Solaris Smartcard Administration Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 806–7010–10
May 2002

020115@3062

Contents

Preface

Solaris™ Smartcard enables a user to log in securely to the Solaris 8 or Solaris 9 desktop environment. A smart card is a plastic card that allows you to access a system by inserting a programmable card into a card reader. This guide explains how to configure systems and smart cards for this form of authentication. It also explains how to use a smart card after it has been configured.

Who Should Use This Book

The *Solaris Smartcard Administration Guide* is intended for the system administrator who sets up and administers the Solaris Smartcard environment. This guide assumes that you have a solid knowledge of authentication and related network security concepts.

If you are merely a user of a Solaris Smartcard, you do not need to read this book. Simply insert your smart card in your card reader and enter your personal identification number (PIN) when prompted to do so.

Related Books

Solaris Smartcard can be used in conjunction with any Solaris administration tools or Solaris commands and procedures. Refer to one or more of the following for additional information on Solaris installation or administration procedures:

- *(SPARC Platform Edition) Installation Guide*
- *System Administration Guide, Volume 1*

- *System Administration Guide, Volume 2*
- *System Administration Guide, Volume 3*
- Other software documentation that you received with your system

Accessing Sun Documentation Online

The docs.sun.com[SM] Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

Typographic Conventions

The following table describes the typographic changes used in this book.

TABLE P–1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type **`rm`** *filename*.
AaBbCc123	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in *User's Guide*. These are called *class* options. You must be *root* to do this.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

CHAPTER 1

Solaris Smartcard Overview

This chapter provides an overview of Solaris Smartcard features, supported smart cards and card readers, and planning information:

Smartcard Features

A Solaris Smartcard provides a somewhat more secure method for logging in to the Solaris desktop environment than is provided by the standard UNIX login. Information stored on the smart card verifies the identity of the user during login. A user who cannot provide the login information that is on the smart card is denied access to the desktop. The Solaris Smartcard software:

- Implements the Smartcard framework, which is based on the OCF1.1 standard
- Supports a variety of card readers
- Supports three widely-used smart cards
- Allows management from the Solaris Smartcard Console or the Solaris command line
- Protects login to the desktop environment through PIN authentication and provides a screen lock via `dtsession` when a smart card is removed from the card reader
- Lets a user store security credentials directly onto the card (Java cards only)

Smartcard Requirements

To use the Solaris Smartcard software, you need:

- A SPARC system running the Solaris 8 or Solaris 9 operating environment.
- A supported internal or external card reader and smart cards.

Solaris Smartcard supports the following smart cards and card readers.

- Payflex card
- iButton card
- Cyberflex card
- Sun SCRI External Serial Card Terminal Reader
- Sun SCRI Internal Card Terminal Reader
- iButton External Serial Card Terminal Reader

Smartcard Login

Secure desktop environments can be protected by requiring users to log in with a configured Solaris Smartcard. The following sequence explains what happens in the login process:

1. The `dtlogin` daemon prompts the user to insert a smart card and then to enter a personal identification number (PIN).
2. The `pam_smartcard` module compares the entered PIN with the PIN stored on the card.
3. If the typed PIN and PIN stored on the card match, the username and password are read from the card and used to authenticate the user, based on the specified search order for passwd in `/etc/nsswitch.conf`.

Package Descriptions

The following table lists the Solaris Smartcard packages added during a Solaris 9 installation.

TABLE 1–1 Solaris Smartcard Packages

Package Name	Description
SUNWjcom	Java Communications API for smart card support - Java code and Native code
SUNWjcomx	Java Communications API for smart card support - Native code (64–bit)
SUNWjib	Dallas Semiconductor serial iButton OCF Card Terminal Driver
SUNWocf	Open Card Framework - core libraries and utilities
SUNWocfr	Open Card Framework - configuration files
SUNWocfh	Open Card Framework - header files
SUNWocfx	Open Card Framework - core libraries (64–bit)
SUNWpamsc	Pluggable Authentication Module for smart card authentication
SUNWpamsx	Pluggable Authentication Module for smart card authentication (64–bit)
SUNWscgui	Solaris Smartcard Console
SUNWscmos	Smart OS used by SCM card terminal driver
SUNWscmsc	Sun SCRI OCF Card Terminal Driver

To remove a package, use the standard `pkgrm` command. Reinstall the package using the `pkgadd` command.

See "Managing Software (Tasks)" in *System Administration Guide: Basic Administration* for information on using these commands.

Smartcard Man Pages

Refer to the following man pages for detailed information about Smartcard commands:

- `ocfserv(1M)`
- `pam_smartcard(5)`
- `smartcard(1M)`

CHAPTER 2

Getting Started With Solaris Smartcard

This chapter shows an administrator how to set up an initial Solaris Smartcard configuration:

Starting or Restarting the Smartcard Console

The Smartcard Console is the graphical user interface (GUI) used to manage the Solaris Smartcard software.

