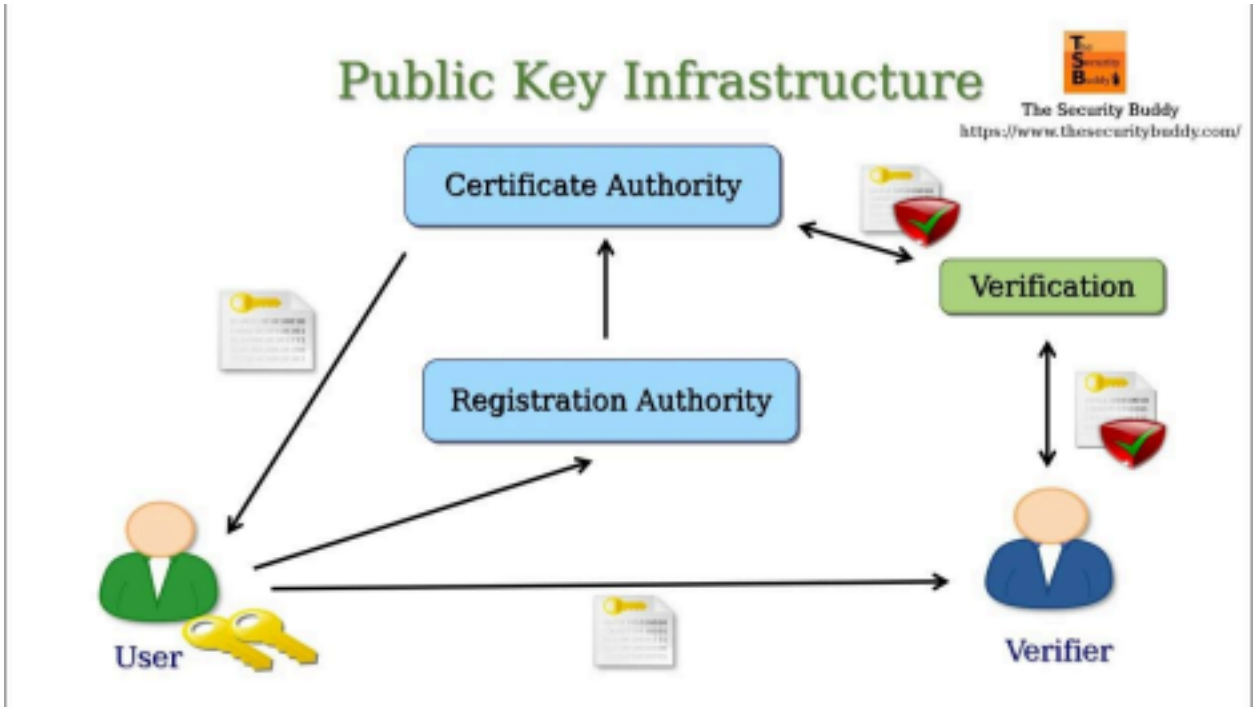
Cyber Security

Objective: Develop a Public Key Infrastructure (PKI) system that enables secure signing of digital certificates and verification of other certificates. By completing this assignment, you will gain an understanding of how public key verification works and how PKI operates.

Working of PKI



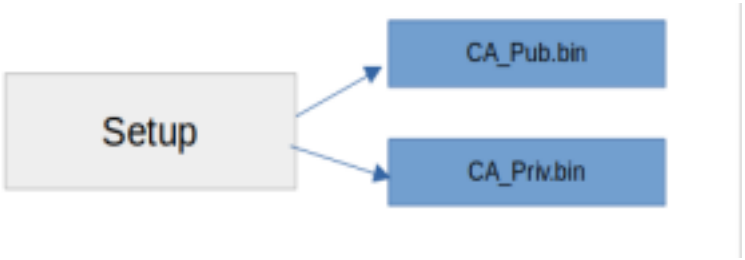
In this assignment, you have to create four programs.

1. Setup
2. KeyGen
3. IssueCertificate
4. VerifyCertificate

1. Setup

Objective : generates the public-private key pair of the CA(Certificate Authority) - saves those as two different binary files, i.e, CA_Pub.bin, CA_Priv.bin
Note : CA public key and private key pair must be 2048 bit long.

