubernetes.io/kube-apiserver-client
    usages:
    - client auth
    username: kubernetes-admin
  status:
    certificate: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUM5akNDQWQ2Z0F3SUJBZ0lSQUtja3E2emdNTmZSMHVBOVllUW5xbU13RFFZSktvWklodmNOQVFFTEJRQXcKRlRFVE1CRUdBMVVFQXhNS2EzVmlaW
    conditions:
    - lastTransitionTime: "2024-10-30T07:41:48Z"
      lastUpdateTime: "2024-10-30T07:41:48Z"
      message: This CSR was approved by kubectl certificate approve.
      reason: KubectlApprove
      status: "True"
```


Comparison between SSL and TLS in table format:

Feature	SSL (Secure Sockets Layer)	TLS (Transport Layer Security)
Security	Vulnerable to various attacks, weaker encryption	Stronger encryption, more secure, supports PFS
Handshake Process	Slower and more complex	Faster, simplified handshake, especially in TLS 1.3
Cipher Suites	Limited, lacks modern algorithms	Expanded support for secure, modern cipher suites
Deprecation Status	Deprecated and unsupported	Current standard for secure communications
Usage in Certificates	Often referred to as "SSL certificates" due to legacy naming	Technically uses TLS encryption, even in "SSL certificates"