▼ To Start the Smartcard Console from the Command Line

1. **Log in as root or `su` to root.**

Note – If you log in as a regular user, you can run Smartcard, but you can only perform two tasks: Load Applets and Configure Applets.

2. **Start the Smartcard Console:**

```
# /usr/dt/bin/sdtsmartcardadmin &
```

Note – Before you `su` to root you may need to disable X server access control, since root is not granted access by default. Disable X server access control by running `/usr/openwin/bin/xhost +`*hostname* where *hostname* is the local host. After starting the Smartcard Console, run `xhost -`*hostname* to enable access control again.

▼ To Start the Smartcard Console from the CDE Desktop

1. **Log in as root to the Common Desktop Environment (CDE).**

   If you are currently running CDE under your login name, exit CDE and log in as root.

Note – If you log in as a regular user, you can run Smartcard, but you can only perform two tasks: Load Applets and Configure Applets.

2. **On the CDE control panel, click the up arrow on the Applications subpanel.**

   By default, the Text Note icon, a pinned note with a pencil above it, represents the Applications subpanel.

3. **Select Applications to display the Application Manager.**

4. **Double-click the System_Admin icon in Application Manager.**

5. **Double-click the Smart Card icon to start the Smartcard Console.**

   You may have to scroll down to find the Smart Card icon.

Note – You can also start the Smartcard Console from the desktop Workspace menu; `sdtsmartcardadmin` should be found at the top level or in the Tools submenu.

Setting Up a Desktop for Smartcard Login

To set up Smartcard login for the desktop of a Sun workstation running the Solaris 8 or Solaris 9 operating environment, perform the tasks described below. For some tasks, a command line example is shown first, followed by Smartcard Console instructions. For complex tasks, the command line example is a link to a later chapter.

Note – You must be root to perform most of these tasks.

▼ To Activate a Card Reader

Note that even if your new workstation has an internal card reader, you must activate it before it can be used. If you are activating an external card reader, it must first be physically attached to a serial port of the system, according to instructions in the card reader documentation.

Command Line Example

See "Adding a Card Reader (Command Line)" on page 26 for examples.

Smartcard Console Instructions

1. **Click Card Readers in the Smartcard Console's Navigation pane.**

   The Add Reader icon is displayed in the Console pane. Icons for any enabled card reader types are also displayed.

2. **Double-click Add Reader in the Console pane.**

   The Add Reader dialog box is displayed.

3. **Double-click the type of card reader you want to add or select it and click OK.**

   To enable the Sun internal card reader, select Sun SCRI Internal Card Terminal Reader. The CardReaders dialog box is displayed.

4. **Select the Basic Configuration tab.**

5. **Type a name for the reader in the Unique Card Terminal Name field.**

   Leave the current name if you do not wish to change it. Do not include any spaces in the name.

6. **Click the down arrow under Device Port.**
7. **Select the port that the card reader is attached to.**
8. **Click OK.**
9. **Restart `ocfserv`, if prompted to do so.**

   The `ocfserv` process is restarted the next time you use the Smartcard Console or execute the `smartcard` command.

▼ To Add Support for a New Card Type (New ATR)

To use a new type of smart card, you have to provide its Answer to Reset (ATR) property to `ocfserv`. Do the following to add support for a new card type.

Command Line Example

As root, type the following to add "12345" as a new PayFlex ATR:

```
# smartcard -c admin -x modify "PayFlex.ATR=3B69000057100A9 3B6911000000010100 12345"
```

Note – You must enter the current ATRs *and* the new ATR.

Smartcard Console Instructions

1. **Insert the smart card with the new ATR in the card reader.**
2. **In the Navigation pane, select Smart Cards.**
3. **Double-click the icon representing the type of card currently inserted.**

   The Smart Card dialog box displays a list of the known ATRs for this card type.
4. **If this is a new ATR, click Add.**

   The Add ATR dialog box is displayed, with the ATR of the card inserted in the card reader shown in the "Inserted Card's ATR" listbox.

Note – To determine if the ATR value of the inserted card has been registered, click the Add button. If nothing is listed, your card's ATR is already known; otherwise you should perform the steps below.

---

5. **Select the ATR of the inserted card or type the new ATR in the New ATR field.**

You can find the new ATR value in the smart card product literature.

6. **Click OK in the Add ATR dialog box.**
   The new ATR is added to the list in the Smart Card dialog box.
7. **Select the new ATR in the list in the Smart Card dialog box.**
8. **Click OK in the Smart Card dialog box to activate the change.**

▼ To Load the Smartcard Applet to a Smart Card

Do the following to load the Solaris Smartcard applet (`SolarisAuthApplet`) to a smart card. You must do this before you can add the user profile information.

