Hello everyone! In this video you will learn about the digital certificate, it's need and the issuing process.

A digital Certificate is a digital file that certifies the identity, a public key of an individual or institution seeking access to computer-based information. It is issued by a Certification Authority (CA) and serves the same purpose as a driver's license or a passport. The purpose of digital certificates is to securely distribute public keys for protecting them from various online frauds.

Digital certificates also known as public key certificates allow key exchange without real-time access to public-key authority.
It binds an **identity** to a **public key** usually with other info such as period of validity, rights of use, etc

The digital certificate is issued by a certifying authority (CA). The CA signs the certificate with its own private key to approve that the public key mentioned in the certificate, officially belongs to the holder.
with all contents **signed** by a trusted Public-Key or Certificate Authority (CA), it can be verified by anyone who knows the public-key authorities public-key. Usually, all modern web browsers have the public keys of the certifying authorities.

Certifying authorities are Digital world's equivalent to passport offices. They issue digital certificates and validate holders' identity and authority, By embedding an individual or institution's public key along with other identifying information into each digital certificate and cryptographically signing it as a tamper-proof seal verifying the integrity of the data within it and validating its use.

Some of the authorized Certifying authorities, authorized by the controller of Certifying Authorities, Government of India are NIC, IDRBT, Safe script, E-Mudra etc.

The signed certificate by a CA contains its version number, serial number, issuer name, subject name, public key, etc. the objective of these fields is well written in the table.

Let’s understand the process of digital certificate issuing and distribution. The user(Bob here) creates a key pair using the public key cryptography algorithm and applies for the digital certificate to the Certifying authority by providing the public key and other supporting information and documents. The certifying authority verifies the user’s information and creates the certificate by digitally signing it with its private key. The CA also updates its database with the identity and key pair of the user.
After creation, the certificate is ready to be distributed to the public. Anyone having the public key of the CA can verify the certificate and use the public key given in the certificate for communicating with the user.

Thank You…