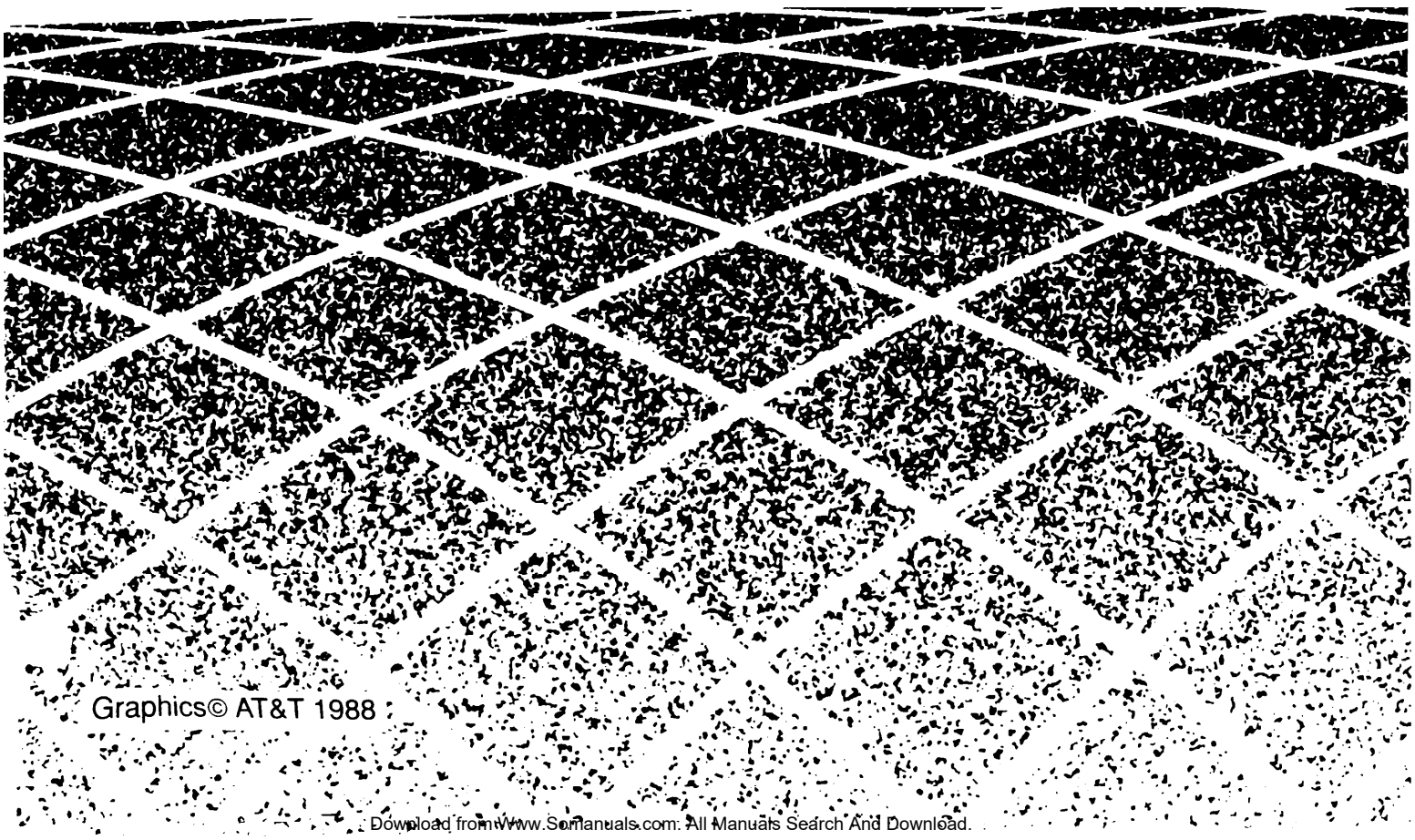
AT&T

DEFINITY® Communications System

Remote Port Security Device User's Manual



While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, AT&T can not assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

TRADEMARK NOTICE

AUDIX is a trademark of AT&T.
DATAPHONE, DEFINITY, DIMENSION, and UNIX are registered trademarks of AT&T.

ORDERING INFORMATION

To order copies of this document:

Call: AT&T Customer Information Center at 1 800 432-6600
In Canada call 1 800 255-1242

Write: AT&T Customer Information Center
2855 North Franklin Road
P.O. Box 19901
Indianapolis, Indiana 46219-1385

Order: Document No. 555-025-400
Issue 2, October 1991

Published by
Technical Publications
AT&T Bell Laboratories

IMPORTANT SAFETY INSTRUCTIONS

To reduce the risk of injury from fire or electric shock, always follow the basic safety precautions when using this product. The safety symbol (exclamation point inside a triangle) on the RPSD Lock or RPSD Key alerts you to the important operating and maintenance instructions below.

