Public Key Infrastructure

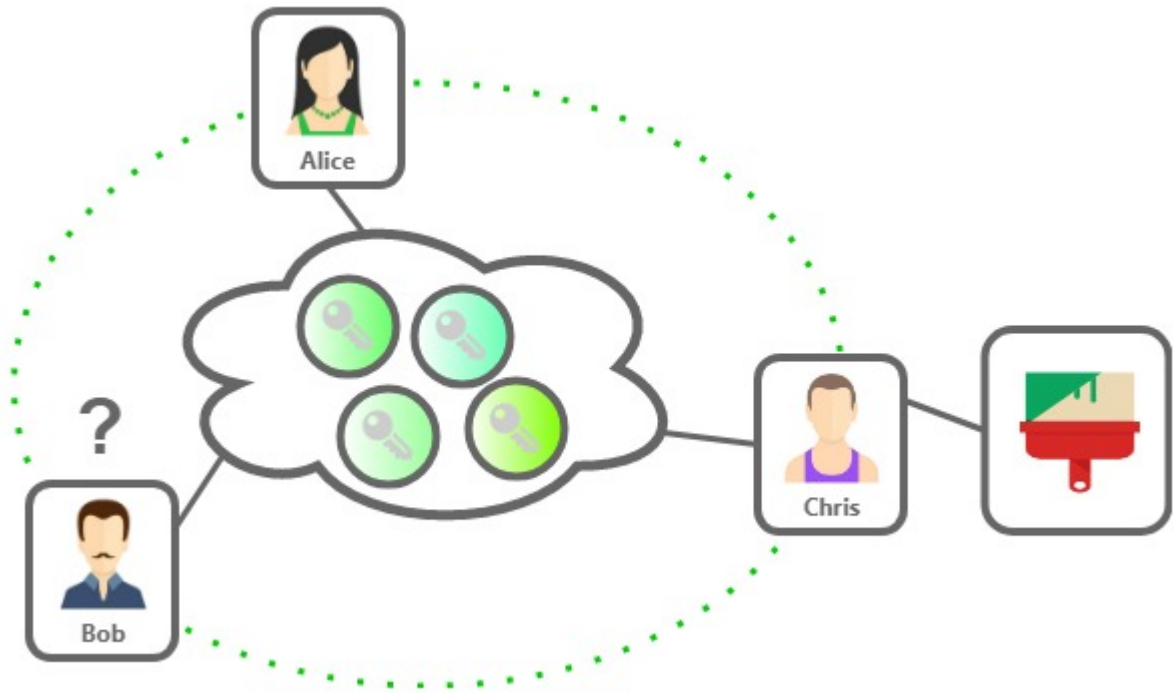
In this lesson, we will understand the concept of public key infrastructure and see how certificate authority works.

WE'LL COVER THE FOLLOWING

We have seen how Hash functions and asymmetric encryption can help us digitally sign any message.

On an open or insecure internet, in order for a receiver(Bob) to verify a signature done by a sender(Alice), he needs Alice's public key beforehand.

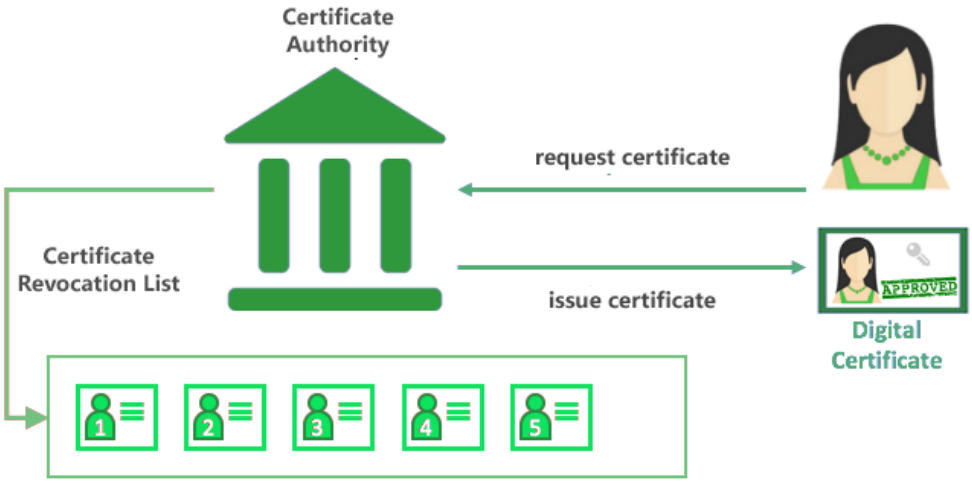
If Alice was to send her public key to Bob on the internet, how can Bob be sure that it is really Alice who has sent him her key and not Chris pretending to be Alice?



