




Smart Card Setup Guide

 Apple Computer, Inc.
© 2006 Apple Computer, Inc. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of Apple.

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Every effort has been made to ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

Apple, the Apple logo, Keychain, Mac, Macintosh, and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Safari and Tiger are trademarks of Apple Computer, Inc.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products.

The product described in this manual incorporates copyright protection technology that is protected by method claims of certain U.S. patents and other intellectual property rights owned by Macrovision Corporation and other rights owners. Use of this copyright protection technology must be authorized by Macrovision Corporation and is intended for home and other limited viewing uses only unless otherwise authorized by Macrovision Corporation. Reverse engineering or disassembly is prohibited.

Apparatus Claims of U.S. Patent Nos. 4,631,603, 4,577,216, 4,819,098 and 4,907,093 licensed for limited viewing uses only.

Simultaneously published in the United States and Canada.

019-0793/7-20-2006

Contents

Chapter 1	4 About Using Smart Cards with Mac OS X
	4 Setting Up Your Computer
	5 Updating Your Computer's System Software
	5 Compatible Smart Card Readers
	5 Compatible Smart Cards
Chapter 2	6 Setting Up Your Smart Card
	6 Enabling Smart Card Login
	8 Setting Up an Account for Smart Card Access
	8 Setting Account Preferences
	8 Securing Your Idle Computer
	9 Using Keychain Access
	10 Setting Up Directory Services for Smart Cards
	10 Using the Public Key Hash Method
	11 Using the Attribute Lookup Method
	12 Modifying the Configuration File for Attribute Lookup
Chapter 3	14 Using Smart Cards
	14 Using a Smart Card to Log In
	14 Using Keychain Access to Manage Access
	15 Viewing Smart Card Information in Keychain Access
	15 Changing the PIN in Keychain Access
	15 Getting More Information About Smart Cards

About Using Smart Cards with Mac OS X

1

The security architecture in Mac OS X v10.4 Tiger and later includes improvements in smart card services and integration. Follow the instructions in this guide to configure your system to use smart cards.

A smart card is a plastic card, similar in size to a credit card, that has memory and a microprocessor embedded in it. Smart cards can store passwords, certificates, and keys. A smart card normally requires an additional security measure such as a personal identification number (PIN), or sometimes a biometric measurement (such as a fingerprint). A computer can retrieve information from a smart card through a smart card reader.

Smart card services have been expanded for Mac OS X Tiger. Smart card support is now integrated into the credential management of the security architecture. Smart card services are preinstalled with Mac OS X Tiger and later, and no longer require installation of smart card software. The setup process for smart cards is now simplified, and many of the steps required in previous versions are no longer needed.

Warning: The smart card software that is preinstalled with Mac OS X Tiger is not compatible with software or configuration settings created for previous versions of the Mac OS. Do not install smart card software or use files or configuration settings designed for earlier versions of Mac OS X. Doing so may corrupt the system software, and require that you reinstall Mac OS X.

Setting Up Your Computer

To use a smart card with your Macintosh, make sure you have:

- Mac OS X v10.4 Tiger or later
- A compatible smart card reader
- A compatible smart card

Updating Your Computer's System Software

Make sure you are using Mac OS X Tiger or later to take advantage of the latest smart card features.

- To identify which version you are using, choose Apple (🍏) menu > About This Mac.

You should update your system software regularly to be sure you have the most reliable and up-to-date software.

To update your system software:

- 1 Choose Apple (🍏) menu > Software Update.
- 2 If an update for Mac OS X appears in the list, select its checkbox.
- 3 Click Install, and then follow the onscreen instructions.

Compatible Smart Card Readers

Mac OS X Tiger includes built-in support for many types of smart card readers.

Compatible smart card readers include:

- Any certified Chip Card Interface Device (CCID) USB class reader
- USB readers such as Athena, CryptoCard, GemPlus, and SCM
- PC Card readers such as CryptoCard, SCM, and OmniKey
- USB dongle readers such as OmniKey and GemPlus

Other smart card readers can also be used if you install their software drivers, which are available from the manufacturer.

For more information about compatible smart card readers, visit the Apple Support website at www.apple.com/support.

Compatible Smart Cards

Mac OS X Tiger includes support for many types of smart cards.

Compatible smart cards include:

- U.S. Federal Government smart cards such as Common Access Card (CAC), Government Smart Card Interoperability Specification (GSCIS), and Personal ID Verification (PIV)
- Belgian Personal ID Card (BELPIC)
- Japanese PKI Card (JPKI)

Any supported smart card with signing capabilities can be used for both directory services–based authentication and cryptographic login.

For more information about supported smart cards, visit the Apple Support website at www.apple.com/support.

Follow the instructions in this chapter to learn how to enable smart card services and configure your computer to use smart cards.