1. **Read and understand all instructions in this user's manual.**
2. **Observe all warnings and instructions** marked on this product.
3. **Unplug this product from wall outlets and telephone jacks before cleaning.** Clean exposed parts with a soft, damp cloth. Do not use liquid or aerosol cleaners, and never immerse in water.
4. **Do not use the product near water or when you are wet.** For example, do not use it in a wet basement or near a swimming pool, bathtub, shower, sink, or laundry tub. If the product comes in contact with any liquids, unplug the power and line cords immediately. Do not plug the product back in until it has been dried thoroughly.
5. **Install this product securely on a stable surface.** Damage may result if the product falls.
6. **Install this product in a protected location** where no one can step on or trip over power and line cords. Do not place objects on the cords that may cause damage or abrasion.
7. **Do not allow anything to rest on the power cord.** Do not locate this product where the cord will be abused by persons walking on it. **Do not overload wall outlets,** as this can result in the risk of fire or electric shock.
8. **Never push objects of any kind into this product through housing openings** because they may touch dangerous voltage points or short out parts, resulting in possible fire or electric shock.
9. **If this product does not operate normally, see the troubleshooting section of this manual.** If you cannot resolve the problem, or the product is damaged, report the trouble to AT&T. Do not open the product. Opening the product may expose you to dangerous voltages or other risks.
10. **During thunderstorms, avoid using telephones except cordless models.** There may be a slight chance of electric shock from lightning.
11. **Never install telephone wiring during a lightning storm.**
12. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
13. **Never touch uninsulated telephone wires or terminals** unless the telephone line has been disconnected at the network interface.
14. **Use caution when installing or modifying telephone lines.**
15. **Do not use a telephone in the vicinity of a gas leak.** If you suspect a gas leak, report it immediately, but use a telephone away from the area where gas is leaking.

16 **This product should be operated only from the type of power source indicated on the power transformer** (see Item 18 below). If you are not sure of the type of power supply to your business or home, consult your local power company.

17 **The wiring from the Subscriber (modem) jack should not leave the building premises** unless it interfaces to a product providing primary and secondary protection.

18 **Use only a UL Listed wall plug-in power transformer that has Class 2 outputs and the following characteristics:**

Input rating:	120 V AC +/- 10% 6Hz 150 mA maximum
Output rating:	12 V DC at 1 A

The power transformer supplied with the product has these characteristics.

SAVE THESE INSTRUCTIONS

FCC Notices

Part 15, Subpart A

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.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the 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 operations. 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.

Changes or modifications to the RPSD device or devices that are not expressly approved by AT&T could void the user's authority to operate the equipment.

Part 68

This equipment complies with part 68 of the FCC rules. On the bottom of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of REN's should not exceed five. To be certain of the number of devices that may be connected to the lines, as determined by the total REN's, contact the telephone company to determine the maximum REN for the calling area.

If the Remote Port Security Device Lock and Key (RPSD) causes harm to the telephone network, the telephone company will notify you in advance that the temporary discontinuance of service may be required. But, if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with the RPSD equipment, please contact AT&T for repair and/or warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. Refer to Chapter 5 for repair information or call 1-800-242-2121.

There is one public switched network interface jack (RJ11C), which has been registered for permissive operation.

Contents

1 Getting Started

2 Installation

3 RPSD System Administration

4 RPSD Key Use

5 Troubleshooting

A Cables, Connectors, and Ports Table

B Device LEDs

List of Figures

List of Tables

1 Getting Started

Getting Started

The DEFINITY® Remote Port Security Device (RPSD) is a single line dial-up port protection system that prevents unauthorized access to a host resource. Host resource dial-up ports, called "subscribers," are protected by the installation of the RPSD Lock hardware unit on the analog interface channel leading to the subscriber port. Access is provided only when the calling party uses the RPSD Key, a hardware unit installed on the analog interface channel on the calling party end.

The RPSD system provides security and control for virtually any type of dial-up port on any host resource, regardless of the type of modem associated with the host's dial-up ports. This document specifically targets AT&T Business Communications Systems customers and users of the DEFINITY Communication System, System 85, System 75 PBXs, DIMENSION® PBX, and supporting peripheral products, for which reason most references in this document are specific to Business Communications Systems. However, this should not be understood as restricting other applications of the RPSD system.

The RPSD Lock and Key system also provides the system administrator greater control over the PBX or protected host resource administration by enabling the system administrator to specify the time of day that access to a port is permitted or to block any or all access to the line by users of RPSD Keys. In addition, a system activity log provides a real-time record of access attempts and their outcomes. Session summaries track statistics on all successful and failed attempts, providing convenient MIS data resources.

Note: **The Remote Port Security Device, if properly installed and managed, clearly provides a significant and substantial barrier to unauthorized access to a dial up communication port.**

Note that the Remote Port Security Device cannot be assumed to be impregnable, but needs to be viewed as an important addition to the tools and measures used by system managers to prevent unauthorized access to dial up ports.