Command Line Example

As root, with the smart card inserted in the card reader, type the following:

```
# smartcard -c load -i /usr/share/lib/smartcard/SolarisAuthApplet.capx
```

When the load finishes, the following message displays:

```
Operation successful.
```

Smartcard Console Instructions

1. **Insert the smart card into the reader.**
2. **Select Load Applets icon in the Navigation pane.**
3. **Double-click the SolarisAuthApplet icon in the Console pane**
   The Load Applets dialog box is displayed. Available applets for various card types are displayed in the left listbox.
4. **Select the card type you want to initialize.**
   Choices include CyberFlex, IButton, and PayFlex.
5. **Click the arrow between the two listboxes.**
   The selected applet is copied to the Pending Applet Installations listbox, with a check in the checkbox and the name of the smart card displayed. If no card or the wrong smart card is inserted in the card reader, “No compatible devices inserted” is displayed. Insert the appropriate card.
6. **Click Install.**
   A window labeled “Loading Applet to Device” is displayed. It takes a minute or so for the applet to load. When the installation is complete, a window with a confirmation message (“Applet Installation Successful”) displays.

7. **Click OK to dismiss the confirmation window.**

   The card now stores default values. If the card previously stored different PIN or user profile values, those values have been overwritten. See "PIN Property" on page 33 and "User and Password Properties" on page 33 for more information.

▼ To Set Up a User Profile

Do the following to specify the username and password associated with the application(`dtlogin`) for the card being set up. For more information, see "To Create User Information on a Smart Card" on page 32.

Command Line Example

As root, type the following on one line to set the user name to `xxx` and the password to `yyy` for the `dtlogin` application. In this example, the PIN is `$$$$java`, the default value:

```
# smartcard -c init -A A0000000620304000 -P '$$$$java' user=xxx
password=yyy application=dtlogin
```

Note – You must enter the loaded applet ID and the current PIN. In the example above, `-A A000000062030400` specifies the `SolarisAuthApplet` applet ID and the PIN is the default `SolarisAuthApplet` value. Enclose the PIN, `$$$$java`, or any PIN containing shell special-characters (such as `$`) within single quotes. Otherwise, the shell tries to interpret the PIN as a variable, and the command fails.

Smartcard Console Instructions

1. **Insert the smart card you want to configure into the card reader.**
2. **Select Configure Applets in the Navigation pane.**

   The icon for the type of card in the reader is displayed in the Console pane.
3. **Double-click the icon in the Console pane.**

   The Configure Applets dialog box is displayed.
4. **Select `SolarisAuthApplet` in the Configure Applets dialog box.**

   The `SolarisAuthApplet` configuration folders appear on the right side of the dialog box, represented by tabs labeled PIN and User Profiles (plus RSA Key and PKI Cert, for some smart cards). Only User Profiles changes are described here. See "To Change the PIN on a Card" on page 20 for PIN change information.
5. **Select the User Profiles tab in the Configure Applets dialog box.**

6. **Type `dtlogin` in the User Profile Name field.**

   This represents the CDE desktop.

7. **Type a user name in User Name field.**

   This is the username of the person who will be using the card. The username cannot be more than eight characters long.

   Note – Click Get to determine the current username associated with the card. You will need to enter the PIN to get the current username or to change the username or password.

   ---

8. **Type password in Password field.**

   This is the password associated with the username typed above. The password must correspond to the user's password based on the search order for `passwd` in `/etc/nsswitch.conf` (LDAP, NIS, NIS+, or local files). The password cannot be more than eight characters long.

   Note – If the user's password is changed after you have configured the smart card, you or the user must repeat these steps to store the new password on the smart card. It is not updated automatically.

   ---

9. **Click Set.**

   The Set User Profile popup is displayed, asking for the current PIN.

10. **Type the PIN and click OK.**

    The new username and password are stored on the card.

11. **Click OK to dismiss the dialog box.**

▼ To Verify a PIN for a Smart Card

Do the following to verify the PIN for a smart card.

1. **Insert the smart card into the card reader.**

2. **As root, type the following to verify the PIN for the smart card.**

   ```
   # smartcard -c init -A A000000062030400 -P 'PIN_number'
   ```

   where *PIN_number* represents the PIN set for the card and `A000000062030400` is the applet ID for the `SolarisAuthApplet`.

   If the PIN is invalid, an `Invalid PIN` message is displayed. A valid PIN results in no output.

▼ To Change the PIN on a Card

Do the following to change the PIN on a smart card.

Note – This is a task that can be performed by an end user, if he or she knows the current PIN.

Command Line Example

As root, with the smart card inserted in the card reader, type the following to change the default PIN (`$$$$java`) to `001234`:

```
# smartcard -c init -A A000000062030400 -P '$$$$java' pin=001234
```

Note – You must enter the loaded applet ID and the current PIN. In the example above, `-A A000000062030400` specifies the `SolarisAuthApplet` applet ID (aid) and the PIN is the default `SolarisAuthApplet` value. Be sure to type the new PIN correctly because you will not be prompted to confirm it. Enclose the PIN, `$$$$java`, or any PIN containing shell special-characters (such as `$`) within single quotes. Otherwise, the shell tries to interpret the PIN as a variable, and the command fails.

