HP Praesidium SpeedCard Getting Started Guide

For HP-UX 10.20, 11.0 and 11i

Fifth Edition

HP 9000 Networking

**HEWLETT®
PACKARD**

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Year 2000 Compliance Warranty. Manufacturer warrants that all HP Products will be "Year 2000 Compliant." Year 2000 Compliant products will perform without error, loss of data, or loss of functionality on account of any inability to process, calculate, compare or sequence date data accurately. In addition, Year 2000 Compliant products will not cause any associated HP products or any systems in which they may be used to fail in any of the ways described above. This Year 2000 Compliance warranty will remain in effect through December 31, 2000, notwithstanding any other warranty period specified in this Agreement.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY 3000 Hanover Street Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

The printing history for the *HP Praesidium SpeedCard Getting Started Guide* is listed below.

First Edition: June 1999 (HP-UX Release 10.20, 11.0)

Second Edition: September 1999 (HP-UX Release 10.20, 11.0)

Third Edition: December 1999 (HP-UX Release 10.20, 11.0)

Fourth Edition: June 2000 (HP-UX Release 10.20, 11.0)

Fifth Edition: December 2000 (HP-UX 11i Release)

Contents

Contents

4. Using the SpeedCard

5. Appendix

1 Safety and Regulatory Information

Regulatory Information

This product was tested for conformance to various national and international regulations and standards. The scope of this regulatory testing includes electrical and mechanical safety, electromagnetic emissions and immunity.

When required, approvals are obtained from third party test agencies. Approval marks appear on the product label. In addition, various regulatory bodies require some information under the headings noted below.
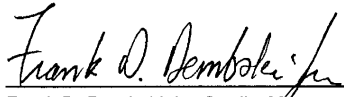
FCC Statement (USA only)

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class A digital device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by Hewlett-Packard could void the user's authority to operate this equipment.

DECLARATION OF CONFORMITY
According to ISO/IEC Guide 22 and EN 45014

Manufacturer's Name: Hewlett-Packard Company
Systems Interconnect Solutions Lab

Manufacturer's Address: 8000 Foothills Blvd.
Roseville, CA 95747
USA

declares, that the product

Product Name: HP Praesidium PKC Accelerator Card

Model Number(s): A5486-60001 (Prod. No. A5486A)

Product Options: All

conforms to the following Product Specifications:

Safety: IEC 950:1991 + A1, A2, A3, A4 / EN 60950:1992 + A1, A2, A3, A4, A11
GB 4943-1995

EMC: CISPR 22:1993 / EN 55022:1994 + A1+A2 - Class A[1]
GB 9254-1988
EN 50082-1:1992, Generic Immunity, including:
IEC 801-2:1991 / prEN 55024-2:1992, 4 kV CD, 8 kV AD
IEC 801-3:1984 / prEN 55024-3:1991, 3 V/m
IEC 801-4:1988 / prEN 55024-4:1993, Signal Lines, not applicable
1 kV Power Line
IEC 1000-3-2:1995 / EN 61000-3-2:1995, not applicable
IEC 1000-3-3:1994 / EN 61000-3-3:1995, not applicable

Supplementary Information:

The product herewith complies with the requirements of the Low Voltage Directive
73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly.

1) The Product was tested in a typical configuration with Hewlett-Packard information
technology equipment.

Roseville, CA, July 26, 1999   Frank D. Dembski Jr., Quality Manager

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH,
Department HQ-TRE, Herrenberger Straße 130, D-71034 Böblingen (FAX: + 49-7031-14-3143)

Declaration of Conformity Statement

Declaration Of Conformity Statement (Canada only)

This Class A digital apparatus meets all the requirements of the
Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du
Règlement sur le matériel brouilleur du Canada.

Europe RFI Statement

This is a Class A product. In a domestic environment, this product may
cause radio interference, in which case the user may be required to take
adequate measures.

Australia and New Zealand EMI Statement

This product meets the applicable requirements of the Australia and
New Zealand EMC Framework.

N279

Safety Information

These products comply with IEC 950/EN 60950; Printed Circuit Board is rated 94V-0.

Safety Symbols

WARNING   **A WARNING denotes a hazard that can cause personal injury.**

CAUTION   A CAUTION denotes a hazard that can damage equipment.

2   Introduction

Overview

Thank you for choosing the HP Praesidium SpeedCard for HP-UX Internet web servers. The SpeedCard is a hardware- based security solution that plugs into your server's bus and enables your server's CPU to sustain maximum performance. This product is a member of the HP Praesidium family of security products. For more information about HP's Praesidium products, please refer to the HP Praesidium website at:

```
http://www.hp.com/praesidium.html
```

Who Should Read this Guide?

This guide is intended for anyone who needs to install and/or use the HP Praesidium SpeedCard in an HP-UX system.

What this Guide Contains

This guide contains information to assist you in installing and setting up your SpeedCard.

Table 2-1   **Contents by chapter**

CHAPTER/APPENDIX	DESCRIPTION
Chapter 1 - Introduction	Gives an overview of the HP Praesidium SpeedCard.
Chapter 2 - Installation Issues	Provides information that is important to know when installing a SpeedCard.
Chapter 3 - Using The HP Praesidium SpeedCard	Describes how to use the SpeedCard.
Appendix A	Export considerations and card specifications.