For the entire secure communication system to work, both parties(Bob and

Alice) need to establish trust in each other's public key while using the same open unsafe internet.
How to share the key and prove its ownership to ensure future secure communication?

To help solve this issue we have a concept of a trusted authority in the middle that all network participants trust. This trusted authority is called a CA or certificate authority.



Here is how it works with a CA:

1. Alice must contact the CA to get a certificate(digitally signed public key) to prove her public key to others. All other participants on the network will be able to trust the public key is Alice's if they trust the CA.

2. The CA would take Alice through an approval/on-boarding/manual-verification process and issue a certificate. The certificate itself is a list of certified attributes of the entity its issued to Alice. It has attributes like the public key, name of the holder etc. All this data is digitally signed by the CA using its own private key.

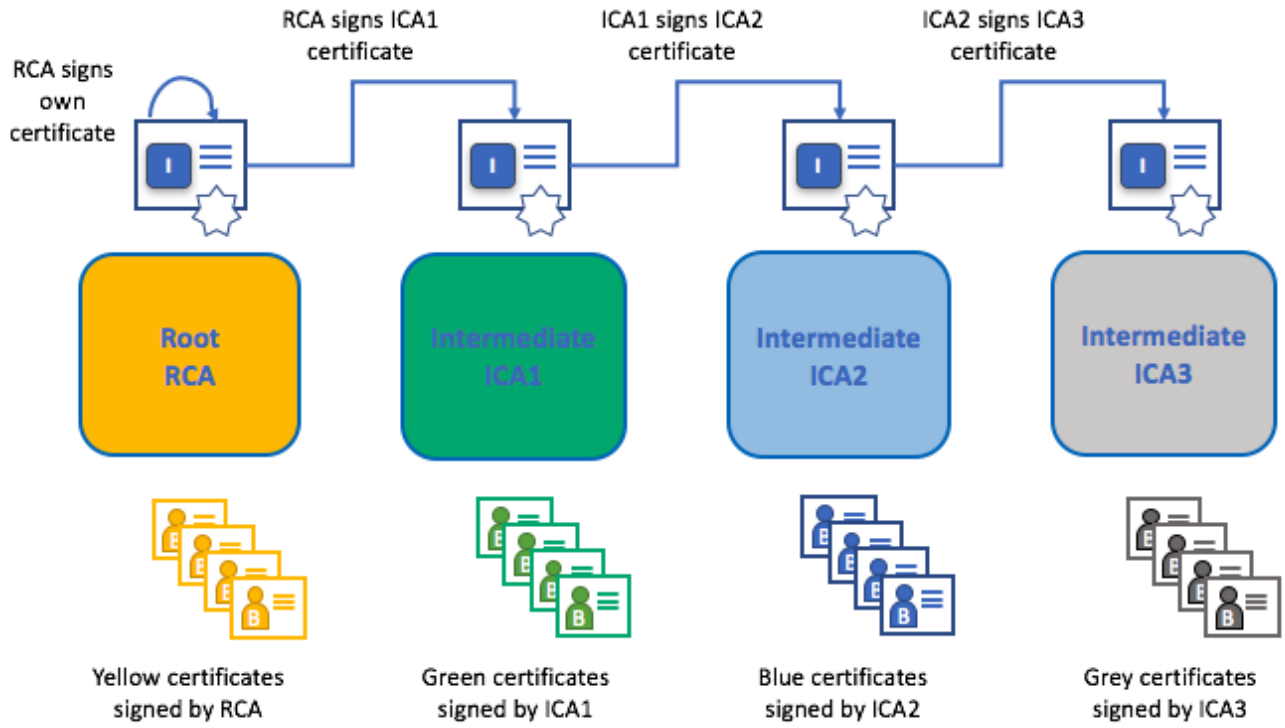
3. Alice then shares this certificate as a proof of her public key to Bob.

4. Since Bob has the CA in his trusted CA list(CA's public key), he can verify and trust the certificate shared by Alice and hence trust her public key.

Chain of Trust

A chain of trust is established between a Root CA and a set of Intermediate

CAs as long as the issuing CA for the certificate of each of these Intermediate CAs is either the Root CA itself or has a chain of trust to the Root CA.



Test Yourself

1 What is the primary purpose of a certificate authority?

COMPLETED 0%

1 of 2

In the next chapter, we will discuss blockchain data storage.