Smartcard Console Instructions

1. **Insert the smart card you want to configure into the card reader.**
2. **Select Configure Applets in the Navigation pane.**
   The icon for the type of card in the reader is displayed in the Console pane.
3. **Double-click the card icon in the Console pane.**
   The Configure Applets dialog box is displayed.
4. **Select `SolarisAuthApplet` in the listbox.**
   The `SolarisAuthApplet` configuration folders appear on the right side of the dialog box, represented by tabs labeled PIN and User Profiles (plus RSA Key and PKI Cert, for some smart cards). Only PIN change is described here.
5. **Select the PIN tab.**
6. **Type and retype a new PIN.**
   A PIN can contain up to eight characters.
7. **Click Change.**
   A popup window labeled “Change PIN” is displayed.

8. **Enter the previous PIN in the pop-up window and click OK.**

   The default PIN, loaded on the card when the `SolarisAuthApplet` was installed on the card, is `$$$$java`.

▼ To Enable Smartcard on a System

Do the following to enable Solaris Smartcard on a system. This must be done on each system that will use Smartcard authentication. See `smartcard(1M)`, `pam_smartcard(5)`, and `ocfserv(1M)` for detailed information about Solaris Smartcard commands.

Command Line Example

See "To Enable Smartcard Usage (Command Line)" on page 35 for instructions.

Smartcard Console Instructions

1. **Select OCF Clients in the Navigation pane.**

   The Desktop icon is displayed in the Console pane.

2. **Double-click the Desktop icon.**

   The Configure Clients dialog box is displayed.

3. **Select the Cards/Authentications tab in the dialog box.**

   The three supported smart cards — CyberFlex, IButton, and PayFlex — are listed in the listbox at the left.

4. **Select the radio button labeled "Activate Desktop's Smart Card capabilities."**

Note – As soon as you click OK in the Configure Clients dialog box, Smartcard is activated. Be sure you have a working card reader on the system and a smart card configured with your username and password. And be sure you know the PIN on the card or you will be locked out of the system. If you cannot access your system because of Smartcard, `rlogin` to the system and disable Smartcard by typing, as superuser: `smartcard -c disable`. You can disable Smartcard from the Configure Clients dialog box by selecting the radio button labeled "Deactivate Desktop's Smart Card Capabilities" and clicking OK.

---

5. **Click Apply or OK.**

   Solaris Smartcard is now enabled on the system.

6. **Exit CDE to activate the change.**

Other Setup Tasks

If you don't want to use the default values for Smartcard timeouts and card removal actions, you can change them, as described below.

▼ To Set Smartcard Timeouts (Console)

1. **Select OCF Clients in the Navigation pane.**
2. **Double-click the Desktops icon in the Console pane.**
   The Configure Clients dialog box is displayed.
3. **Select the Timeouts tab in the dialog box.**
4. **Adjust the timeouts by sliding the indicator for each timeout with the mouse.**
   - Card Removal timeout – specifies the number of seconds the desktop waits after a smart card is removed before locking the screen; this only applies when the "Ignore Card Removal" box is *not* checked under the options tab. If Card Removal Logout Wait is set to 0, a user will never be logged out (that is, the screen remains locked until the user reauthenticates to unlock it).
   - Reauthentication timeout – specifies the number of seconds the Reauthentication screen is displayed when the card has been removed and the screen is locked.
   - Card Removal Logout Wait – specifies the number of seconds the desktop waits for a smart card to be reinserted when the Reauthentication screen is displayed. If the card is not reinserted in time, the user is logged out. Note that this timeout is relevant only when Reauthenticate After Card Removal (in the Options tab) is set to False.
5. **Click Apply or OK.**
6. **Exit CDE to activate the change.**

▼ To Set Card Removal Options (Console)

1. **Select OCF Clients in the Navigation pane.**
2. **Double-click the Desktops icon in the Console pane.**
   The Configure Clients dialog box is displayed.
3. **Select the Options tab in the dialog box.**
4. **Click the checkboxes to toggle them.**

- Ignore Card Removal – if checked, nothing happens when a smart card is removed from the reader.
- Reauthenticate After Card Removal – If checked, a user is logged out when a card is removed. If it is not checked, the Card Removal Logout Wait setting (in the Timeouts tab) determines what happens.

5. **Click Apply or OK.**
6. **Exit CDE to activate the change.**

CHAPTER 3

Card Readers

This chapter describes the procedures for setting up and maintaining card readers of various types:

Supported Card Readers

Solaris Smartcard supports two external card readers, the iButton and the Sun SCRI External Reader 1, and an internal card reader, the Sun SCRI Internal Card Reader 1.

The following table shows the supported card readers and the corresponding values you need to supply to add them.