Smart card services are preinstalled with Mac OS X v10.4 Tiger or later, but smart card login and system administration are not enabled. You can enable smart card login on any system with or without a smart card reader attached.

When the smart card services are enabled, your computer checks whether a smart card reader is attached. Enabling smart card login does not affect performance even if a card reader is not attached. If a card reader is not attached, you can continue to use your user name and password to log in.

Enabling Smart Card Login

To enable smart card login, you must edit the `/etc/authorization` file. To modify this file, you need an administrator password and you must be authorized to use the `sudo` command in Terminal to modify the system's configuration files. You must also be familiar with editing text files using a terminal text editor such as `pico`; a text editing application; or a property editor such as Property List Editor, which is included in the Apple Developer Kit.

Follow these steps to enable smart card login:

- 1 Open the Terminal application, located in the Utilities folder in the Applications folder.
- 2 To access the authorization files, enter the following command in Terminal:

```
sudo -s
```

- 3 To navigate to the correct directory, enter:

```
cd /etc
```

- 4 To delete the outdated `authorization.cac` file installed on your computer, enter:

```
rm authorization.cac
```

- 5 To back up the original authorization file and create a separate file to modify, enter:

```
cp authorization authorization.orig
cp authorization /tmp/authorization.mod
```

- 6 Open the authorization.mod file you just created in a text editor or property list editor. The file is located in the tmp folder on your startup drive:

```
/tmp/authorization.mod
```

- 7 The authorization.mod file is made up of a list of properties arranged in a hierarchy of dictionaries. At the root level of the property list is the `rights` dictionary, which contains a long list of other dictionaries.

Find the `system.login.console` dictionary in the `rights` dictionary. It contains an array called `mechanisms` that must be modified.

- 8 Make the following changes to the `mechanisms` array within the `system.login.console` dictionary:

- a Add `<string>builtin:smartcard-sniffer,privileged</string>` after the item `<string>builtin:auto-login,privileged</string>`.

- b Delete `<string>authinternal</string>`.

- c Add `<string>builtin:authenticate,privileged</string>` after the item `<string>builtin:reset-password,privileged</string>`.

- 9 At the root level of the property list is the `rules` dictionary.

Find the `authenticate` dictionary. It contains an array called `mechanisms` that must be modified.

- 10 Make the following changes to the `mechanisms` array within the `authenticate` dictionary.

- a Add `<string>builtin:smartcard-sniffer,privileged</string>` to the beginning of the `mechanisms` array.

- b Delete `<string>authinternal</string>`.

- c Add `<string>builtin:authenticate,privileged</string>` after the item `<string>builtin:authenticate</string>`.

- 11 Save your changes.

- 12 Your original session should still be running in Terminal. To replace the actual authorization file with the edited version, enter:

```
cp /tmp/authorization.mod /etc/authorization
```

The changes take place immediately; you don't need to restart the system.

After smart card login is enabled, the system starts checking whether a card reader is attached to the computer. Unlike with previous versions of smart card software, you do not need to enter additional commands for your computer to recognize the reader.

Setting Up an Account for Smart Card Access

You must have a user account to bind to the smart card, and then configure that account to work properly with the smart card. Follow these instructions to set up a user account for a smart card.

Setting Account Preferences

Use the Accounts preferences pane in System Preferences to create or configure the user account that will be bound to the smart card.

To create or configure a user account for a smart card:

- 1 Choose Apple () menu > System Preferences, and then click Accounts.
- 2 If some settings are dimmed, click the lock icon and then enter an administrator name and password.
- 3 Select the user account you want to change, or if you want to create a new user, click Add (+) and then enter the user's name and password in the Name, Password, and Verify fields.

If you don't want to use the automatically generated short name, enter a new short name. (After the account is created, you won't be able to change the short name).

- 4 If you want the user to have administrator privileges, click Password and select the option "Allow user to administer this computer."
- 5 Click Login Options.
- 6 Deselect the option "Automatically log in as."
- 7 Deselect the option "Show the Restart, Sleep, and Shut Down buttons."
- 8 Deselect the option "Enable fast user switching."
- 9 Close System Preferences.

Securing Your Idle Computer

If you want to be sure that the computer is secured when it is idle, you can require users to authenticate using the smart card and PIN when they wake the computer from sleep or return to the desktop from a screen saver.

To require user authentication:

- 1 Open System Preferences, and then click Security.
- 2 If some settings are dimmed, click the lock icon and then enter an administrator name and password.
- 3 Select the option "Require password to wake this computer from sleep or screen saver."
- 4 Close System Preferences.

Using Keychain Access

You must set up Keychain Access to work with your organization's policy. There are two common methods for verifying the validity of a certificate: Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL). Information about the status of certificates is stored on a revocation server. The Mac OS X security system can check with the revocation server to validate the certificate.

