Appendix C

Understanding the Local KDC

The local Key Distribution Center (LKDC) facilitates single sign-on for Apple Filing Protocol (AFP) file sharing and screen sharing, and although it is outside the scope of this book, Back to My Mac. Every computer running Mac OS X or Mac OS X Server (version 10.5 and later) has its own LKDC that facilitates access to the Kerberized services running locally.

Because the LKDC shows up when you look at various configuration files, you may want to understand how it fits in with the other authentication services. Even though Apple Knowledge Base article TS1245, "Mac OS X 10.5: Duplicate computer name alert when binding to Open Directory" (support.apple.com/kb/TS1245) refers specifically to an issue with Mac OS X v10.5, it contains a good explanation of the LKDC: "Every computer running Mac OS X or Mac OS X Server, from version 10.5 and above, maintains a local KDC for local computer security. A computer-specific certificate named com.apple.kerberos.kdc is created during the installation of OS X and a SHA1 hash of the certificate is generated and entries are added to the Kerberos keytab for each service that uses the LKDC. This SHA1 hash is part of the computer account created for clients when bound to Open Directory and must be unique for each client computer."

With that in mind, once your computer running Mac OS X or Mac OS X Server joins a Kerberos realm, its services no longer use the LKDC, and it shouldn't interfere with authentication, even though you may still see traces of, and references to, the LKDC.

Use the following instructions with two Mac OS X computers that are not part of any other Kerberos realm to demonstrate that you can obtain a Kerberos Ticket Granting Ticket (TGT) from another computer's LKDC simply by browsing for services and authenticating. The other computer must not be part of another Kerberos realm, otherwise its services will not be configured for its own LKDC.

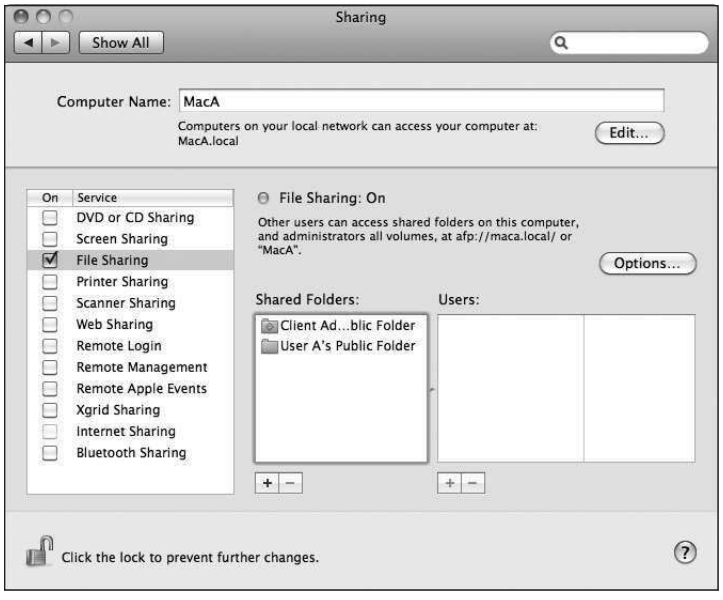
The steps are as follows:

1. On one Mac OS X computer, use the Sharing pane of System Preferences to configure the Computer Name to be `MacA`.

2. On MacA, use the Accounts pane of System Preferences to create a standard user `User A` with short name and password `usera` on computer MacA.

3. On MacA, select Guest Account from the accounts list, and then select the "Allow guests to connect to shared folders" checkbox.

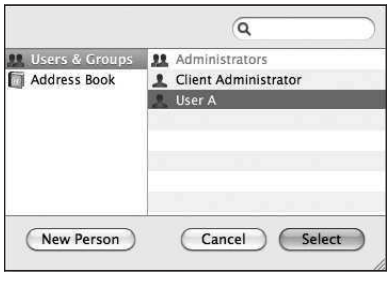
4 On MacA, open the Sharing pane in System Preferences. Select the File Sharing radio button, select File Sharing, and then confirm that User A's Public Folder is included in the list of Shared Folders.



5 On MacA, enable Screen Sharing, and then select the Screen Sharing checkbox.

6 On MacA, click the Add (+) button to add more users that are allowed to authenticate to MacA in order to take control of the keyboard and mouse remotely.

7 Select User A from the list of Users & Groups, and then click Select.



8 On MacA, confirm that User A is listed as shown in the following figure, and then quit System Preferences.

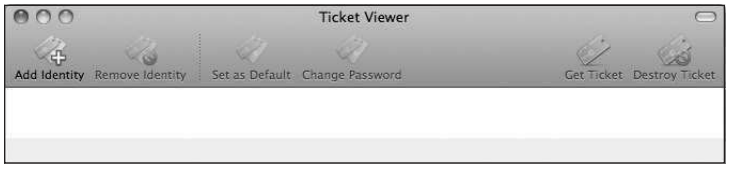
9 On a second Mac OS X computer, use the Sharing pane of System Preferences to configure the Computer Name to be `MacB`.

10 On MacB, create a standard user `User B` with short name and password "`userb`".

11 On MacB, log out, and log in with User B credentials.

12 On MacB, open Ticket Viewer (from /System/Library/CoreServices). Note that there should be no identities listed.

Leave the Ticket Viewer window open and position it so that you can see when a ticket automatically appears.



