How can you trust this website?

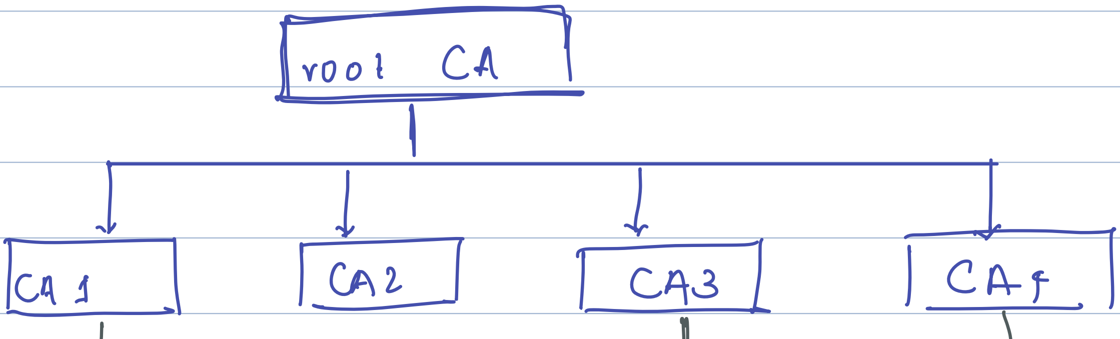
- How can Alice trust Bob on internet?

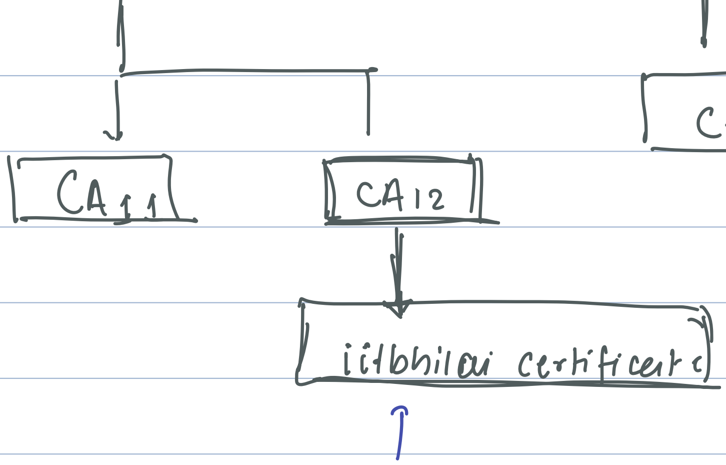
→ There should be some physical identity to verify that the website we are accessing and Alice on the internet are verified entities.

Solution:: Public key Infrastructure:

- Public key Infrastructure helps establish the identity of people, devices and services.

- A governing body behind issuing the digital certificate.