The RPSD system protects a port in the following manner: a call into the channel to the protected host activates the RPSD Lock. Without involving the protected host resource or its associated modem, the RPSD Lock performs a verification of the caller's identity through a set of communications with the RPSD Key using DTMF signaling. This process is described in the following procedure and is illustrated by Figure 1-1.

1. The Lock, installed on tip and ring on the network side of any modem or protected host resource, answers the incoming call.
2. The Lock sends the caller a polling tone. If the calling party has an RPSD Key, the Key responds with its User ID. If there is no Key on the calling end, the Lock terminates the call.
3. The Lock must recognize the Key's User ID (it must be previously initialized with all valid Keys); if not, the Lock terminates the call.
4. Using an algorithm governed by ANSI/DES standards, the Lock generates a random 10 digit value (known as the "dynamic challenge," for which there are 10 billion possible values). Using a secret encryption key that is uniquely associated with the calling RPSD Key's User ID, the Lock puts the value through the encryption process and encrypts it.
5. It stores the encrypted "expected value," and sends the dynamic challenge to the Key.
6. The Key repeats the encryption process and calculates the necessary response. The Key transmits the "expected value" to the Lock.
7. The Lock authenticates the response by comparing it to the expected value it calculated and stored. If the Lock receives the precise value it expects, it generates ringing and sends the call on to the protected resource.

The entire sequence occurs in less than 20 seconds.

FIGURE 1-1
Protection Process

The RPSD Lock device is approximately the size of a modem and is connected between the PBX modem and the Central Office (CO) line. The RPSD Key device is of similar size and is connected between the client's (caller's) modem and CO line. See Figure 1-2.

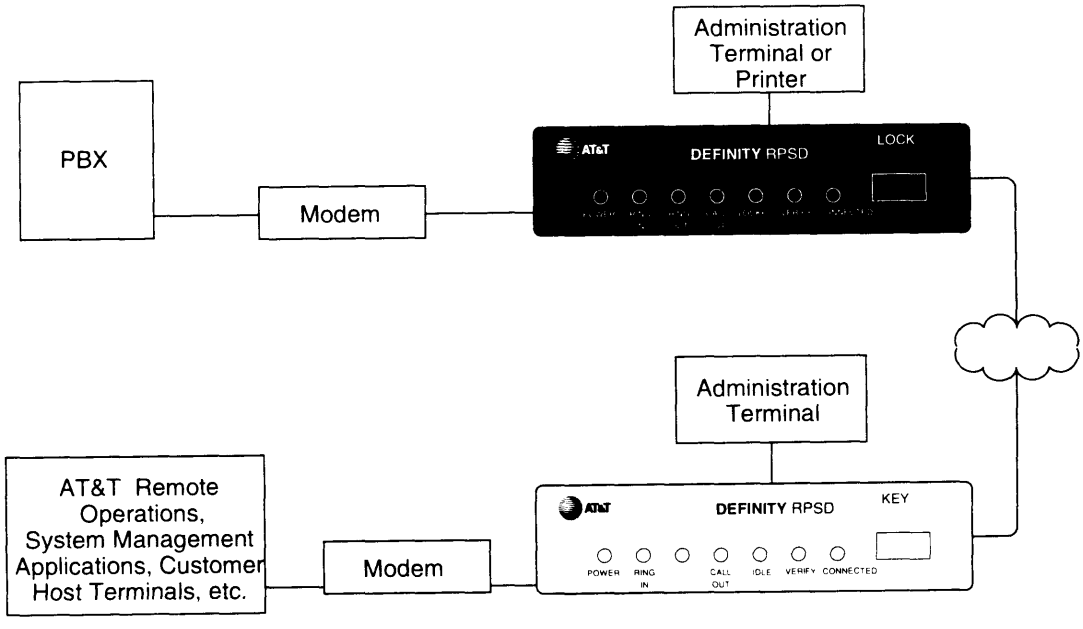


FIGURE 1-2
RPSD Lock and Key Configuration

In Figure 1-2, the term "AT&T Remote Operations" refers to Technical Services Center remote administration and maintenance operations, Bell Labs Field Support and other entities.

The system administrator administers the RPSD Lock via a direct connection from an administration terminal to the Lock. The administration interface is menu driven.

Note: In this document, a caller's computer terminal or personal computer is referred to as the caller's or user's terminal. The terminal connected to the RPSD Lock is referred to as the system administrator's terminal or administration terminal.

Audience

This document is intended for the following audience:

- AT&T Technicians
- RPSD System Administrators
- RPSD Key Users

AT&T Technicians refers to the personnel from AT&T who install the RPSD Lock device at the customer premises. It is assumed that AT&T Technicians are familiar with the technical language used to describe the hardware components, cables, connectors, and ports involved in the installation of the RPSD Lock device. It is further assumed that they will have the tools and equipment necessary for installation.

RPSD system administrators refers to the customer personnel who administer and maintain the RPSD Lock device. It is assumed that RPSD system administrators are familiar with menu-driven software systems and that they understand the references to the various telecommunications hardware components. It is also assumed that they understand the need for maintaining security in administering the PBX switch.