Here is an explanation of the settings available:

- **Off:** No revocation checking will be performed.
- **Best Attempt:** The certificate passes unless an indication of a bad certificate is returned from the server.
- **Require if Cert Indicates:** If the URL to the revocation server is provided in the certificate, this setting requires a successful connection to a revocation server and no indication of a bad certificate.
- **Require for All Certs:** This setting requires successful validation of all certificates. It is most useful in a tightly controlled environment that guarantees the presence of a CRL server or OCSP responder.
- **Priority:** Determines which method (OCSP or CRL) is attempted first. If the first method chosen returns a successful validation, the second method is not attempted.

Check with your network administrator for the settings required by your organization.

To set certificate validation in Keychain Access preferences:

- 1 Open Keychain Access, located in the Utilities folder in the Applications folder.
- 2 Choose Keychain Access menu > Preferences.
- 3 Click Certificates.
- 4 Choose settings from the Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) pop-up menus to match the requirements of your organization's policy. If there is no policy in place, it often works well to choose Best Attempt from the OCSP and CRL pop-up menus.

If you are a U.S. Federal Government Department of Defense user, you need to enable the X.509 Certificates in Keychain Access.

To install the X.509 Certificates in Keychain Access:

- 1 Open Keychain Access, located in the Utilities folder in the Applications folder.
- 2 Choose Edit menu > Keychain List.
- 3 Click Add (+), and then select X509Certificates located in /System/Library/Keychains/.
- 4 Click Open.

Setting Up Directory Services for Smart Cards

Smart card login does a lookup for the expected user in a directory service to authenticate the user's identification. It uses one of two methods:

- The public key hash method
Adds the public key hash (pubkeyhash) to the user's directory record. This method uses Open Directory and the default directory schema is NetInfo.
- The attribute lookup method
Performs a search for a value based on a key from the email signing certificate on the smart card. This method uses user accounts in an existing directory service. All U.S. Federal Government smart card users use the attribute lookup method.

Using the Public Key Hash Method

This is the most convenient and secure way of identifying a smart card user. It uses Open Directory. The default for the user record is a local NetInfo network. You will retrieve a key from the smart card, and then bind that key to the account.

After setting up the user account, you are ready to attach the smart card reader and read the card identity information.

To read the smart card identity information:

- 1 Attach the smart card reader to the computer.
- 2 Insert the smart card into the card reader.
- 3 Open the Terminal application, located in the Utilities folder in the Applications folder.
- 4 To read the identity keys, or hash, from the smart card, use the `sc_auth` command. You can enter the command in Terminal without any parameter to see a description of the command's usage displayed, for example:

```
$ sc_auth
Usage:  sc_auth accept[-v][-u user][-k keyname] #by key on inserted card(s)
        sc_auth accept[-v][-u user] -h hash #by known pubkey hash
        sc_auth remove[-v][-u user] #remove all public keys for this user
        sc_auth hash[-k keyname] #print hashes for keys on inserted card(s)
```

Enter the following command in Terminal:

```
sc_auth hash
```

Here is an example of the results:

```
$ sc_auth hash
01C2E294XP77B57B63B0A15B8F204C1 Identity Private Key
443F30C356E676F447CD4DCCED19737 Email Signing Private Key
4845564C1F8C6B372CE422933CF1FD1 Email Encryption Private Key
```

Not all cards have three private keys. In this example, any of the hash entries listed could be used for binding the card to the account. The following example uses the identity private key to bind the smart card to the user account.

- 5 You bind the card to the user's local directory domain by using the `sc_auth accept` command. Using the identity private key from the previous example, the command looks like this:

```
sudo sc_auth accept -u myuser -h 01C2E294XP77B57B63B0A15B8F204C1
```

In Terminal, enter the following command, using the account's short user name for `<username>` and the smart card's identity private key for `<# Identity Private Key>`:

```
sudo sc_auth accept -u <username> -h <# Identity Private Key>
```

The `sc_auth` command adds a field to the user's authentication called the `authentication_authority` property. You can see the `authentication_authority` property by using the `nidump` command. The following example shows the new identity private key written into the user public key hash.

```
nidump -r /users/myuser
...
"authentication_authority" = ( ";ShadowHash;", ";pubkeyhash
    01C2E294XP77B57B63B0A15B8F204C1" );
...
```

In the previous example with three hash keys, any of the key entries could have been used for binding the card to the account. More than one smart card can be bound to a single user account by running the script again with the hash for each additional card.

Note: Multiple cards can be bound to a single account, but a single card cannot be bound to multiple accounts accessible from a single system.

Using the Attribute Lookup Method

If your network doesn't use NetInfo with Open Directory, the attribute lookup method should be used to bind the user account to the smart card. This method looks up the user based on values drawn from the email signing certificate. Attribute lookup works with user accounts from an existing directory service such as LDAP, NetInfo, NIS, or Active Directory. You configure the smart card authorization plug-in to map an attribute from a certificate on the smart card to a field in the directory.

