Week 3 Assignment 1: Public and Private Key Management

Shaun Hoadley

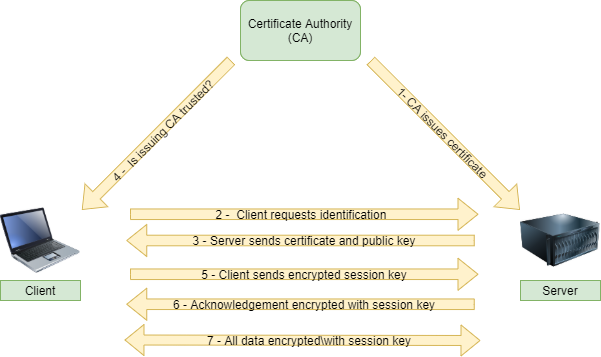
CST316: Information Security Management

Professor Amr Elchouemi

July 27, 2021

When it comes to the management of public and private keys in asymmetric cryptography, there are many things to consider. First, there are the differences between public and private keys. The public key is used to encrypt the data from the sender. Public keys are mathematically linked to the private keys of the receiver. The private key is used to decrypt data from the sender if the private key is linked to the public key that encrypted it.

Certificate management is used for verifying that an entity’s identity and public keys are bound to each other (Wills, 2019). Following is a diagram of how digital certificates are issued by certificate authorities (CAs).



***Figure 1. How CAs issue digital certificates.***

Digital certificates work as electronic passwords on the transport layer in network communications. Transport layer security, or TLS, uses the digital certificate during the handshake between devices or nodes to validate user keys and generate session keys for the established connection.

**References**

Wills, M. (2019). [(ISC)2 SSCP Systems security certified practitioner: Official study guide](https://ashford.instructure.com/courses/87741/modules/items/4439845) (2nd ed.). John Wiley & Sons.