“RPSD Key users” refers to all those who dial in to a channel locked with an RPSD Lock device using an RPSD Key device. It is assumed that RPSD Key users are familiar with placing calls via a modem, either from a telephone or terminal.

Responsibilities

Installation of the RPSD Lock device is performed by AT&T technicians. These technicians are responsible for installing the device, testing it upon installation, and making certain that a working product has been installed at that time. AT&T technicians also perform any replacement of the RPSD Lock device should it become necessary. AT&T technicians are not responsible for the initialization of the RPSD Lock. The RPSD Lock is initialized prior to delivery and the RPSD Key devices that are used by AT&T are already installed and initialized.

RPSD Keys purchased by the customer can be installed by AT&T technicians at the customer’s request or installed by the customers.

The troubleshooting material in this document may be used by the technician at the time of installation, but is written primarily for the customer. Failure of any RPSD Lock or RPSD Key device is always resolved by replacement of the failed device.

The RPSD Lock commands and administration material is written for RPSD system administrators. The material on RPSD Key commands and use is written for RPSD Key users.

Supplying equipment peripheral to the RPSD Lock, such as terminals, modems, printers, etc., is the customer’s responsibility. If any material is required in addition to the material shipped in the RPSD package, it is billable to the customer.

In This Document

This document comprises the following material:

- **Chapter 1: Getting Started** provides an overview of the RPSD system, a description of this document and its intended audience, and an explanation of typographical conventions.
- **Chapter 2: Installation** describes the recommended hardware environment and lists the RPSD system hardware and software components. Finally, the chapter describes the installation procedures for the hardware and software.
- **Chapter 3: RPSD Administration** explains the features and variants of the RPSD system that must be administered, system status messages, and system administrator commands.
- **Chapter 4: RPSD Key User Information** describes the procedure for accessing the RMATS port via a "keyed" terminal, what to do if access fails, and the RPSD Key commands.
- **Chapter 5: Troubleshooting** lists and explains the status messages, tests for the RPSD Lock and Key, what to do in the event the RPSD Lock or Key fails, RPSD system response to a power failure, and saving the "seed" value of the authentication algorithm.
- **Appendix A: Cables, Connectors, and Ports Table** contains a table showing the cables, connectors, and ports required for each hardware component.
- **Appendix B: Device LEDs** explains the meaning of the LEDs on the RPSD Lock and the RPSD Key devices.

Typographical Conventions

Throughout this guide, all forms of output or responses are shown in bold, sans serif style type. For example:

Call authentication completed

Data that you enter is shown in italic, sans serif style type. For example you may be instructed as follows:

Enter the command:

Block user [RETURN]

Note the following characteristics of the data entry representation:

- The first line is a normal text line of the document.
- The second line is the information you are instructed to enter. The [RETURN] at the end of the line tells you to press the Enter or Return key to complete the command.

Hotline or Other Service Call Numbers/Addresses

If assistance is needed with the RPSD Lock, Key, or the PBX, or problems occur in the RPSD Lock or Key that cannot be resolved by using Chapter 5, *Troubleshooting,* contact the technical support center at:

1 800 242-2121

2 Installation

Installation

This chapter describes the recommended room layout and environment, hardware components, installation procedures, and testing for the RPSD. In addition to this chapter, you may wish to refer to Appendix A, *Cables, Connectors, and Ports Tables* for quick reference materials on the installation of the hardware components. If this is the first time you have installed an RPSD system, or it has been a long time since you last installed an RPSD system, it is highly recommended that you read this chapter.

Room Layout/Environment

While the location of the RPSD Lock is not critical to its function, it is best if the Lock is kept in an equipment cabinet near the PBX modem. This helps protect the Lock against dust and other precipitate, as well as protecting against physical damaging from being knocked to the floor or having things dropped on it. Alternative locations are on a table near the PBX modem or on top of the PBX cabinet. This last location is discouraged as heat tends to accumulate at the top of the PBX cabinet.

Note: A damaged Lock prohibits use of the RMATS channel. Secure location of the RPSD Lock is very important to maintaining uninterrupted service.

If more than one RPSD Lock is installed at a particular customer site, the Locks may be stacked on top of each other to save space. Very little heat is generated by the Locks, so separating them is not warranted.

Note: In a multiple Lock installation, be certain that you label the Locks according to which lines they protect, to prevent confusion.

Power Supply

The RPSD Lock and the RPSD Key devices are both powered by ordinary AC outlets. These need not be grounded (three prong) outlets. Use of extension cords where needed is acceptable. However, given that an interruption in power to the RPSD Luck unit will result in a complete blockage of both incoming and outgoing calls on the RMATS channel, and given that a power outage could require administration of the PBX, it is advised that the RPSD Lock be powered from the Uninterruptible Power Supply (UPS) that is frequently included in a PBX configuration. Additionally, if the modem to the RMATS channel is external (System 85 and DEFINITY Generic 2 models), the modem should also be powered from the UPS.