TABLE 3–1 Card Readers Supported

Reader Type	Card Terminal Factory Name	Reader Model Name
Sun SCRI External Card Reader 1	`com.sun.opencard.terminal.scm.SCMStc.SCMStcCardTerminalFactory`	`SunSCRI`
iButton	`com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory`	`DS1402`
Sun SCRI Internal Card Reader 1	`com.sun.opencard.terminal.scm.SCMI2c.SCMI2cCardTerminalFactory`	`SunISCRI`

Adding a Card Reader (Command Line)

You add a card reader by using the `smartcard -c admin` command with the following syntax:

`smartcard -c admin -t terminal -j` *card_terminal_factory_name* `-x add -d` *device_pathname* `-r` *user_friendly_reader_name* `-n` *card_reader_model*

`-c admin`	Indicates that you are viewing or modifying OCF properties.
`-t terminal`	Indicates that you are about to configure a card reader.
`-j` *card_terminal_factory_name*	Defines the card terminal factory name of the card reader type. See the specific Card Terminal Factory Name in the procedures below.
`-x add`	Indicates that you want to add a card reader.
`-d` *device_pathname*	Specifies the device port where you have plugged in the card reader.
`-r` *user_friendly_reader_name*	Specifies a unique name for the reader.
`-n` *reader_model_name*	Designates the model name of the card reader. See the specific card reader model name in the procedures below.

Refer to the `smartcard`(1M) man page for more information.

▼ To Add an iButton Reader

1. **Attach the external card reader to the system.**

   Physically attach the external smart card reader to the serial port, following instructions in the card reader documentation.

2. **Become superuser on the system where you are attaching the card reader.**

3. **Add the iButton reader by typing, for example, the following on one line:**

```
# smartcard -c admin -t terminal
-j com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory
-x add -d /dev/cua/b -r MyButtonReader -n DS1402
```

`-c admin`	Indicates that you are viewing or modifying OCF properties.

`-t terminal`	Indicates you are configuring a card reader.
`-j com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory`	Identifies the card terminal factory name of the iButton reader. Be careful to type the card terminal factory name following `-j` option exactly as shown in the procedure above, with no spaces or returns between characters.
`-x add`	Indicates that you want to add a card reader.
`-d /dev/scmi2c0`	Defines the device port where the card reader is attached.
`-r` *MyButtonReader*	Specifies a unique name for the iButton reader.
`-n DS1402`	Indicates the model name for the iButton card reader.

4. **Stop** `ocfserv`**.**

```
# pkill ocfserv
```

The `ocfserv` process is restarted the next time you use the Smartcard Console or the `smartcard` command.

▼ To Add a Sun SCRI External Card Reader 1

1. **Attach the external card reader to the system.**

   Physically attach the external smart card reader to the serial port, following instructions in the card reader documentation.

2. **Become superuser on the system where you are attaching the card reader.**

3. **Add the Sun SCRI External Card Reader 1 by typing, for example, the following command on one line:**

```
# smartcard -c admin -t terminal
-j com.sun.opencard.terminal.scm.SCMStc.SCMStcCardTerminalFactory
-x add -d /dev/cua/b -r MyExternalReader -n SunSCRI
```

`-c admin`	Indicates that you are viewing or modifying OCF properties.
`-t terminal`	Indicates you are configuring a card reader.

`-j`
 	
`com.sun.opencard.terminal`
`.scm.SCMStc.SCMStcCard`
`TerminalFactory`
	The card terminal factory name of the Sun SCRI External Card Reader 1.
	
	Be careful to type the card terminal factory name following `-j` option exactly as shown in the procedure above, with no spaces or returns between characters.

`-x add`	Indicates that you want to add a card reader.
`-d /dev/scmi2c0`	Defines the device port where the card reader is attached.
`-r` *MyExternalReader*	Specifies a unique name for the SCRI External Card Reader 1.
`-n SunSCRI`	Indicates the model name for the SCRI External Card Reader 1.

4. **Stop** `ocfserv`**.**

   ```
   # pkill ocfserv
   ```

   The `ocfserv` process is restarted the next time you use the Smartcard Console or execute the `smartcard` command.

▼ To Add a Sun SCRI Internal Card Reader 1

1. **Become superuser on the system where you are attaching the card reader.**
2. **Add the Sun SCRI Internal Card Reader 1 by typing, for example, the following command on one line:**

   ```
   # smartcard -c admin -t terminal
   -j com.sun.opencard.terminal.scm.SCMI2c.SCMI2cCardTerminalFactory
   -x add -d /dev/scmi2c1 -r MyInternalReader -n SunISCRI
   ```

`-c admin`	Indicates that you are viewing or modifying OCF properties.
`-t terminal`	Indicates you are configuring a card reader.

`-j`
`com.sun.opencard.terminal.`
`scm.SCMI2c.SCMI2cCard`
`TerminalFactory`
	The card terminal factory name of the Sun SCRI Internal Card Reader 1.
	
	Be careful to type the card terminal factory name following `-j` option exactly as shown in the procedure above, with no spaces or returns between characters.