Typographic Conventions

The following typographic conventions are used throughout this guide:

Table 2-2   **Typographic conventions**

CONVENTION	PURPOSE
italic	Used to signal a new term, for place holders, variables, and file names; or for emphasis.
bold	Used for command-line options, names of commands, menus, dialog boxes, and check boxes.
`computer`	This font denotes syntax, prompts, and code examples.

Where to find information on-line

A file of *this document* may be found at the following URL:

`http://www.docs.hp.com/hpux/pdf/A5486-90013.pdf`

What is the HP Praesidium SpeedCard?

The HP Praesidium SpeedCard is a hardware-based security solution that enables your server's CPU to sustain maximum performance. It is designed for applications that demand security yet still need to handle large client loads. An HP Praesidium SpeedCard is the secure server performance solution when you experience the following capacity issues:

- Your server is CPU bound (utilization is over 90%) under peak load.

- Your server's response time is slowing during busy periods, but your network pipe is not full.

- Your clients are being turned away.

An HP Praesidium SpeedCard dramatically increases your server's response time and the number of clients it can support. This is the server performance solution to help your business grow! The HP Praesidium SpeedCard easily plugs into your server's bus and performs the critical cryptographic functions required by your security system. An HP Praesidium SpeedCard not only accelerates the lengthy RSA public key decryption and encryption process, but also relieves the server CPU bottleneck.

The HP Praesidium SpeedCard also increases the number of clients your web server can support with security running Secure Sockets Layer (SSL) transactions. It improves CPU utilization and off-loads your server to perform other tasks.

The HP Praesidium SpeedCards provide two classes of cryptographic capabilities:

1. Modular exponentiation functions, including DH, DSA, RSA and raw modular exponentiation.

2. Random number generation, appropriate for secure key generation.

HP Praesidium SpeedCards are a balanced, economical co-processor with performance of a basic 1024-bit RSA private key decrypt or sign taking as little as 5 ms. For increased efficiency, multiple cards can be installed in the same system.

On Line Addition and/or Replacement (OLAR)

NOTE   The HP Praesidium SpeedCard, version A5486A, can only take advantage of OLAR features if your system is running the HP-UX 11i operating system and has a PCI bus.

OLAR Concepts for PCI Cards

Introduction

The letters O, L, A and R stand for On Line Addition [and] Replacement. This, of course, refers to the ability of a PCI I/O card to be replaced on an HP-UX computer system designed to support this feature without the need for completely shutting down, then re-booting the system or adversely affecting other system components. The system hardware uses the per-slot power control combined with operating system support to enable this feature.

IMPORTANT   Certain "Classes" of hardware are not intended for access by users. At this time this includes V-Class and Superdome systems. HP recommends that these systems only be opened by a qualified HP Engineer. Failure to observe this requirement can validate any support agreement or warranty to which the owner might otherwise be entitled.

Important Terms and Concepts

The addition or replacement of an OLAR-compatible card may be done in either one of two ways:

1. Using the SAM utility.

2. Issuing command-line commands using rad.

If detailed information about the use of either of these two procedures is required, you should refer to the following document:

Configuring HP-UX For Peripherals, HP Part Number B2355-90698

This document may be ordered from HP, or you may view, download and print it from the following website: `www.docs.hp.com`

Table 2-3   **Important Terms**

Term	Meaning
OLAR	All aspects of the OLAR feature including On-line Addition (OLA) and On-line Replacement (OLR).
Power Domain	A grouping of 1 or more interface card slots that are powered on or off as a unit. (NOTE: Multi-slot power domains are not currently supported)
target card / target card slot	The interface card which will be added or replaced using OLAR, and the card slot in which it resides.
affected card / affected card slot	Interface cards and the card slots in which they reside, and which are in the same power domain as the target slot.

IMPORTANT   In many cases, other interface cards and slots within the system are dependent upon the target card. For example:

- If the target card is a multiple-port card, suspending or deleting drivers for the target card slot also suspends individual drivers for the multiple hardware paths on that card).

During a card replacement operation, SAM performs a *Critical Resource Analysis*, which checks all ports on the target card for critical resources that would be temporarily unavailable while the card is shut down.

Planning and Preparation

For the most part SAM prevents you from performing OLAR procedures that would adversely affect other areas of the server. Refer to

Configuring HP-UX For Peripherals, HP Part Number B2355-90698 for detailed information.

Critical Resources

Replacing a card that is still operating can have extensive ramifications. Since power to the slot must be off when the old card is removed and the new card is inserted, the effects of shutting down the card's functions must be considered.

This is particularly important if there is no on-line failover or backup card to pick up those functions. For example:

- Which mass storage devices will be temporarily disconnected when the card is shut down?

- Will a critical networking connection be lost?

A critical resource is one that would cause a system crash or prevent the operation from successfully completing if the resource were temporarily suspended or disconnected. For example, if the SCSI adapter to be replaced connects to the un-mirrored root disk or swap space, the system will crash when the card is shut down.

During an OLAR procedure, it is essential to check the targeted card for critical resources, as well as the effects of existing disk mirrors and other situations where a card's functions can be taken over by another card that will not be affected.

Fortunately SAM performs a thorough critical resource analysis automatically, and presents options to you based on it's findings. If you determine that critical resources will be affected by the procedure, you could replace the card when the server is off-line, or if you must take action immediately, you can use `rad` to attempt an on-line addition of a backup card and deletion of the target card.

Firmware Patch Information

For those wishing to use OLAR, your system may n*eed to update its firmware. For additional details, please refer to the Readme Before Installing or Updating to HP-UX 11i* document provided with your HP product.

