Introduction to Certificate authority and letsencrypt.org

Mahdi ataeyan

http://www.ataeyan.com





SSL - TLS

- cryptographic protocols to provide communication security over the Internet.
- •exchange a symmetric key.
- •session key to encrypt data flowing between the parties.





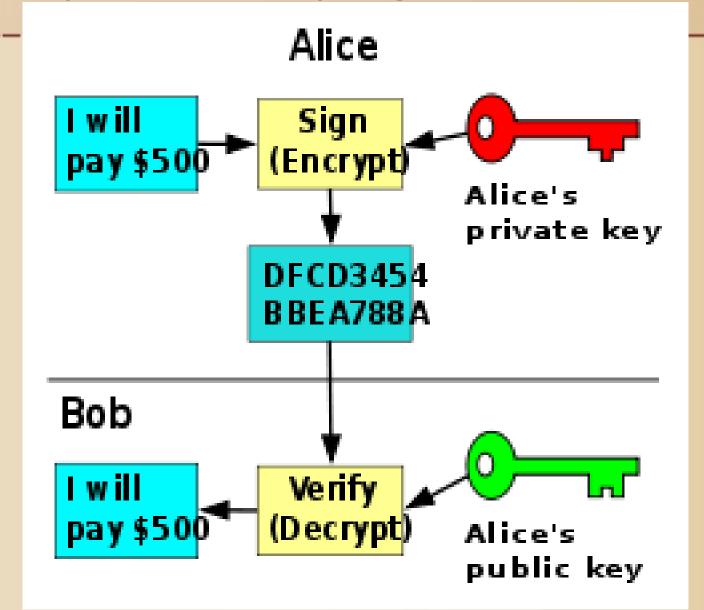


Key Generation Program

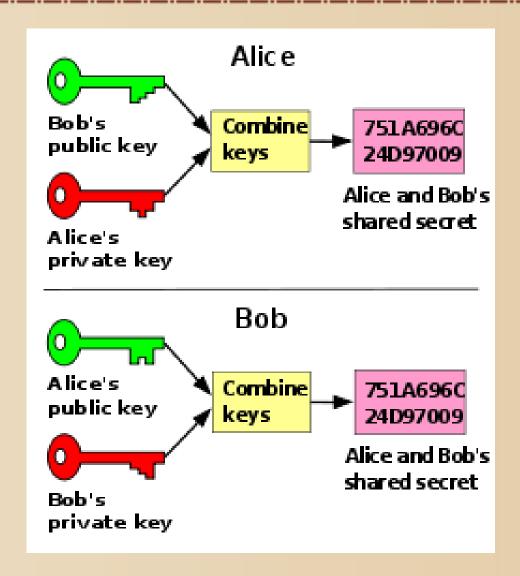
















Key Management

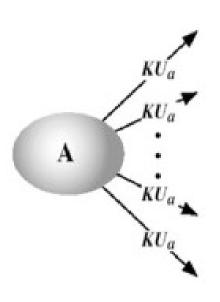


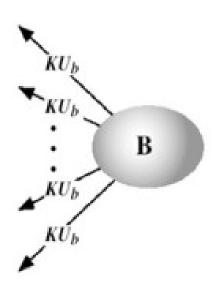
Distribution of Public Keys

- Public Announcement of Public Keys
- Publicly available directory
- Public-key authority
- Public-key certificates



