# Section 7: Security

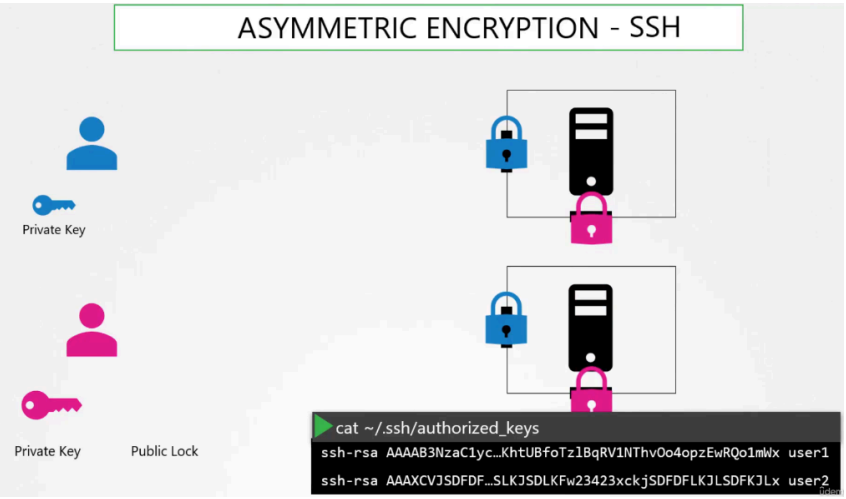
## 153. Kubernetes-Security-Primitives

- Authentication (인증) : 접근 가능 대상 관리
  - Username and Passwords, Username and Tokens, Certificates, External Authentication Providers (ex. LDAP), Service Accounts
- Authorization (인가) : 권한 관리
  - RBAC Authorization, ABAC Authorization, Node Authorization, Webhook Mode

## 154. Authentication

- static password file
  - csv 파일 생성 후 `kube-apiserver.service` 의 `-basic-auth-file=user-details.csv` 로 설정
- static token file
  - `-token-auth-file=user-token-details.csv` 로 설정
- 둘 다 권장하지 않는 방법

## 157. TLS-Basics




### 대칭/비대칭 암호화

- **대칭 암호화(Symmetric Encryption)**
  - 동일한 키로 암호화/복호화
- **비대칭 암호화(Asymmetric Encryption)**
  - Private Key와 Public Key(Public Lock이라 생각하면 쉽다) 쌍 사용

### 인증서

- CA (Certificate Authority) : 인증서의 유효성을 검증하는 신뢰할 수 있는 기관
- 인증서 서명 과정: CSR 제출 → 정보 검증 → 인증서 서명 및 발급

### PKI(Public Key Infrastructure)

- 인증서 관련 파일 형식:
  - Public key/인증서: `.crt`, `.pem`
  - Private key: `.key`, `-key.pem`

## 158. TLS-in-Kubernetes

- **루트 인증서**
  - CA가 루트 인증서를 관리하며 다른 모든 인증서 서명에 사용
  - ex) `ca.crt`, `ca.key`
- **서버 인증서**
  - 쿠버네티스 컴포넌트의 서버를 위한 인증서
    - ex) `apiserver.crt`, `apiserver.key`, `etcdserver.crt`, `etcdserver.key` ...
- **클라이언트 인증서**
  - kube-apiserver 입장에서는 아래 컴포넌트들이 모두 클라이언트
    - admin (REST API), scheduler, controller manager, kube-proxy, etcd client, kubelete client (다른 노드에 있는)

## 159. TLS-in-Kubernetes-Certificate-Creation

- **CA 인증서 생성**

```
# 개인키 생성
openssl genrsa -out ca.key 2048

# 인증서 서명 요청(CSR) 생성
openssl req -new -key ca.key
-subj "/CN=KUBERNETES-CA" # 구성요소의 이름을 지정 (Common Name, 즉 CN 필드에)
-out ca.csr

# 인증서 서명
openssl x509 -req -in ca.csr -signkey ca.key -out ca.crt
```

- **클라이언트 인증서 생성 (예: admin)**

```
# admin용 개인키 생성
openssl genrsa -out admin.key 2048

# CSR 생성 (그룹 정보 포함)
openssl req -new -key admin.key
-subj "/CN=kube-admin/OU=system:masters" # kube-control 명령을 실행할 때, kube-control client 인증을 위한 이름을 지정, mastser는 관리 권한을 가진 그룹 이름
-out admin.csr

# CA로 서명 (ca 인증서와 ca 키 지정)
openssl x509 -req -in admin.csr -CA ca.crt -CAkey ca.key -out admin.crt
```

- **서버 인증서 생성 (예: kube-apiserver)**

```
# 개인키 생성
openssl genrsa -out apiserver.key 2048

# CSR 생성 (SubjectAltName 포함)
openssl req -new -key apiserver.key -subj "/CN=kube-apiserver" -out apiserver.csr -config openssl.cnf

# CA로 서명
openssl x509 -req -in apiserver.csr -CA ca.crt -CAkey ca.key -out apiserver.crt
```

## 160. View-Certificate-Details

- 인증서 세부 정보 조회: `openssl x509 -in file-path.crt -text -noout`
  - issuer, common name, alternate names 등 확인 가능