Public key Infrastructure

Presented By **Eshita Guin**
Dept: Computer Science and Engineering
Roll no: 16800116074
4th year, 8th Sem

Public key Infrastructure:

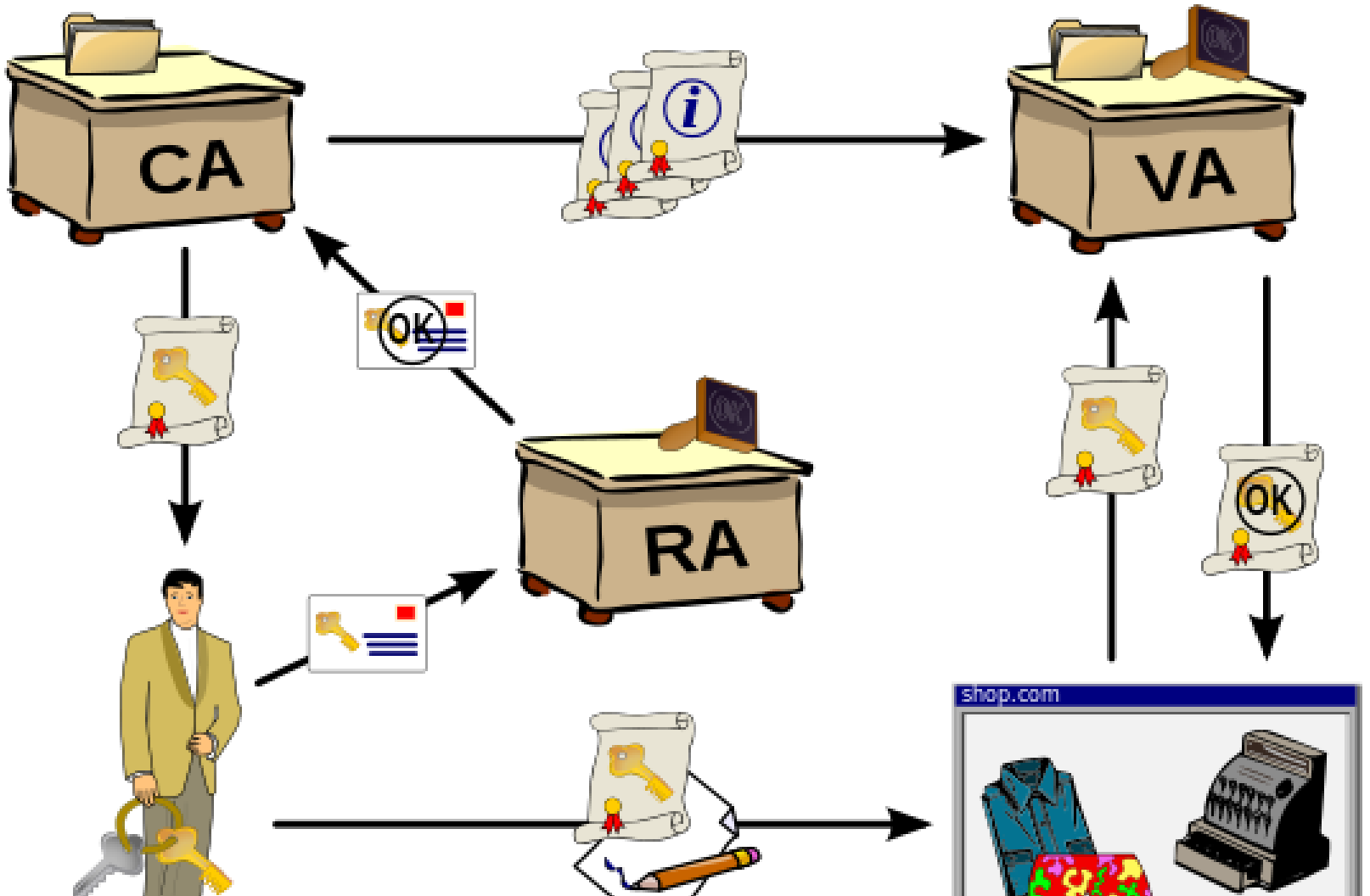
- **A public key infrastructure (PKI)** is a back-end cybersecurity measure that is described as a “set of rules, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.” PKI is based on asymmetric cryptography and is widely used today to secure electronic communication for online shopping, Internet banking and email as well as to protect communications between millions of users and the websites they connect to using HTTPS.

