Class Notes Thursday

October 28th, 2021

**Digital Certificates:**

Issued by a trusted authority

Authenticates a user using their public key

Computer Bits that represent your identity

**Certificate Authority:**

**Certificate Chain:**

**Root Certificates:**

Browser or operating has a list of root certificates it already trusts, they use these to check against.

**Validation of Certificates:**

* + Browser
  + CA
  + Domain vs Extended

Agent Lets Encrypt CA

-> I own CS558

<- Sign this Nonce

-> Signed Nonce with a public key

Authorized Key Pair

We can now serve the website