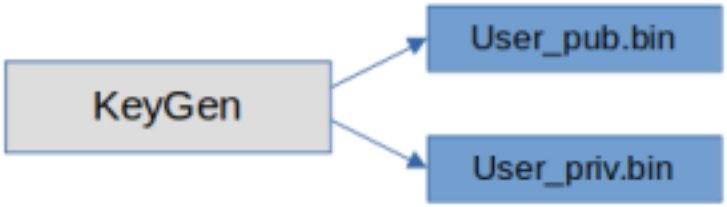
WorkFlow:



2.KeyGen

Objective : generates a public-private key pair for any user (same as the previous) - saves those as two different binary files - User_Pub.bin , User_Priv.bin
Note : user public key and private key pair must be 1024 bit long.

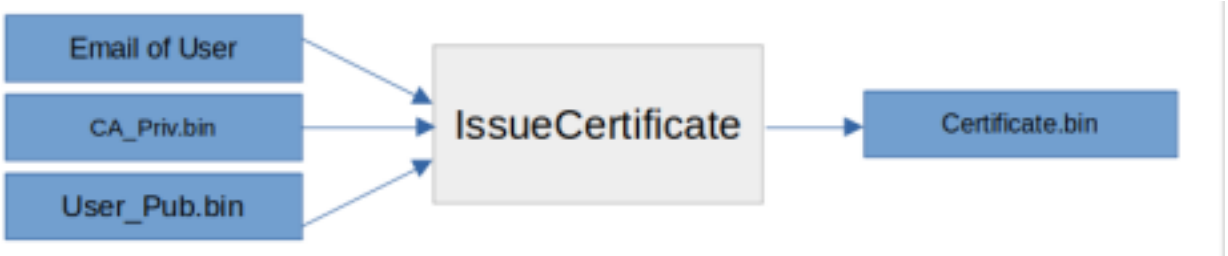
WorkFlow:



3.IssueCertificate

Objective : generates the certificate as Certifcate.bin
Input : the ID (email) of the user, the two files CA_Priv.bin, User_Pub.bin
Output : certificate.bin

WorkFlow:



Certificate Format:

Issuer Name: IIITA
Subject ID: user email id
Validity:

- **NotBefore:** Sun, 16 Jun 2024
- **NotAfter:** Sun, 22 Jun 2026

Signature Algorithm: DSA
Subject PublicKey: (RSA) your public key
Signature: CertificateSignature

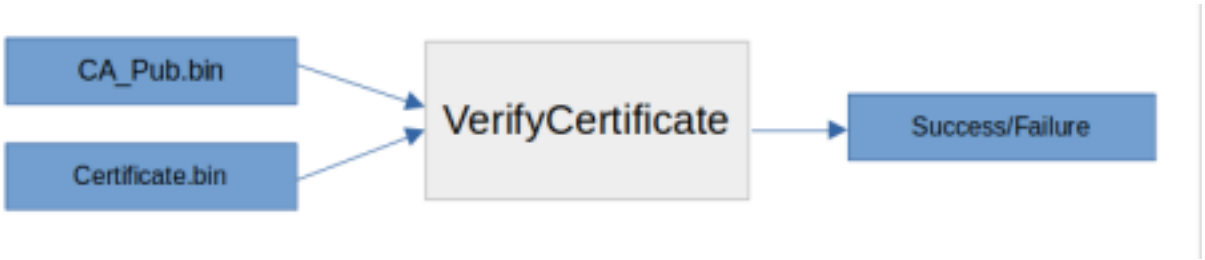
To generate signatures for certificates, follow these steps:

1. **Generate a Hash of the Certificate Data:** Note that the signature is not part of the data used for generating the hash.
2. **Sign the Hash using DSA Signature algo (Crypto++ function):** This creates the digital signature.
3. **Attach the Signature to the Certificate:** Include the digital signature in the certificate file, along with the certificate data.

4.VerifyCertificate

Objective : this programme verifies the certificate (certificate.bin).
Input : Certifcate.bin, CA_Pub.bin
Output : Prints Success / Failure.

WorkFlow:



To verify the signature of a certificate, follow these steps:

1. **Obtain the Certificate:**
    - Retrieve the certificate that needs verification.
2. **Extract the Signature and Data:**
    - Extract the digital signature from the certificate file and the data that was signed (i.e., the certificate data excluding the signature).
3. **Generate a Hash of the Certificate Data:**
    - Use the same hash function (e.g., SHA-256) that was used to create the original hash. Compute the hash of the certificate data.
4. **Verify the Hash and the Signature using DSA Verif:**
    - Use the Certificate Authority's public key to verify the digital signature. This will yield the hash value that was originally created and signed by the CA.
5. **Verify the Certificate's Validity:**
    - Ensure that the certificate is within its validity period and has not expired.