Card Compatibility

On-Line Addition (OLA).

When on-line adding an interface card, the first issue that must be resolved is whether the new card is compatible with the system. Each OLAR-capable PCI slot provides a set amount of power. The replacement card cannot require more power than is available.

The card must also operate at the slot's bus frequency. A PCI card must run at any frequency lower than its maximum capability, but a card that could only operate at 33 MHz would not work on a bus running at 66 MHz. `rad` provides information about the bus frequency and power available at a slot, as well as other slot-related data.

On-Line Replacement (OLR)

When on-line replacing an interface card, the replacement card must be identical to the card being replaced or at least be able to operate using the same driver as the replaced card. This is referred to as *like-for-like* replacement and should be adhered to because using a similar but not identical card may cause unpredictable results. For example, a newer version of the target card which is identical in terms of hardware may contain an updated firmware version that could potentially conflict with the current driver.

The PCI specification allows a single physical card to contain more than one port. A single-port SCSI bus adapter can not be replaced by a dual-port adapter, even if the additional port(s) on the card are identical to the original SCSI bus adapter.

When the replacement card is added to the system, the appropriate driver for that card must be configured in the kernel before beginning the operation. SAM ensures the correct driver is present. (In most cases, the replacement card will be the same type as a card already in the system, and this requirement will be automatically met.) If you have any question about the driver's presence, or if you are not certain that the replacement card is identical to the existing card, you can use *ioscan* together with `rad` to investigate.

- If the necessary driver is not present and the driver is a dynamically loadable kernel module (DLKM), you can load it manually. Refer to the section Dynamically Loadable Kernel Modules in Chapter 2 of the document: Configuring HP-UX For Peripherals, HP Part Number B2355-90698 for more information.

- If the driver is static and not configured in the kernel, then the card cannot be On-line Added. The card could be physically inserted on-line, but no driver would claim it.

3   Installation

This chapter describes important information related to the installation
and set up of your HP Praesidium SpeedCard.

Card Compatibility

HP-UX Systems

The HP Praesidium SpeedCard comes in three versions to accommodate a wide variety of HP-UX based servers and workstations. They are:

Table 3-1   **SpeedCard Versions**

HP-UX VERSION	SYSTEM	BUS TYPE	SPEECARD PART NUMBER
10.20	A-Class Servers and Workstations	PCI	A5486A
10.20	D-Class Servers and R-Class Servers	HSC	A5485A
10.20	K-Class Servers	HSC	A5484A
11.00 and 11i	N-Class Servers, L-Class Servers, V-Class Servers and Superdome	PCI	A5486A

Operating Systems

The HP Praesidium SpeedCards are compatible with the systems listed in Table 3-1 above running HP-UX, version 10.20, 11.0 or 11i (11.1x).

Physical Attributes

A5484A (HSC Version)
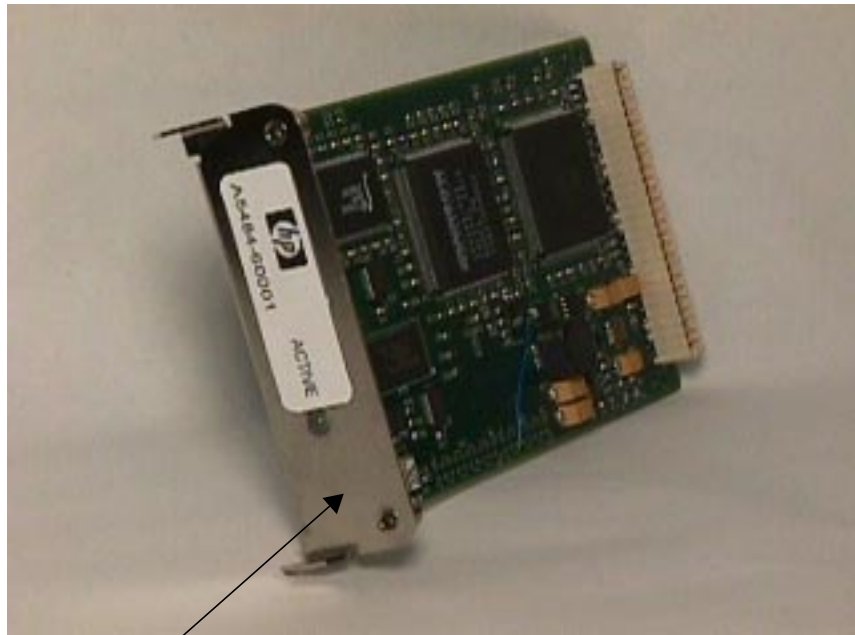
"Bulkhead"

- 3.25 inch (8.26 cm) height
- 1.0 inch (2.54 cm) width
- 5.75 inch (14.61 cm) length
- 4 ounces (113.4 g) weight

