

# Making Sense of Digital Certificates

## Overview

The Digital Certificates service offered by Information Technology Services (ITS) lets you take advantage of security that is built into the Windows, Mac OS X and Linux computer programs you use every day. ITS encourages you to work with your desktop support staff and the ITS Help Desk to ensure that you can download your certificates and set up programs correctly.

You may know that certificates work with other security technologies like SmartCards and Web-based authentication. While the Digital Certificates are capable of working with these technologies, UT is not offering them at this time.

## What are Digital Certificates?

Digital Certificates are files that let you electronically sign and encrypt files. Each certificate comes with a public and private portion, called “keys.” The public key is what you share with the world to allow them to verify your electronic signature and to send you encrypted messages that only you can decrypt. The private key is what you use to sign and what you use to decrypt. **Protecting the private key portion of your certificates is very important.** The programs that use certificates will help ensure that you share only the public keys.

|                    | Signing  | Encryption  |
|--------------------|--|---|
| <b>Public Key</b>  | E-mail address, expiration date, changes to document since certificate was attached. | Code used to encrypt a message. Only your private key can read that code. |
| <b>Private Key</b> | E-mail address, expiration date, your personal signature.                            | Code used to read a message encrypted with your public key.               |

## Why use Digital Certificates?

Any new technology requires a good reason to adopt it. Here are some things to consider with digital certificates:

- The primary use for certificates right now is with e-mail on Windows, Mac, and Linux computers. File and folder encryption is available for Windows users. Certificates do not enable file or folder encryption in Mac OS X.
- Are you using e-mail to send Category-I data, such as human-subjects research data, donor, legal, or health information to other faculty or staff? Certificates let you encrypt that information as long as both the sender and receiver have certificates.
- Are you using a laptop or other portable device that has Category-I data? Certificates can enable security options required by UT System.
- Are you using e-mail to send student grades or other FERPA information? Students are not included in the Digital Certificates service right now, so you won't be able to encrypt messages to them using the Digital Certificates. You may want to think about secure options on UT Direct that are built to handle student information.
- Do you mostly use a mobile device to stay in touch during the day? While you should be able to read signed messages on your BlackBerry, PDA, and almost any computer or Web-based mail program, some devices won't let you install certificates, so you may not be able to read encrypted messages.
- If you don't have your certificate files on the computer where you are reading e-mail messages, you will not be able to read encrypted messages, nor send signed or encrypted messages. If there is potential that will spend the majority of your computer time where you can't install certificates, they may provide limited value.
- If you share a computer with someone else, talk to your desktop support staff about whether you should use certificates on that computer.

## Moving certificates between computers

After you download your digital certificate to your primary computer and set up your e-mail, you will want to copy the certificates to any other computers you may use—your home machine, portable device, or other machine.

Make sure that you follow the setup procedures on each computer. It is useful to consult with your desktop support staff or the ITS Help Desk so they can help you.

## Backing up your certificates

It is important to have a backup copy of your signing and encryption files. A backup contains both your public and private keys, and it ensures that you can install the certificates on a new or rebuilt computer.

**Backups must be stored in a secure location to which only you have access.**

You can ask your desktop support person to help you create a backup on WebSpace, CD, USB drive, or other media, but it would not be appropriate to ask that person to store the media for you. If you choose physical media, lock it up in a safe or cabinet to which only you have access. If you choose WebSpace, make sure you save the files in a folder that is not and will never be shared.

## Reporting lost or compromised certificates

Report as soon as possible if you lose your computer, your certificates stop working, or you suspect that someone else has gained access to your private keys. Use the online form at <http://www.utexas.edu/its/user-certs/answers/revoke.php>

## Sharing your public certificates

In addition to verifying that your e-mail messages originated from your e-mail address, your public key enables others to send you encrypted e-mail.

Without that public key, there is no way to encode a message in a way that only you can decode it.

The easiest way to make your public key available is to send a signed e-mail message, which automatically includes the public encryption information that someone else needs to encrypt a message to you.

What if you've never sent a signed message to a person who wants to send you an encrypted message? The university has set up the electronic directories to help:

- The University White Pages (<http://www.utexas.edu/directory>) includes the public certificate file for everyone who has been issued a certificate through the Digital Certificates service.
- The Global Address List (GAL) in the Austin Active Directory contains the public certificate for everyone who uses the Digital Certificates service. Exchange subscribers can use the GAL.

You can set up your e-mail programs to search these directories automatically.

## More Information

The ITS Web site contains more background information and instructions for all the procedures mentioned here, as well as requesting and downloading certificates.

**Web site:** <http://www.utexas.edu/its/user-certs>

**Faculty Help Desk number: 512-475-9200**

**Staff Help Desk number: 512-475-9400**