Note: A locked channel is inaccessible during a power outage for the duration of the outage. No administration of the RPSD Lock need be done when the outage ends. That is, when power is restored, the RPSD Lock device will automatically come back on-line and reset itself to an Idle/Locked state. Key information and parameters will be unchanged by the outage.

Where a UPS is present, there are often many demands placed on it. The power pack for the Lock draws a maximum of 18 watts. This should not place any great strain on the UPS, but should be considered with the overall draw on the UPS.

External surge protection is optional.

Location of Administration Terminal or Printer

For the purposes of installation, it is simplest if the RPSD Lock or Key administration terminal or printer is co-located with the RPSD Lock or Key. However, this is not always possible. In the event that the terminal or printer must be located at some distance from the RPSD Lock or Key (in another room, on another floor, etc.), the limitations of the EIA-RS232 interface must be considered.

To overcome such restrictions, the baud rate of the administration terminal or other equipment connected to the Aux. Port should be adjusted as follows:

- Cables of 0-50 feet - a maximum 9600 baud
- Cables of 50-100 feet - a maximum 4800 baud
- Cables of 100-2000 feet - a maximum 2400 baud

Set the link speed by using the Set Communications Parameters command from the Menu of Commands. See Chapter 3, *RPSD System Administration* for details on using this command with the RPSD Lock or Chapter 4, *RPSD Key Use* for details on using this command with the RPSD Key.

Hardware Components

When you order the RPSD Lock device, you receive the Lock, power supply, a 7-foot cable with modular connectors on each end, and a 14 foot cable with modular connectors on each end. If any other cables or connectors are required, they must be ordered separately. In addition, any peripheral devices, such as the administration terminal or printer, are customer supplied.

A PBX and modem are assumed to be at the customer site already.

Note: Although the printer is not essential to system operation, it is highly recommended that a printer be dedicated to the RPSD Lock. Because the System Activity Log is limited to storing sixty messages, the only means of retaining a more permanent record of system activity is to either install a dedicated printer for the RPSD Lock or to save all messages from the Lock to disc.

With regard to RPSD Key devices, the AT&T entities which require access to the PBX already have the Keys that they need. Any additional RPSD Keys for customer use must be ordered separately.

Each of the hardware components (both supplied and otherwise) and their requirements are described in the following sections.

RPSD Lock

The RPSD Lock is 5.75 inches wide by 9.5 inches long by 1.75 inches high. The RPSD Lock has seven LEDs on the front panel and four ports on the back panel. For a detailed description of the front panel LEDs, see Appendix B, *Front Panel LEDs.* The back panel ports are:

- an RJ11 port for the CO line, labeled **Telco**
- an RJ11 port for the modem connection, labeled **Subscriber**
- a female DB25 port for the terminal or printer (or a modem), labeled **Aux. Port**
- a port for the power supply (supplied with the RPSD Lock).

Use a modular telephone plug to connect the CO line to the Telco port on the RPSD Lock, and to connect the subscriber port on the RPSD Lock to the modem. Use only the tip and ring leads.

Install the RPSD Lock between the CO line that is reserved as the remote maintenance and administration channel and the PBX modem. If one is not already present, install an RJ11 port on the CO line to facilitate installation of the RPSD Lock device and also to make subsequent service easier. Be certain to label all connections to make subsequent service easier.

RPSD Power Monitor Adapter

The Power Monitor Adapter (PMA) (Comcode 406453662) provides an installation option that allows you to control the behavior of the RPSD during power failure conditions.

In the event of a unit failure or a power failure, the RPSD is designed to block incoming and outgoing calls to the port, protecting the port against unauthorized access. This call blocking also prevents the PBX or other protected resources from originating an alarm and will block dial-up access to the port.

When a PMA is installed, a failure condition causes the RPSD to be bypassed until the failure condition is cleared. Incoming calls to the PBX or other host resource will be permitted, and RPSD Lock security is bypassed.

A failure condition forces a contact closure within the PMA which can be connected via the PMA Alarm Leads to an external alarm sensing device (such as PBX external alarm connections).

The pma can also be used to generate a signal failure through the Alarm Lead connection without bypassing the RPSD and compromising security. This is referred to as **Alarm Only** installation.

For more information on the PMA, refer to the *Addendum to DEFINTY Remote Port Security Device (RPSD) User's Manual - Power Monitor Adapter.*

A second pair of RJ11 port connections may be installed for simple bypass of the RPSD Lock. To bypass the Lock, the modular connection cords are removed from the RPSD Lock **Telco** and **Subscriber** ports and connected to the bypass connection block, which connects the line directly. See Figure 2-1 for the recommended cabling diagram.