A5485A (HSC Version)
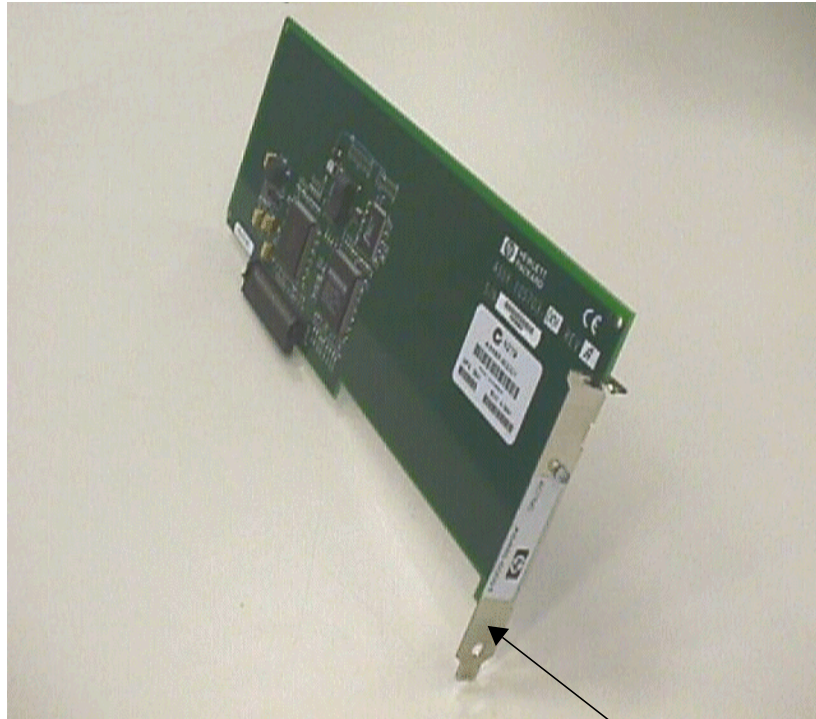
"Bulkhead"

- 4.75 inch (12.07 cm) height
- 0.75 inch (1.91 cm) width
- 13.25 inches (33.66 cm) length
- 4 ounces (113.4 g) weight

A5486A (PCI Version)
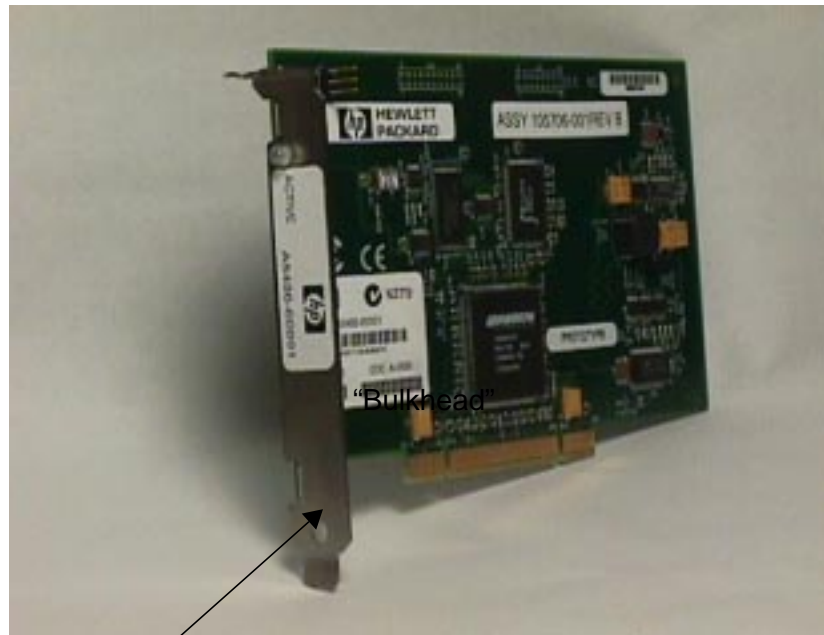
"Bulkhead"

- 4.25 inch (10.8 cm) height
- 0.75 inch (1.91 cm) width
- 7.0 inch (17.78 cm) length
- 5 ounces (141.7 g) weight

Installing the hardware and software

This section describes the process of installing your HP Praesidium SpeedCard and matching software.

Electrostatic Discharge (ESD) Precautions

CAUTION   The HP Praesidium SpeedCard contains electronic components that can easily be damaged by small amounts of static electricity. To avoid damage, follow these guidelines:

• Store the card in its antistatic plastic bag until you are ready to install it.

• Work in a static-free area, if possible.

• Handle the card only by the edges. Do not touch electronic components or electrical traces.

• Use the disposable grounding wrist strap provided with the card. Follow the instructions included with the strap.

• Use a suitable ground—any exposed metal surface on the computer chassis.

NOTE   Before attempting to install an HP Praesidium SpeedCard, please review your system documentation to determine if there are any safety warnings, special cautions, or installation requirements for your system.

Installing an A5484A HSC SpeedCard

The HSC version of the HP Praesidium SpeedCard is installed in K-class systems in either the HSC Expansion I/O card or the Core I/O card. Before you begin installing the card, be sure you have free slots available in the HSC Expansion I/O card or the Core I/O card.

Please refer to the user documentation provided with your computer for

details about how to open the cabinet and access the various areas within.

For each card you are installing into the system, follow these steps:

Step 1. Exit all running programs and shut down the system by using this command:

```
/etc/shutdown -h
```

Step 2. Wait until the system responds with "OK to press reset" or "Halted, you may now cycle power," and then power off the system.

Step 3. Turn off the power to the HP 9000 system.

Step 4. Determine whether you will install the card in the Core I/O card or the HSC Expansion I/O card. The Core I/O card provides one card slot. The HSC Expansion I/O card provides four card slots. If the system does not have an HSC Expansion I/O card, install the HP Praesidium SpeedCard in the Core I/O card.

Step 5. Remove the Core I/O or HSC Expansion I/O card from the HP 9000.

