

# Update to Chapter 12

---

## Keychain preferences

One helpful feature of the Keychain Access application is that it displays its status in the menu bar. One glance at the icon and you can quickly tell if your Keychain is locked or unlocked. (See Figure 12.15.) You can also choose to lock and unlock the Keychain manually from the menu bar icon, as well as launch the Keychain Access application.

**FIGURE 12.15**

Keychain Access, menu bar style



A new feature in the Keychain Preferences is the ability to reset your keychain. Click on the Keychain Access menu --> Preferences. Under the general tab is a Reset My Keychain button. This resets your keychain to factory defaults, renames the current keychain, and removes it from use. This is especially useful if you are having unsolvable issues with your keychain such as Safari constantly bugging you for a password and it not going away.

## Certificates and Kerberos

Certificates and Kerberos tickets (a specialized certificate) can be created, destroyed, and managed through keychain access. Kerberos and the issuance of certificates allow MacOS X to transmit data securely over an unsecured network.

A digital certificate is an electronic document that associates your digital identity with other information, such as your name, e-mail address, or business. A certificate contains the public part of your digital identity, the identity of the organization (“certificate authority” or CA) that signed your certificate, and whatever other data it chose to associate with your identity. A certificate is usually restricted for a particular “use,” such as digital signatures, encryption, or use with Web servers. It is possible to make one identity (and one certificate) with multiple uses, but is unusual. A certificate is only valid for a limited amount of time, after which it becomes invalid and must be replaced with a newer version. The certificate authority can also invalidate (“revoke”) a certificate before it expires. The validity of a certificate can be verified electronically, using the “public key infrastructure” or PKI, which Mac OS X supports.

Built into keychain access under the Keychain Access menu is the Certificate Assistant. This assistant allows you to create a Certificate Authority (CA), create CA relationships, request certificates from existing CAs, set the default CA, and view and evaluate existing certificates.

### *What is a Certificate Authority?*

A certificate authority (CA) is a digital identity that you create for use by other parties. It is part of or the start of a digital certificate chain. As long as all portions of the chain are valid, the last CA in the chain is valid. Since CAs are digital identities themselves, they can also be validated by another CA. All this certificate validity is automatically determined by Mac OS X when it evaluates a certificate.

### *Where do I keep my certificates?*

Mac OS X stores digital identities, including certificates, in your keychain. From there, it is instantly available to all your programs, including Mail, Safari, iChat, .Mac, and so on. Likewise, certificates for others (mail correspondents, Web sites, or iChat friends) are also stored in your keychain as your computer obtains them for you. You can use Keychain Access to view and manipulate your certificates. You can move and copy certificates freely because they don’t contain personal or private information that

you need to protect. If you need to send a certificate to someone else, you can export it using Keychain Access and send it safely through e-mail or by other means and the recipient can import the certificate using Keychain Access, and vice versa.

Kerberos tickets are types of certificates. Kerberos lets two parties who have previously identified themselves to each other — in this case, through .Mac digital certificates — to validate each other's identity and share information securely. The system can issue tickets, which authorize certain access for specific periods of time.

Click on the Keychain Access menu and then Kerberos Ticket Viewer. Here you can create, destroy, and renew tickets. In the event you are having trouble authenticating off a server that uses Kerberos (such as Back to My Mac), this is a great way of forcing a ticket to refresh itself to allow server access.

Advanced use, creation, and management of Kerberos tickets and certificates are beyond the scope of this book. For more information please visit <http://www.apple.com/support/> and <http://web.mit.edu/Kerberos/>.