`-x add`	Indicates that you want to add a card reader.

`-d /dev/scmi2c0`	Defines the device port where the card reader is attached. For example, `/dev/scmi2c`*n*, where *n* in `scmi2c`*n* is the *n*the SunISCRI reader on the system.
`-r` *MyInternalReader*	Specifies a unique name for the SCRI Internal Card Reader 1.
`-n SunISCRI`	Indicates the model name for the SCRI Internal Card Reader 1.

3. **Stop** `ocfserv`**.**

   ```
   # pkill ocfserv
   ```

   The `ocfserv` process is restarted the next time you use the Smartcard Console or execute the `smartcard` command.

Removing a Card Reader

You might need to remove an external card reader from a system when a user no longer needs to use a smart card, or when you want to move the card reader to another system. Be sure to remove the card reader logically before you disconnect the physical device.

▼ To Remove a Card Reader (Console)

1. **Click Card Readers in the Navigation pane.**
2. **Select the card reader in the Console pane that you want to remove.**
3. **Select Remove Terminal from the Action menu.**
4. **Click OK to remove the card reader.**
5. **Restart** `ocfserv`**, if prompted.**

   The `ocfserv` process is restarted the next time you use the Smartcard Console or execute the `smartcard` command.

▼ To Remove a Card Reader (Command Line)

1. **Become superuser on the system with the card reader to be removed.**
2. **Remove the card reader.**

   ```
   # smartcard -c admin -t terminal -r user_friendly_reader_name -x delete
   ```

3. **(Optional) Unplug the external card reader from the port.**

4. **Stop** `ocfserv`**.**

   ```
   # pkill ocfserv
   ```

   The `ocfserv` process is restarted the next time you use the Smartcard Console or execute the `smartcard` command.

CHAPTER 4

Setting Up a Smart Card

This chapter provides an overview of setting up a smart card. You can set up a smart card from the Smartcard Console or the command line. The tasks in this chapter assume that you have identified how you will implement smart cards at your site and that you have set up a card reader on all systems that will use smart cards. The following subjects are included:

Loading the `SolarisAuthApplet`

You must add the default `SolarisAuthApplet` applet to the card before you can add the user profile information. See "To Load the Smartcard Applet to a Smart Card" on page 17 for instructions.

Initializing a Smart Card

After the default applet (`SolarisAuthApplet`) has been loaded, create the user profile information on the card. The user profile information specifies a login name and password for the card user, and names the protected application. The default PIN for the `SolarisAuthApplet` is `$$$$java`.

▼ To Create User Information on a Smart Card

Example—Creating User Information on a Smart Card (Command Line)

This command is appropriate for all smart cards devices supported by Solaris Smartcard. Insert the card in the card reader. For Smartcard Console instructions, see "To Set Up a User Profile" on page 18 and "To Change the PIN on a Card" on page 20.

Set the login name, password, and application for the card by typing the following on one line:

```
# smartcard -c init -A A000000062030400 -P '$$$$java' user=anyone
password=changeme application=dtlogin
```

In the example, the username is set to `anyone`, the password to `changeme`, and the application is `dtlogin`. The username and password can be set to any value; these will be changed by a system administrator or the user when the card is issued. See "To Set Up a User Profile" on page 18 for instructions.

Note – You must enter the loaded applet ID and the current PIN. The `-A A000000062030400` part of the command specifies the `SolarisAuthApplet` applet ID. You must enclose the default PIN, `$$$$java`, or any PIN containing shell special-characters (such as `$`) within single quotes. Otherwise, the shell tries to interpret the PIN as a variable, and the command fails.

Defining Authentication Properties on a Smart Card

You set the properties on each smart card based on the user's requirements, your site's security policies, and the limitations of the type of smart card used. Using the Configure Applets dialog box, define corresponding properties for each smart card. The client and server programs on the system read the properties on the smart card to determine whether to give the user access to a particular application.

Note – These properties apply only to cards initialized with the `SolarisAuthApplet` applet provided with Solaris Smartcard. If your site uses a different smart card applet, the available properties might differ. Refer to the `smartcard(1M)` man page for more information.

PIN Property

The PIN property is an authentication property that defines a personal identification number (PIN) for the card. The default PIN created on the card is `$$$$java`. Either you or the user can change `$$$$java` to a personalized PIN. Consider giving all users at your site the same default PIN name (for example, `changeme`). Then make sure each user changes the PIN to a value known only to that user.

See "To Change the PIN on a Card" on page 20 for step-by-step instructions on changing the PIN on a smart card.

User and Password Properties

The user and password properties are authentication properties that identify the user and associate the user with the smart card's PIN. To set these properties, you must know the user's login name and password.

On systems using the default authentication mechanism of PIN, `ocfserv` verifies the authenticity of the PIN. Next, `ocfserv` reads the user and password properties on the card. If the password on the smart card matches the user's entry in the system's password database, `ocfserv` gives the user access to the application.