Step 6. Simultaneously pull out the extractor levers on both ends of the Core I/O or HSC Expansion I/O card. Carefully pull the card out of its system slot. Allow the card to follow the runners as you pull out the card, to avoid bending it.

Step 7. If you are installing the HP Praesidium SpeedCard in the Core I/O card, install the Accelerator Card in the available HSC slot. If you are installing the Accelerator Card in the HSC Expansion I/O card, install the Accelerator Card in one of the four available slots. Use a screwdriver to unscrew the two screws on the front of the slot until they pop out.

Step 8. Attach the grounding strap to your wrist or ankle.

Step 9. Remove the HP Praesidium SpeedCard from its antistatic plastic bag.

Step 10. Position the card over the slot so that the hinges point up.

Step 11. Place the hinges on the front end of the card into the hinge slots on the Core I/O or HSC Expansion I/O slot. If you are installing the card into the Expansion I/O slot, align the standoffs to the holes on the Expansion I/O slot. The figure below shows the card's hinges, standoffs, and HSC
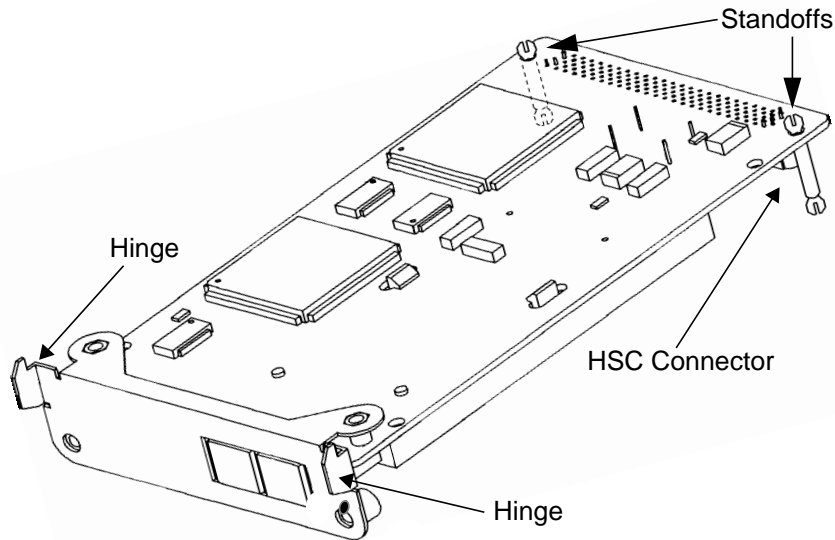
connector.

Step 12. Align the HSC connector on the HP Praesidium SpeedCard with the HSC connector in the slot.

If you are installing the SpeedCard in the Expansion I/O card, make sure the nylon standoffs on the SpeedCard are properly aligned with the small round holes on the Expansion I/O card. (Note that if you are installing the SpeedCard in the Core I/O card, the standoffs do not connect to the Core I/O card.)

Step 13. Press the SpeedCard firmly into place, making sure that the two HSC connectors are flush with each other. If you are installing the card in the HSC Expansion I/O card, make sure the nylon standoffs on both sides of the HSC connector are snapped firmly into place, to properly complete the card's installation.

Step 14. Use a screwdriver to screw the card into place by screwing in the two screws on the front of the slot. The following figures show the SpeedCard

installed in the Core I/O card and the HSC Expansion I/O card.

Front of Core I/O Card

HSC Connector ⟶
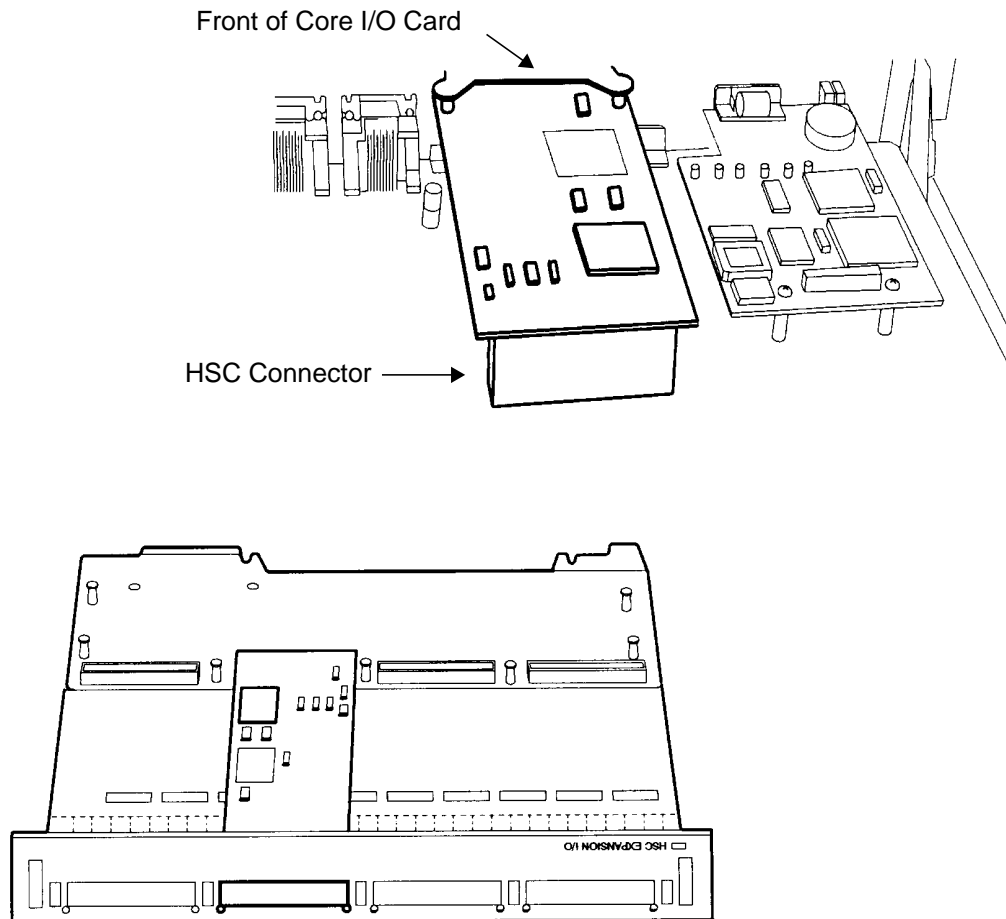
Step 15. Reinstall the Core I/O or HSC Expansion I/O card. If you are reinstalling the Core I/O card, position the card so that the SpeedCard is on the right side. If you are reinstalling the Expansion I/O card, position the card so that the SpeedCard is on the left side.