13 On MacB, open Terminal (from /Applications/Utilities).

14 On MacB, in Terminal, enter the following command:

```
MacB:~ userb$ klist
Klist: No credentials cache found while getting the ccache principal
```

Because this is a new local user account that just logged in, it is expected that no credentials cache is found.

Keep the Terminal window open.

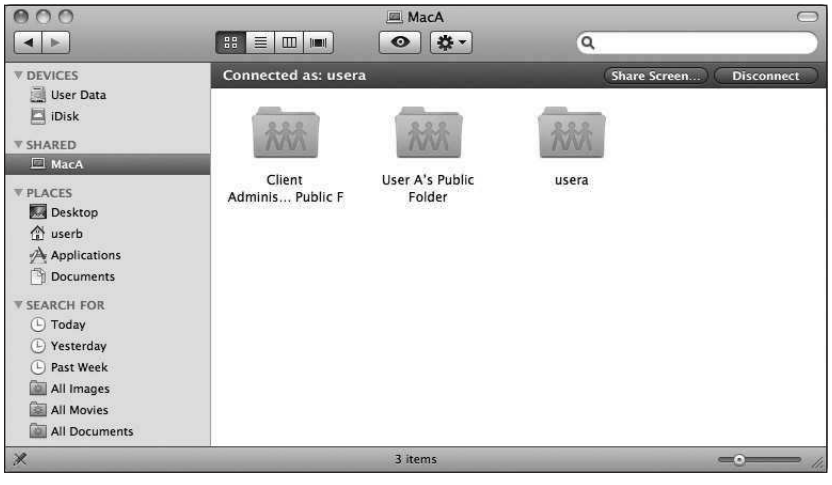
15 On MacB, use the Finder to browse for file services. Open a new Finder window, and then click the icon for the other Mac OS X computer (MacA) in the SHARED section of the Finder sidebar.

Your computer connects as Guest for AFP file sharing to the AFP service offered by computer MacA. In the following figure, you are logged in as User B on MacB, and you have connected as Guest from MacB to MacA, which you configured to allow AFP guest access. Note the text under the Finder's toolbar: "Connected as: Guest." Note also the two buttons in the upper-right corner: Share Screen (for virtual network computing [VNC] for screen sharing) and Connect As (for AFP file sharing).

16 On MacB, click Connect As to authenticate as a user rather than a Guest. Authenticate as a user local to MacA.

17 On MacB, note that you are now connected as User A to MacA in the Finder. Note that the status under the toolbar is "Connected as: usera," the two buttons in the upper-right corner are Share Screen and Disconnect, and the Finder window now displays User A's home folder (usera), whereas previously the Finder window displayed Public folders only.

For this exercise, do not close or navigate away from this Finder window.



18 On MacB, note that Ticket Viewer now displays a valid ticket.

As User B on MacB, you now have a valid Ticket Granting Ticket (TGT) for User A in the LKDC for MacA. This is somewhat amazing, as you did not configure MacB or MacA to join each other's LKDC realm, and all you had to do was select a service and authenticate.

Do not close the Ticket Viewer window; you will use it later.

19 On MacB, in the Terminal window, enter the `klist` command again. This confirms that you have a TGT (the ticket that starts with `krbtgt/LKDC`), and it also shows that you have a service ticket for the AFP service on MacA (the ticket that starts with `afpserver/LKDC`). The string `AE6139ABAA945739A7635FCA721D36AA9D20A19E` is the SHA1 hash of MacA's unique certificate (com.apple.kerberos.kdc).

```
MacB:~ userb$ klist
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: usera@LKDC:SHA1.AE6139ABAA945739A7635FCA721D36AA9D20A19E
Valid Starting     Expires            Service Principal
10/26/09 16:19:49  10/27/09 02:19:27  krbtgt/LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E@LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E
    renew until 11/02/09 15:19:49
10/26/09 16:19:50  10/27/09 02:19:27  afpserver/LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E@LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E
    renew until 11/02/09 15:19:49
```

20 On MacB, click the Share Screen button in the Finder window.

Because you have a TGT for MacA's LKDC, when you click Share Screen from the Finder window, Mac OS X automatically obtains the necessary service ticket on your behalf.

The Screen Sharing application automatically opens with a session for MacA, without you having to provide authentication again.

21 On MacB, in Terminal, run the `klist` command again, and note the additional entry for Screen Sharing (the service ticket that starts with `vnc/LKDC`).

```
MacB:~ userb$ klist
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: usera@LKDC:SHA1.AE6139ABAA945739A7635FCA721D36AA9D20A19E

Valid Starting     Expires            Service Principal
10/26/09 16:19:49  10/27/09 02:19:27  krbtgt/LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E@LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E
    renew until 11/02/09 15:19:49

10/26/09 16:19:50  10/27/09 02:19:27  afpserver/LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E@LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E
    renew until 11/02/09 15:19:49

10/26/09 16:20:49  10/27/09 02:19:27  vnc/LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E@LKDC:SHA1.
AE6139ABAA945739A7635FCA721D36AA9D20A19E
    renew until 11/02/09 15:19:49
```

22 On MacB, quit Screen Sharing, Terminal, and Ticket Viewer, and then click Disconnect in the Finder window.

23 Optionally, on MacA, deselect the File Sharing and Screen Sharing options, if they were not originally selected.

You have demonstrated that for Mac OS X computers that are not part of another Kerberos realm, you can obtain a TGT in another Mac OS X computer's LKDC realm, and then use this TGT to access another service that is Kerberized in that LKDC realm, without providing user name and password credentials to authenticate.