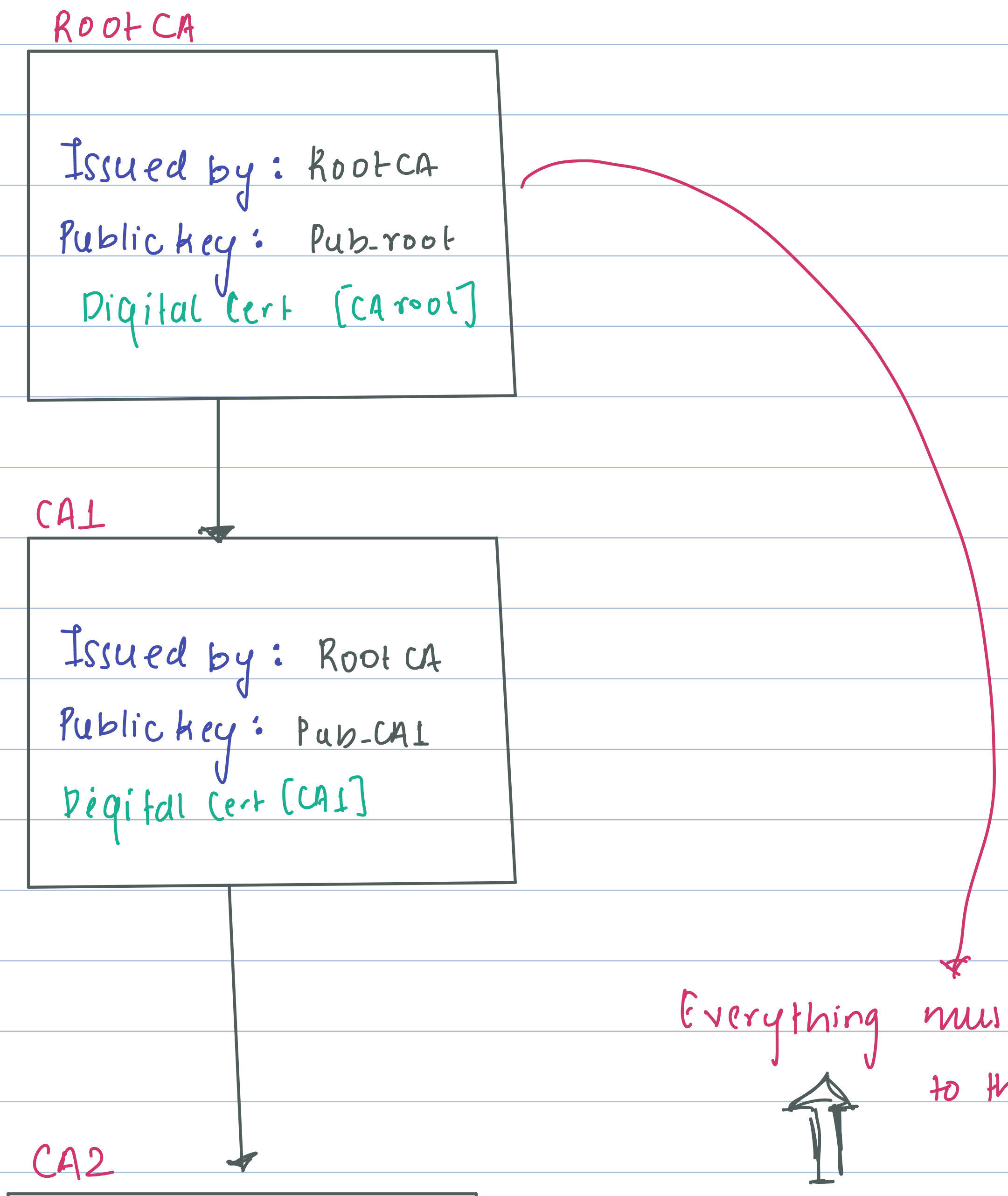




iitbhilai.ac.in certificate is provided by CA12.

it has its own digital certificate issued by CA12.

digital certificate => X.509 certificate


Root CA

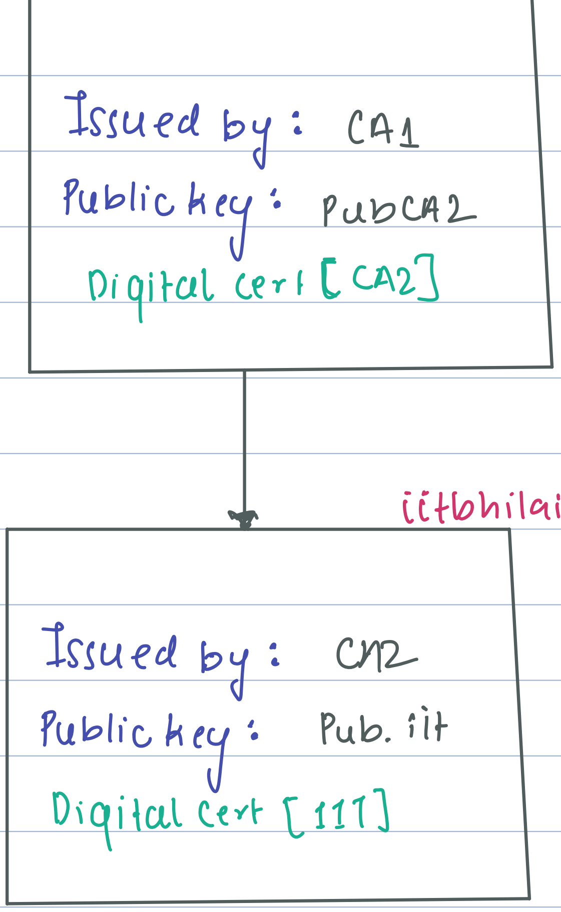
Issued by : RootCA
Public key : Pub-root
Digital Cert [CA root]

CA1

Issued by : Root CA
Public key : Pub-CA1
Digital Cert [CA1]

CA2

Everything must trace back to the root CA.



Issued by: CA1
Public key: PubCA2
Digital cert [CA2]

Issued by: CA2
Public key: Pub. iit
Digital cert [IIT]

Now check the Digital cert of CA2 using CA1's Public key

iitbhilai.ac.in

- If you want to check that the certificate is actually ecce

- Check the issuer and get it's public key.

- Check the digital cert of IIT using PubC2

“Digital certificates binds public key to the identity of the private key owner”.