Component Of PKI:

- Certificate Policy
- Root Certificate Authority (CA)
- Intermediate CA
- Certificate Database
- Revocation Services
- Digital Certificate

Diagram Of Public key Infrastructure:

Diagram:



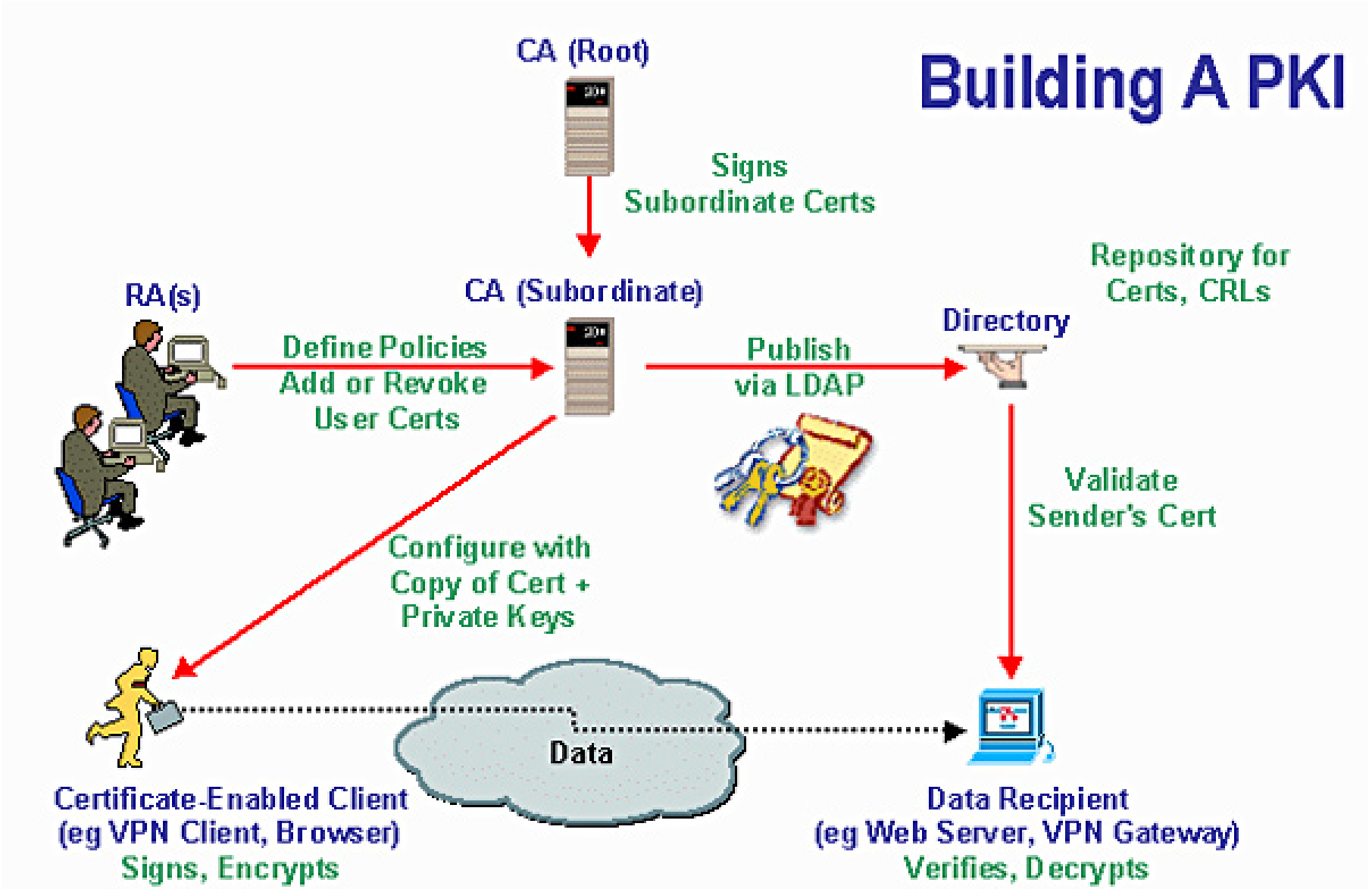
What is PKI used for?

- “PKI enables trusted electronic identities for people, services and things, which make it possible to implement strong authentication, data encryption and digital signatures.
- “These security mechanisms are used to grant secure access to physical and digital resources; secure communication between people, services and things; and enable digital signing of documents and transactions,” says Furuhed, product manager of Nexus’s certificate authority (CA) software Certificate Manager.

Popular Ways PKI is Used

- Securing emails
- Securing web communications (such as retail transactions)
- Digitally signing software
- Digitally signing applications
- Encrypting files
- Decrypting files
- Smart card authentication

How does Public Key Infrastructure (PKI) work?



What is a PKI good for?

- Public Key Infrastructure (PKI) is a security mechanism for guaranteeing that on-line communications are authentic and private. It is gaining as a means implementing secure e-commerce, thereby combating one the major concerns about doing business online.

Advantage And Disadvantage of PKI:

- Advantage: In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem. The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.
- Disadvantage: Speed. One disadvantage of public-key encryption is that is is slower than other methods, such as secret-key encryption. In secret-key encryption, a single key provides that only way to encrypt and decrypt, simplifying and speeding up the process.

Conclusion:

If you want to ensure completely secure transfer of data, PKI is a must. Whether you want secure communication for your organization, for IoT devices, for your personal emails, for secure data transfer or for any other purpose, PKI is the way to get complete security with an assurance of identity.

Reference:

- Wikipedia
- Network Sequrity Essentials- By William Stallings

Thanking you