Application Property

Use the application authentication property (called a "user profile" in the Smartcard Console) to designate which applications the user needs to log in to with a login name and password. For example, to require a smart card login to the desktop, you must specify `dtlogin` as the application associated with the login name and password on the card. You can also require a smart card login for an application specific to your site, such as a financial package or personnel database, by specifying its name as the application property.

Before initializing an application on the card, find out which applications a user needs to access through smart card authentication. This step is particularly important when preparing a smart card for a system administrator or other user who might need to log in to an application as root or another restricted login name.

Note – Payflex cards do not support multiple profiles; they cannot be used in cases where a user needs to log in to the desktop and one or more secure applications or uses multiple user names.

The application property on the smart card works in tandem with the other authentication properties. For example, suppose you initialized a smart card for user Frank with the following information:

- `A000000062030400` – The `SolarisAuthApplet` applet.
- `'$$$$java'` – The default PIN for this card, which user Frank can change later.
- `dtlogin` – The application requiring the smart card login.
- `frank` – The name that Frank must provide to log in to the desktop.
- `changeme` - The password that Frank must type to log in to the desktop.

The preceding information would be entered on the command line, as follows:

```
# smartcard -c init -A A000000062030400 -P '$$$$java' application=dtlogin
user=frank password=changeme
```

When Frank inserts his card into the reader and tries to log in to the desktop (`dtlogin`), `ocfserv` reads the card to determine whether any authentication properties are associated with `dtlogin`. The `ocfserv` server finds that the user and password properties are associated with `dtlogin`.

The `ocfserv` server prompts Frank for his PIN, and the typed PIN is compared with the PIN stored on the smart card assigned to the `dtlogin` application. Also, `ocfserv` uses the login name and password on Frank's card, along with the passwords in the system's password database, to verify that Frank is who he claims to be. If these properties match, Frank is logged in to the desktop.

Enabling Solaris Smartcard Desktop Login

The final step in setting up a desktop system is to enable desktop login using Solaris Smartcard. See "To Enable Smartcard Usage (Command Line)" on page 35 for step-by-step instructions.

You cannot log in through `dtlogin` if you enable Smartcard and either of the following conditions is true:

- You do not have a working smart card, or

- You have not configured a smart card successfully

If you enable Smartcard before you have set up a working smart card configuration, do the following to disable Smartcard so that you can set up Smartcard for use:

1. Log in in to the system remotely with the `ssh` or `rlogin` command.
2. Become superuser (root).
3. Disable smart card operations.

```
# smartcard -c disable
```

▼ To Enable Smartcard Usage (Command Line)

Do the following to enable Solaris Smartcard usage on a system. A user must use an accepted smart card for the system and might need to type a PIN to successfully log in to this system after the desktop is enabled for Smartcard.

1. **Become superuser on each system to be used in Smartcard operations.**
2. **Stop the desktop.**

```
# /etc/init.d/dtlogin stop
```

3. **Turn on Solaris Smartcard operations.**

```
# smartcard -c enable
```

4. **Restart the desktop.**

```
# /etc/init.d/dtlogin start
```

Note – When CDE is configured for Smartcard login, `/etc/pam.conf` is modified to include `pam_smartcard`. For example, when `smartcard -c enable` is executed, the following lines are inserted at the top of the `auth` stacks for `dtlogin` and `dtsession`:

```
dtlogin auth requisite pam_smartcard.so
dtsession auth requisite pam_smartcard.so
```

CHAPTER 5

Troubleshooting

This section explains how to solve Solaris Smartcard problems. The following sections are included:

You can debug smart card operations on a system by setting the debugging properties. Solaris Smartcard offers standard debugging and a detailed trace of your operations, if specified. If enabled, debugging information is logged to a file. You can control the level and amount of debugging information on 0–9 scale. Debugging is disabled by default.

The following debugging properties are defined for `ocfserv` by default:

```
debugging.filename        = /var/run/ocf.log
debugging                 = 0
OpenCard.trace            = com.sun:9 opencard.core:9
```

Note – If you are running a previous Solaris 8 release, the debugging log file might be called `/tmp/ocf_debugfile`.

`/var/run/ocf_log`	The name of the file to contain debugging information.
`debugging = 0`	Means that debugging is disabled. Debugging is enabled if `debugging = 1`.

`OpenCard.trace`	The OpenCard trace level.

To Enable Debugging (Console)

Use the Debug folder if you want to set up the `ocfserv` debugging property. Setting up debugging is optional.

1. **Select OCF Server from the Navigation pane.**
2. **Double-click the icon representing the local system.**
3. **Select the Debug folder.**
4. **Slide the indicator for the OCF Debug Level slider to the right to indicate the level of debugging you want on the OCF Server.**
5. **Slide the indicator for the Open Card Trace Level slider to the right to indicate the trace level you want on the OCF Server.**
6. **(Optional) Specify an alternate name for the debug file.**
   a. **Click Browse to view the file systems on the system.**
   b. **Type the fully qualified path name for the debug file in the OCF Debug File Location field.**
7. **Click Apply or OK.**

To Enable Debugging (Command Line)

Use the following procedure to enable smart card debugging.

