Digital Certificates

08 February 2024 17:07

{ Public key — Publicly available
{ Private key }

Scenario

Public key — Publicly

Lokesh — PU_A →

V

(PU_K, Pr_K)

L

(Pu,Pr)

A →

Avoid?

How do you verify the public key of an entity?

Digital certificate — Issued by a trusted third party
— CA — Certificate Authority

Name: Lokesh
Digital Sig of CA
Public key of Lokesh
Serial: No: unique -
Expires: /

} — Proof that the public key actually belongs to Lokesh -

Certificates — Verifies the identity

Contact a web Server — Certificate
Public key

Every computer
— Certificate — Public key

What's the use of Certificates? — To verify the public key (or) identity of an entity.

Who issues the certificate? — CA — Trusted third party (TTP)

What does DS contain — Pu, DS of CA, Name, Expiry and Serial No

X-509 Certificate