Step 16. Align the Core I/O or Expansion I/O card with the runners in its slot and gently push the card back into the system. Carefully use the runners in the slot to guide it.

Step 17. Push the Core I/O or HSC Expansion I/O card firmly back into place.

Step 18. Push down firmly on the extractor levers on both ends of the card, to secure it in place.

Step 19. Screw the two slot screws back into place.

Step 20. Repeat the above process if you have additional cards to be installed.

Step 21. Power on the system.

Step 22. Continue with the section titled, "Loading the software driver and tools" at the end of this chapter.

Installing an A5485A HSC SpeedCard

Please refer to the user documentation provided with your computer for details about how to open the cabinet and access the various areas within.

Step 1. Exit all running programs and shut down the system by using this command:

```
/etc/shutdown -h
```

Step 2. Wait until the system responds with "OK to press reset" or "Halted, you may now cycle power," and then power off the system.

Step 3. Turn off the power to the HP 9000 system.

Step 4. Remove the screws that attach the top panel(s). You may find it helpful to move the system away from other hardware for easier access to the internals of the system.

Step 5. Attach the grounding strap to your wrist or ankle.

Step 6. If necessary, remove the cover plate(s) from the opening(s) for the slots you will use. Keep the screw for later use.

Step 7. Remove the HP Praesidium SpeedCard from its antistatic plastic bag.

Step 8. Find an empty slot and align the connector on the SpeedCard with the connector in the slot, being sure that the card slides down the slot guides on each side.

Step 9. Press the card firmly into place, making sure that the connector is fully inserted. Note that the LED on the card's bulkhead is not visible from the outside of an R-Class system as it is on other types of systems. To view the card's indicator LED, you must remove the top panel(s) of the system.

Step 10. Make sure the screw hole in the card's bulkhead lines up with the hole in the chassis assembly. Use the screw you saved earlier to attach the card's bulkhead to the chassis.

Step 11. Repeat the above process if you have additional cards to install.

Step 12. Power on the system.

Step 13. Continue with the section titled, "Loading the software driver and tools" at the end of this chapter.

Installing an A5486A PCI SpeedCard

Please refer to the user documentation provided with your computer for details about how to open the cabinet and access the various areas within.

NOTE   Users of V-Class and Superdome systems should call their HP support contact for card installation. These systems are not intended to be opened by the customer. Doing so could void any existing warranty and/or support contract.

Step 1. Exit all running programs and shut down the system by using this command:

```
/etc/shutdown -h
```

Step 2. Wait until the system responds with "OK to press reset" or "Halted, you may now cycle power," and then power off the system.

Step 3. Turn off the power to the HP 9000 system.

Step 4. Disconnect the computer from the A.C. power source.

Step 5. Disconnect all attached cables and wires.

Step 6. Open the cabinet.

Step 7. If necessary, remove the cover plate(s) from the opening(s) for the slots you will use. Keep the screw for later use.

Step 8. Attach the grounding strap to your wrist or ankle.

Step 9. Remove the HP Praesidium SpeedCard from its antistatic plastic bag.

Step 10. Align the connector on the SpeedCard with the slot connector which is closest to the opening in the chassis. Note that the card only connects with one of the two connectors for that slot.

Step 11. Press the card firmly into place, making sure that the connector is fully inserted, and the card's bulkhead shows through the chassis slot opening. The LED on the card's bulkhead should be visible from the outside once the cover has been replaced.

Step 12. Make sure the screw hole in the card's bulkhead lines up with the hole in

---

the chassis assembly. Use the screw you saved earlier to attach the card's bulkhead to the chassis.

Step 13. Close the cabinet.

Step 14. Re-attach all of the cables and wires.

Step 15. Connect the A.C. power cable.

Step 16. Power on the system.

Step 17. Continue with the section titled "Installing the software" at the end of this chapter.

Installing the Software

Required Patches

Refer to Release Notes for a list of required patches.

Installation overview

The software installation for HP-UX has been divided into four steps. Steps 1-3 will apply to most users. Step 4 only applies if you are installing on a Netscape 3.x server.

1. Install the device driver and SwiftAPI.

2. Quick verify process.

3. Install the Netscape plug-in module.

4. Installation procedure for Netscape 4.x servers.

Step 1: Install the device driver and SwiftAPI

This procedure installs the device driver and SwiftAPI from a depot file.