Attribute lookup is mainly used by Common Access Card (CAC) smart cards although it does work with other similarly designed smart cards. Attribute lookup is required for all U.S. Federal Government smart cards.

The examples show commonly used attribute lookups. However, you need to be familiar with the attributes and directory fields required by your particular directory service. Check with your network administrator for configuration information specific to your directory service.

Modifying the Configuration File for Attribute Lookup

In most directory services you will use a configuration file that contains a search key for an Open Directory search. A configuration file is an array of dictionaries. Each dictionary in this array contains one search key in an Open Directory search.

The default configuration file is:

```
/etc/cacloggingconfig.plist
```

The following example shows a common configuration:

```
<dict>
  <key>dsAttributeString</key>
    <string>dsAttrTypeNative:userPrincipalName</string>
  <key>fields</key>
    <array>
      <string>NT Principal Name</string>
    </array>
  <key>formatString</key>
    <string>${1}</string>
</dict>
```

The `dsAttrTypeNative: string` is followed by the `ntprincipalname` token, which represents the name of the attribute to use in your directory schema.

When an Open Directory search is performed on the `ntprincipalname` token, it returns is the ID. For example: `0123456789@mil`

Another example shows multiple strings formatted to return the ID:

```
<dict>
  <key>values</key>
    <array>
      <string>RFC 822 Name</string>
      <string>NT Principal Name</string>
      <string>Country</string>
    </array>
  <key>format</key>
    <string>${1}#${2}/${3}</string>
  <key>directorySearchKey</key>
    <string>dsAttrTypeNative:uniqueid</string>
</dict>
```

The `directorySearchKey` is the user's lookup key. It specifies the directory key to search for.

This example returns a combined search string:

```
smith@navy.mil#0123456789@mil/US
```

Here is an example of CAC keys that can appear as fields in the configuration file:

Key String	Example
Country	U.S.
Organization	U.S. Government
Organizational Unit:1	DoD
Organizational Unit:2	PKI
Organizational Unit:3	USN
Common Name	SURNAME.GIVEN.MI.1160048910
RFC 822 Name	gsurname@navy.mil
NT Principal Name	0123456789@mil

Follow the instructions in this chapter to learn how to use smart cards in Mac OS X v10.4 Tiger or later and how to manage authorization.

You can use smart cards to provide authentication for a number of applications and services in Mac OS X, including:

- Login
- Mail
- Safari
- Waking from sleep or screen saver
- VPN
- System administration
- Other applications that use CDSA or CDSA based APIs

Using a Smart Card to Log In

After the smart card login is enabled, the standard login screen appears.

To log in using your smart card:

- 1 Insert your smart card into the reader. The standard login screen is replaced by a smart card login screen asking for a PIN.
- 2 Enter your PIN number.

You are now able to access and use your computer normally.

Using Keychain Access to Manage Access

When a smart card is used to log in to a computer in Mac OS X Tiger, the smart card becomes a keychain in Keychain Access. Use Keychain Access to manage all of your keychains and passwords.

Viewing Smart Card Information in Keychain Access

Smart cards are displayed in Keychain Access as keychains in the Keychain list. With Keychain Access you can view and manage authorization information related to your smart card.

To view smart card information:

- 1 Open Keychain Access located in the Utilities folder in the Applications folder.
- 2 Select the smart card keychain in the Keychains list (click Show Keychains if the list is not open).

Changing the PIN in Keychain Access

You can use Keychain Access to change your smart card's PIN.

Warning: Check with your smart card administrator to be sure that you are allowed to change the PIN, and to confirm the required format of the PIN. The card or the card management system may require certain formats or types of characters, for example, only numeric or alpha-numeric characters.

To change the PIN used with your smart card:

- 1 Open Keychain Access located in the Utilities folder in the Applications folder, and then select the keychain in the Keychains list (click Show Keychains if the list is not open).
- 2 Choose Edit menu > "Change Password for Keychain 'smartcard# '." (The name of the keychain in the menu matches the name of the selected keychain).
- 3 If the keychain is locked, enter the password to unlock it.
- 4 Type the current password for the keychain.
- 5 Type a new password, and then type it again to verify it.
- 6 Click OK.

Getting More Information About Smart Cards

For more information about smart cards, visit these websites:

- Apple Support website at www.apple.com/support
- Apple Customer Training website at train.apple.com
- Apple Discussions website at discussions.info.apple.com
- Apple Product Security website at www.apple.com/support/security
- Apple Government website at www.apple.com/itpro/federal
- Apple Enterprise website at www.apple.com/itpro

For more information about security configurations, visit these websites:

- NSA security configuration guides at www.nsa.gov/snac/
- NIST Security Configuration Checklists Repository at checklists.nist.gov/repository/category.htm