1. **Become superuser.**
2. **Enable smart card debugging by setting** `debugging=1`**.**

```
# smartcard -c admin -x modify debugging=1
```

In the following example, the location of the `ocfserv` debugging file is changed by specifying the `-x modify debugging.filename` option and a fully qualified file name for the debugging file.

```
# smartcard -c admin -x modify debugging.filename=/var/tmp/sc.debug
```

To Disable Smartcard

You might need to disable Smartcard on a system if a Smartcard setup problem does not allow a user to log in with a smart card, or if a system no longer needs a smart card login.

1. **Become superuser.**
2. **Disable smart card operations.**

```
# smartcard -c disable
```

To Resolve Smart Card Login Problems

After you have enabled Smartcard and logged off from a system, the CDE login screen displays the following prompt:

```
Please insert Smart Card
```

If you are unable to log into a system using a smart card because of Smartcard setup problems, try the following:

1. **Log in to the system remotely with the** `rlogin` **or** `telnet` **command.**
2. `su` **to root.**
3. **Disable Smartcard:**

```
# smartcard -c disable
```

After Smartcard is disabled, the CDE screen displays the following prompt:

```
Enter User Name
```

4. **Correct the Smartcard setup problem.**

To Resolve Configuration Problems

The `/etc/smartcard/opencard.properties` file stores important smart card configuration information. This file requires no administration and should not be edited manually. However, if you inadvertently introduced a problem in your smart card configuration by using either the Smartcard Console or the command line, you can restore the previous version of the `/etc/smartcard/opencard.properties` file from the command line.

1. **Become superuser.**
2. **Change to the `/etc/smartcard` directory.**
3. **Save the current version first.**

   ```
   #  cp opencard.properties opencard.properties.bad
   ```

4. **Copy the previous version to the current version.**

   ```
   # cp opencard.properties.bak opencard.properties
   ```

To Resolve Applet Downloading Problems

1. **If you see the following message while trying to download the applet on the card, it is possible that you have not added the ATR of the smart card inserted in the reader to the list of valid ATRs the system can accept.**

   ```
   SmartcardInvalidCardException
   ```

2. **Try updating the card's ATR by following the procedure in "To Add Support for a New Card Type (New ATR)" on page 16.**

To Add a Missing ATR

When you try to add a smart card in the Smartcard Console, a screen displays the ATR of the card inserted in the reader. If the ATR displayed does not exist in the list of valid ATRs, add the ATR to the *card-name*`.ATR` property.

See “To Add Support for a New Card Type (New ATR)” on page 16 for more information. See command-line example below.

Example—Adding a Missing ATR (Command Line)

Display `ocfserv` properties to see if the *card_name*.ATR property exists.

```
# smartcard -c admin
```

For example, `ocfserv` lists a property `MySCM.0.ATR`, where `MySCM` is the user-friendly name of the card reader. This property reflects the ATR of the smart card inserted in the reader. This property is temporary and is added by `ocfserv` only for the time the card is in the reader. This property is removed when the card is removed.

Add this ATR to the *card_name*.ATR property if the ATR displayed by this property does not exist in the list of valid ATRs.

Glossary

Answer to Reset	A property assigned to each smart card type by the manufacturer that identifies the version of the smart card. An equivalent property is stored on the system to assist in authentication. Abbreviated ATR.
ATR	See Answer to Reset.
authentication	The process of verifying a user's identity.
CDE	See Common Desktop Environment.
challenge-response	A form of authentication whereby the smart card is loaded with a DES key used in response to a random number generated by the system and sent to the card when the card is inserted in the card reader.
Common Desktop Environment	A desktop application used in the Solaris operating environment. Abbreviated CDE.
Console pane	The pane in the Smartcard Console that contains icons for various management tasks.
Information pane	The pane in the Smartcard Console that contains a brief description of the category or icon just clicked, as well as instructions for beginning the task associated with that category or icon.
Navigation pane	The pane in the Smartcard Console that lists major categories of tasks involved in setting up smart cards.
personal identification number	A unique number used to identify a user. Abbreviated PIN.
PIN	See personal identification number.
private key	A type of security that works in a public-key infrastructure, involving pairs of key strings. The private key part of this pair is stored on the smart card.
Solaris Smartcard	Name of the software that enables the use of smart cards in a Solaris operating environment.

smart card	A plastic card that has been initialized in such a way as to allow the user to access a system by inserting the card into a card reader.
Smartcard Console	The GUI tool that enables an administrator to manage Solaris Smartcard.
symmetric key	Another term for the DES key described in challenge-response authentication method.

Index

D

E

F

G

R

S

T

U

W

X