1. Be sure you have installed the HP Praesidium SpeedCard in your system using the previous instructions.

2. Run the `swinstall` program.

3. Select the appropriate source depot type (Local CD, Local Tape, Local Directory, Network Directory).

4. Select the source host name.

5. Select the source depot path. Click the "Source Depot Path" button to list all.

6. Highlight `Praesidium SpeedCard software`.

7. Choose "Mark for Install" from the "Actions" menu.

8. Choose "Install" from the "Actions" menu. An analysis window will pop up.

9. Activate the "OK" button in the "Installation Analysis Window" when the status field displays a "READY" message.

10. Activate the "Yes" button at the Confirmation Window to confirm that you want to install the software. "swinstall" loads the fileset, runs the

control scripts for the fileset, and builds the kernel. The estimated time required for processing will be 3 - 5 minutes.

11. When the status field indicates "Ready", a Note Window will open. Activate the "OK" button on the Note Window to reboot the system.

Step 2: Quick verify process

This section allows you to verify that the hardware, device driver, and SwiftAPI function correctly.

1. After re-booting the system (see step 11 in the previous section), change into the /opt/cryptofast subdirectory.

2. run csdiag -1

   Sample Output (example has two SpeedCards)

   ```
   >csdiag -1

   Praesidium SpeedCard Diagnostics & Maintenance

   Accelerators

   Accelerator     Hardware     Firmware     BIOS

   Card 0          103c:2.0.0   2.0.22       0.0.0
   Card 1          103c:2.0.0   2.0.22       0.0.0
   ```

3. If the csdiag diagnostic program outputs a list of accelerators similar to the output above, the hardware, device driver and SwiftAPI are working properly.

Step 3: Install the Netscape plug-in module

This procedure installs the Netscape plug-in module.

1. Make sure that the Netscape Server has already been installed and the SSL secure protocol is functional. Point a web browser to https://<servername> to verify.

NOTE   For instructions on how to setup SSL under Netscape, please refer to Netscape documentation.

2. On the HP-UX server, change the directory to `/opt/cryptofast`.

3. Run the script `csinstall.sh`.

4. Restart the Netscape server by running the `start` script from the <Netscape Root> directory.

5. Repeat step (1) to make sure that the `https` protocol is still working.

Compatibility with Netscape Navigator browser version 3.51

A documented bug in the Netscape Navigator (browser) version 3.51 may cause the Praesidium SpeedCard software to fail. For this reason, it is recommended that Navigator users use Netscape Navigator version 3.6x, or later, with the HP Praesidium SpeedCard.

Cryptoki Module Installation Instructions

To install a Cryptoki module into the iPlanet iWS 4.1 SP 2, you must add the module into the Netscape Security Module database. Follow these steps to install the Rainbow Cryptoki module:

NOTE	The utility program, *setuser*, and shell script files, *add_cryptoki.sh* and *list_cryptoki.sh* are in the /opt/cryptofast directory.

1. Run the *setuser* utility to create the Cryptoki token file. Run `setuser <SOpin> <USERpin>` to create the file */etc/RnboCryptoki*.

   `<SOpin>` is the Security officer password and `<USERpin>` is the user password. *The password must be an alphanumeric string, at least 8 characters long.*

2. Check that the file */etc/RnboCryptoki* is created with write permission enabled for everyone.

3. Install iPlanet iWS version 4.1 SP 2 or above on your system and set up the Administration Server.

4. Start the Administration Server and, using your browser, create a new Netscape Server. e.g `https-<hostname>`

5. From the Administration Server, click on *manage* to manage the new server.

6. In the *security* section, click on *Create Database*. Use the same

password as for the Cryptoki library `<USERpin>` above.

7. Check that the files *<server root>/alias/secmod.db*, *key3.db* and *cert7.db* are created. If the files *https-<hostname>-key3.db* is created instead, create a symbolic link for *key3.db* by typing:

   `ln -s https-<hostname>-key3.db key3.db`

   Repeat the same step for *cert7.db*. This is due to the Admin Server looking for a different name of the same file.

8. After the three database files are created, add the Rainbow Cryptoki module to this security database using the *modutil* utility. Run the shell script: `./add_cryptoki.sh`

9. Check that the Rainbow Cryptoki module is in the database by running the shell script: `./list_cryptoki.sh`

10. Using the Administration Server, create a request by clicking on *Request a Certificate*. A key pair will be generated with the request. Check that your database file *key3.db* and *RnboCryptoki* is being updated.

NOTE   A new certificate is required to use the Rainbow Cryptoki module.

---

11. Complete the form to request a certificate. Make sure that, for the Cryptographic Module, you select *ISG 2.0 Cryptoki Interface* as the module for this certificate and use the `<USERpin>` for the Key Pair File Password.

12. To submit a request, copy the request form with "----Begin Request---" and "---End Request---" included. Paste it into the *CSR* section of the certificate request web site. After the certificate is granted, cut the text wrapped by "---Begin Certificate---" and "---End Certificate---" to paste it to the install certificate page on the new server.

13. Install the downloaded certificate to the database by clicking *Install Certificate* on the same page. Make sure to use *ISG 2.0 Cryptoki interface* for the Cryptographic Module and use the `<USERpin>` as the Key Pair File Password. Click on *add* certificate to add to the database.

14. To check if the certificate is installed properly, click on *Manage Certificate* and type the `<USERpin>` password. The newly installed certificate must be in the database before starting the server.

