Information: What is a Digital Certificate?

- What is a digital certificate?
- What makes up a digital certificate?
- Why should I use a digital certificate?

What is a digital certificate?

A digital certificate is a pair of files on your computer that you can use to create the digital equivalent of handwritten signatures and sealed envelopes. Each pair of files is divided into two parts: the public key and the private key. The public key is the portion that is shared; the private key is the portion that you, and only you, should have access to. Your computer and programs understand how to share only the public portion of your keys so that others can see them, while still keeping your private keys secure.

For example, when sending an email message, you can digitally sign the message by attaching your digital certificate. Once they receive the message, recipients can verify that it came from you by viewing the small attachment on the email, which contains your public key information. This protects you from people who might try to "spoo" an email that looks like it came from you but is really sent from a different email account.

You can also use digital certificates to electronically sign documents. This is one reason why it is extremely important to protect the private key portions of your certificate files and never share them. You could be legally bound to something, and it would be extremely difficult to prove that it wasn't you who digitally signed the message.

When you encrypt a message, you create the equivalent of a sealed envelope so that only you and the recipient can see the message. Normally, when you send an email message, it is the electronic equivalent of a postcard—anyone who has access to the network between you and the recipient can potentially read that postcard. With the encryption offered by the digital certificates, you can avoid this problem. In the case of encryption, you use the recipient's public key, which is easy to find using the university's directory, to encrypt the message. Only the recipient has the private key that allows the message to be decoded.

The digital certificates that are available from ITS are issued by an independent, recognized and mutually trusted third party that guarantees that the certificate is valid, and therefore guarantees that you can trust it. This third party is known as a certificate authority. The university has chosen the InCommon Federation, which uses Comodo Ltd., as its certificate authority.

What makes up a digital certificate?

The electronic files that comprise the digital certificate contain:

1. The person's name
2. An email address
3. A serial number
4. A public key
5. An expiration date (certificates are valid for five years)
6. A digital signature

When you download a digital certificate, you will receive both public and private keys. The public keys are the ones that you will use to sign and encrypt emails. The private keys are the ones that will be stored on your computer. You should never, ever share the private keys.

Why should I use a digital certificate?

There are several benefits to using digital certificates:

- Send signed email messages. This ensures the recipients that the message came from you and not someone pretending to be you. This is particularly important when sending out official university messages, such as from the President's Office.
- Encrypt the contents of email messages and attachments, protecting them from being read by online intruders. Only your intended recipient can decrypt them.
- Streamline business processes by allowing people to use digital certificates to electronically sign documents or approve something at a given stage of the process.