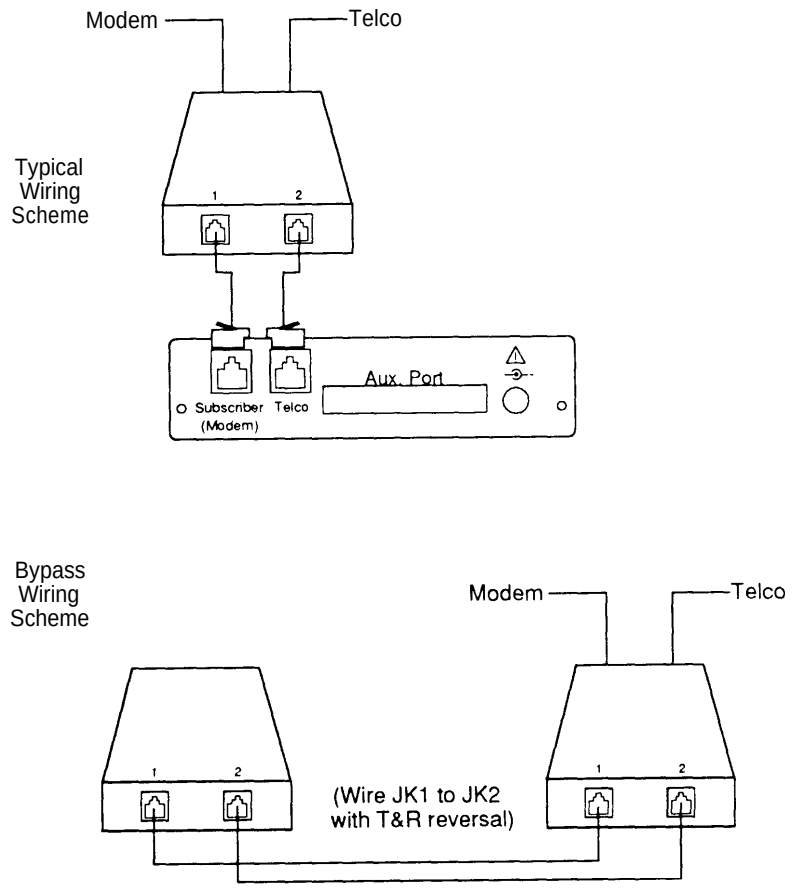


FIGURE 2-1
Bypass Connections

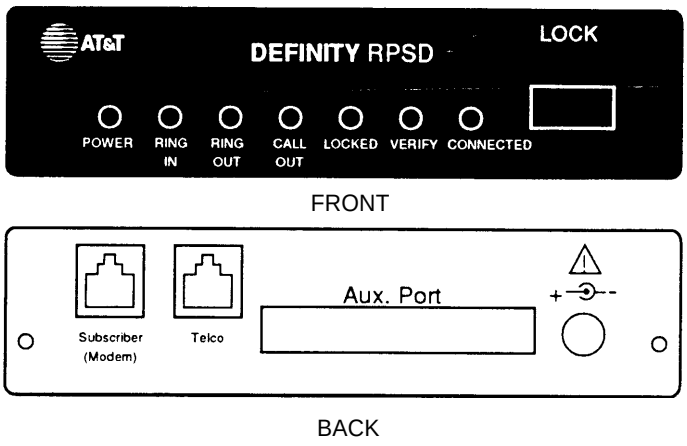


FIGURE 2-2
RPSD Lock

PBXs

AT&T supports RPSD use on the following types of PBXs:

- System 75 (R1V2, R1V3)
- System 85 (R1V1, R1V2, R2V1, R2V2, R2V3, R2V4)
- DEFINITY Generic 1 (all models)
- DEFINITY Generic 2 (all models)
- Dimension® PBX

To install the RPSD Lock you must locate the CO line used for RMATS service. This will usually be in a punch block confguration, but may be set up in a number of different ways, including an RJ11 adaptation or a multiple pair gang plug.

Whatever the situation, if one is not already present, install an RJ11 block on the tip and ring pair of the CO line that provides remote maintenance and administration service. The RJ11 block makes connection to the Telco port on the RPSD Lock easier and also facilitates any subsequent service.

The customer must call the technical support center to find out which channel is used for RMATS service. This information is only given to customers.

Other

Other dial-up port applications may be supported. To install an RPSD Lock device for these applications, locate the CO line used to service that port and install the Lock as you would for the remote maintenance and administration application.

Modems

The RPSD Lock works with any modem that may be used with the PBX. Similarly, the RPSD Key works with any modem that may be used with a terminal. Generally it is assumed that the modems in use are AT&T DATAPHONE® II 212 or 2224 modems.

RPSD Lock or Key Administration Terminal

The administration terminals for both Lock and Key are customer supplied. Any administration terminal for the RPSD Lock or for the RPSD Key must meet the following requirements:

- Asynchronous
- Full or half-duplex
- Standard RS-232 interface for connection to a DCE interface
- Any baud rate in the range 300-19.2K
- Any word size and parity

Connect the administration terminal to the Aux. Port of the RPSD Lock or Key via a standard RS-232 cable. Cabling is not supplied. The Aux. Port is the same port used if a printer is installed. You may wish to install a switch to make changing the Aux. Port connection easier.