---

15. Go to *Preferences* to enable encryption for the new server. Click on *Encryption On/Off* to turn on encryption on port 443. This can also be done with modifying *magnus.conf*. Click on *Apply* to apply changes.

16. Modify the file *magnus.conf* for the newly created Netscape server. This file is located in your *config* directory. It is in:

    `/usr/netscape/server4/https-hostname/config/magnus.conf`

    Add this line to the last section of the file:

    `CERTDefaultNickname ISG 2.0 Cryptoki Interface:Server-Cert`

    where `Server-Cert` is the name of the certificate file you have created. Compare this name to the *Manage Certificate* list.

17. In the file *magnus.conf*, verify that the Port number used is *443* and that Security settings are *on*.

18. Start this new server by running, `./start`. Type in the Key File Password, which is also your `<USERpin>` for the Cryptoki module.

4 Using the SpeedCard

This chapter provides some additional information about using your HP Praesidium SpeedCard.

Once the HP Praesidium SpeedCard has been installed, the cryptographic SSL functions are automatically performed by the card rather than the system's CPU.

Diagnostic and Maintenance Tools

The HP Praesidium SpeedCard software includes three Diagnostic and Maintenance Tools that provides the following functions:

- Diagnostics of all SpeedCards in your system.
- Ability to upgrade your SpeedCard with future versions of the firmware.

The tools are:

- `csdiag`
- `vector`
- `sp1024`

The SpeedCard's LED

The bulkhead of the HP Praesidium SpeedCard has a 3-color Light Emitting Diode (LED) to help in establishing the correct operation of the card. This LED provides the following information:

Table 4-1   **Status LED indications**

LED COLOR	MEANING
Green	Ready (after firmware is loaded)
Red	Error
Yellow	On-going math operations.

NOTE

It is normal for the yellow indication on this LED to flash intermittently, under certain circumstances.

A5484A (HSC) LED Location

The location of the LED on a K-Class card is shown below.

"Active" LED

A5485A (HSC) LED Location

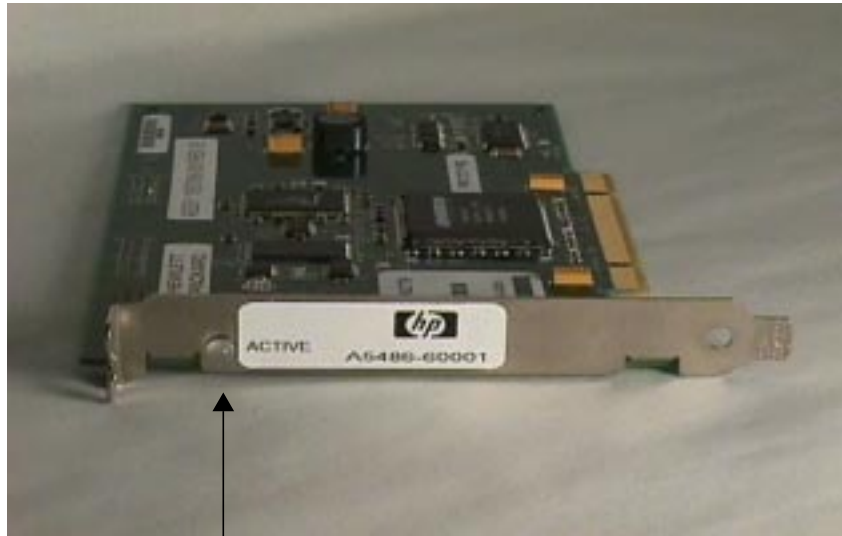The location of the LED on a D-Class or R-Class card is shown below.

"Active" LED

A5486A (PCI) LED Location

The location of the LED on an A-Class card is shown below.

"Active" LED

5   Appendix

Export Considerations

The HP Praesidium SpeedCard falls under the authority of U.S. export controls policy and requires an export license.

The U.S. Government currently allows the export of only short (512-bit) RSA cryptography when used for key establishment. Export of larger key sizes, such as 1024-bit, is permitted when the field of use is limited to authentication. If your web server needs to service foreign clients, it would be sensible to configure SSL to use a short key for key establishment and a long key for authentication.

Using separate keys for key establishment and authentication is more secure and assists in meeting U.S. export laws, but carries even greater computational cost -- two RSA private key operations rather than one.

Using separate keys may also be beneficial for supporting key recovery systems. The export of longer key RSA cryptography is also possible for narrower scope protocols than SSL, such as financial protocols. So, although U.S. and other nations' export controls limit the export of general purpose cryptography to short RSA keys, it is still likely that long RSA keys will be the most commonly used.

Specifications

This section lists specifications that may be important to users.

Physical

Please refer to Chapter 3.

Electrical

These specifications apply to all versions of the card.

- DC power dissipation, 5V mode: 5.1 Watt Max.
- DC power dissipation, 3.3V mode: 4.6 Watt Max.
- Heat dissipation: 8.1 Watts

Environmental

- Operating temperature: 5 degrees C to 40 degrees C
- Storage temperature: -40 degrees C to +70 degrees C
- Relative humidity: 15% to 80% at 40 degrees C non-condensing

Electromagnetic Compatibility

Table 5-1   **Electromagnetic Compatibility**

FCC part 15 Class A	USA, Canada and Latin America
CISPR-22/EN55022 Class A, EN50082-1	International and European Community
AS/NZS 3548:1995 Class A	Australia and New Zealand

Appendix
Specifications