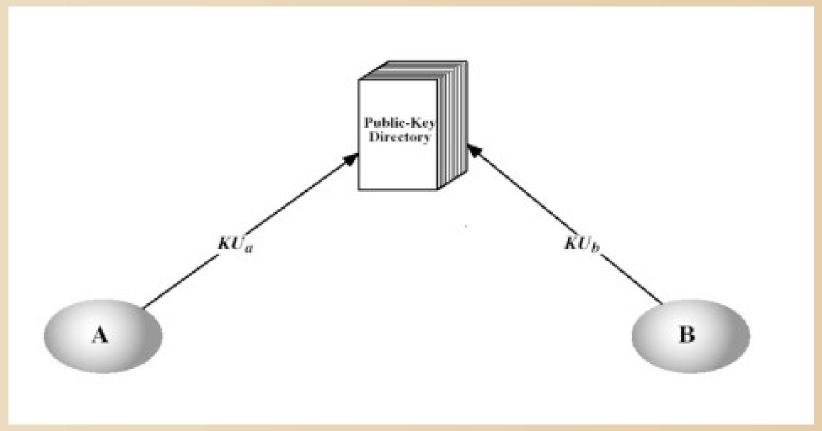
Public Announcement of Public Keys







Publicly available directory



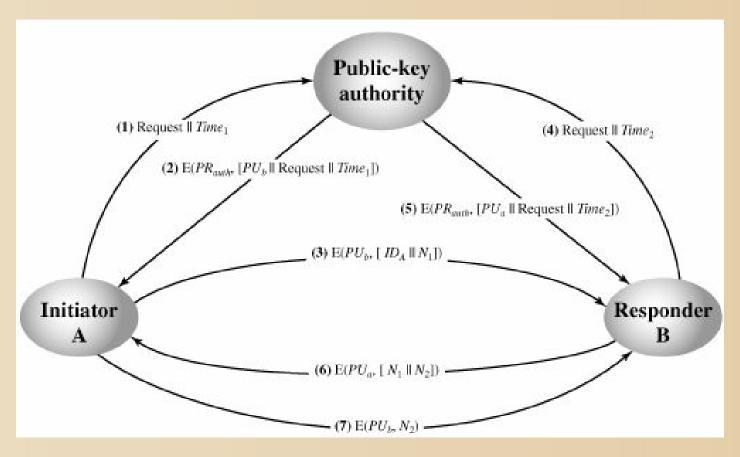


Public-key authority

- a central authority maintains a dynamic directory of public keys of all participants
- each participant reliably knows a public key for the authority



Public-key authority





Public-key certificates

- each and every participant can determine the identity and the public key of of owner of certificate
- Verification can be done by intended participant.
- The generation, modification and updating only can be done by the certification authority.
- Participants can identify the time limit and session for every certificate



Digital Certificate

- an electronic document used to prove ownership of a public key.
- The certificate includes information about the key, its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct.

CertA = < IDA, PKA, Validity Period, SignCA(IDA, PKA, Validity Period) >

Type if Digital Certivicates

- Server certificates
- Personal certificates
- Organization certificates
- Developer certificates

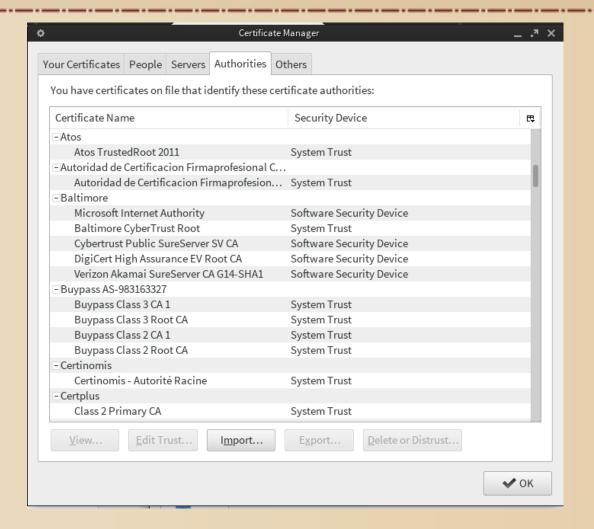


Certificate authority

- CA is an entity that issues digital certificates.
- CA says: yes, this person is who they say they are, and we, the CA, certify that



browsers





ubiquity

high ubiquity meaning that the CA is commonly pre-installed -- and almost universally accepted.

Mozilla Included CA Certificate List



letsencrypt.org

- A Certificate Authority to Encrypt the Entire Web
- Arriving Summer 2015
- Mozilla, Cisco, Akamai, Identrust,
 University of Michigan



letsencrypt.org

- •reducing setup time to 20-30 seconds.
- •lets-encrypt-preview



References

http://www.facweb.iitkgp.ernet.i n/~sourav/KeyManagement.pdf https://www.eff.org/deeplinks/2014/11 /certificate-authority-encrypt-entire -web https://letsencrypt.org/