The terminal should be initially set to 9600 baud and 8 bits, no parity. These are the factory default settings of the Lock and the Key. These parameters may subsequently be changed on both Lock, Key, and administration terminals.

RPSD Lock Administration Printer

The RPSD Lock requires a serial printer with XON/XOFF flow control.

Connect the printer to the Aux. Port of the RPSD Lock. Cabling is not supplied. This is the same port used by the administration terminal. You may wish to install a switch to make changing the Aux. Port connection easier.

RPSD Key

The RPSD Key is similar to the RPSD Lock in size and appearance. Like the RPSD Lock, the RPSD Key has seven LEDs on the front panel and four ports on the back panel. For a detailed description of the front panel LEDs, see Appendix B, *Front Panel LEDs.* The back panel ports are:

- an RJ11 port for the CO line, labeled **Telco**
- an RJ11 port for the modem connection, labeled **Subscriber**
- a female DB25 port for the terminal or printer, labeled **Aux. Port**
- a port for the power supply (supplied with the RPSD Key).

Install the RPSD Key between the Key user's CO line and modem.

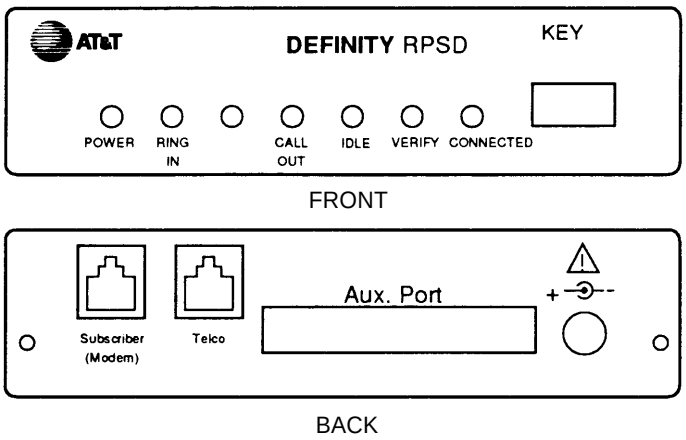


FIGURE 2-3
RPSD Key

Hardware Installation Procedures

It is absolutely required that the first step in installing the RPSD Lock device is to inform the INADS System Administrator at the local or central technical support center when the installation will take place and that the channel will be down at that time. This ensures that they will not attempt to administer the PBX while the channel is disconnected. Informing the technical support center may be done using Services Methods & Procedures, Talkline Case Number 910207.

INADS database updates *must be performed* for the INADS product connection call to be directed through a permanent AT&T RPSD Key. Without INADS updates, AT&T remote maintenance operations will not be able to access the customer's PBX or peripheral product.

Installing the RPSD Lock

Before installing the RPSD Lock, be certain that you have informed the technical support center of the date that the RMATS channel will be down for this installation. Figure 2-4 shows the most common configuration for the RPSD Lock.

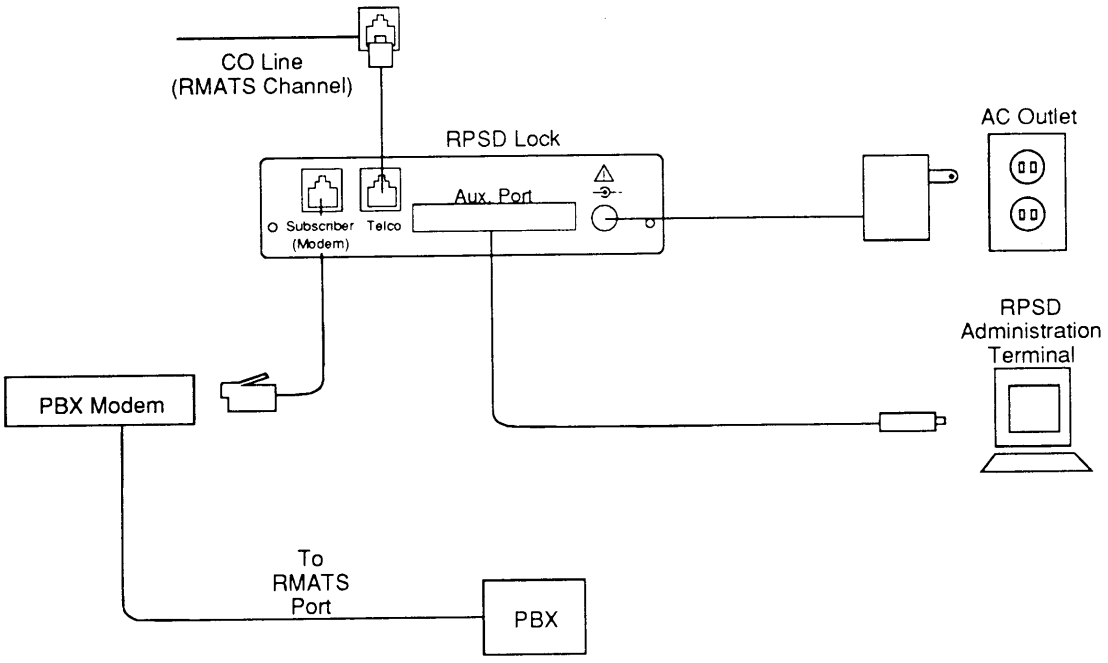


FIGURE 2-4
Common RPSD Lock Configuration

The Lock is installed between the CO line and the PBX modem. The modem location depends on the type of PBX. The modem is located:

- on the circuit pack for System 75 and DEFINITY Generic 1
- external to the PBX for System 85 and DEFINITY Generic 2

The RPSD Lock must also be connected to the administration terminal via the Aux. Port on the back of the RPSD Lock and powered from an AC outlet or Uninterruptible Power Supply (UPS).

On System 85 and DEFINITY Generic 2, the modems are external to the PBX. The modems should also be plugged in to the UPS since a power outage which results in either the RPSD Lock or the modem being inaccessible will result in the RMATS channel being inaccessible.

You will need the following components to install the RPSD Lock:

- RPSD Lock device
- the CO line assigned as the RMATS channel (on customer premises)
- the PBX modem (on customer premises)
- 6 position wire (length depends on local configuration)
- two modular connectors
- two DB25 connectors (male)
- RS-232 cable
- administration terminal
- AC outlet
- RPSD Lock power pack

Connecting the RPSD Lock to the CO Line

The following components are needed to connect the RPSD Lock device to the CO line:

- RPSD Lock
- the CO line assigned as the RMATS channel
- two modular connectors
- 6 position wire
- RJ11 connector (for the CO line)

To connect the RPSD Lock device to the CO line, use the following procedure:

1. The customer must contact the technical support center to get the port number for the RMATS channel.
2. Locate the CO line for the RMATS port where it connects to the modem.
3. Install an RJ11 receptacle on the CO line.
4. Connect a wired modular connector to the CO line.
5. Plug the modular connector on the other end of the wire into the **Telco** port on the back of the RPSD Lock.

Note: Bypass connectors are optional. See Figure 2-1.

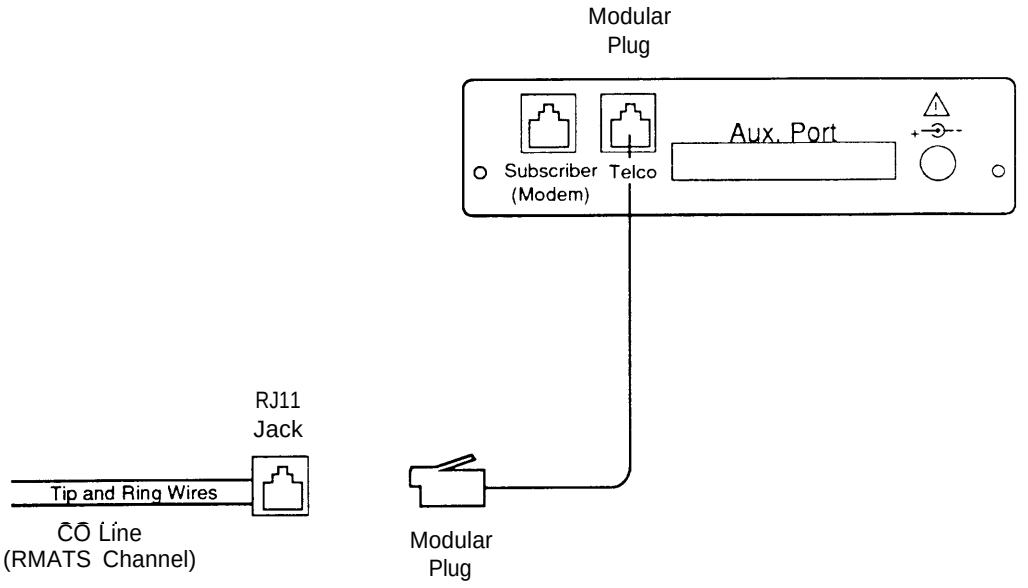


FIGURE 2-5
RPSD Lock to CO Line (RMATS Channel)

Connecting the RPSD Lock to the PBX Modem

The 212A modem has a DB25 input, so the connection to the RPSD Lock must be adapted to connect the tip and ring from a modular plug to a DB25. The two relevant pins for the 212A are pins 7 and 8. Pin 7 is the tip and pin 8 is the ring. Connectors must be adapted to make this connection. A detailed description of this connection is in this chapter in the section titled *Connecting the RPSD Lock to the Administration Terminal or Printer.* Table 2-1 provides the pinout for the Aux. Port. Further information, for either the 212A modem or any other modem, should be obtained from the documentation accompanying that modem.

The following components are needed to connect the RPSD Lock device to the PBX modem:

- RPSD Lock
- PBX modem assigned to the RMATS channel
- two modular connectors
- 6 position wire

To connect the RPSD Lock device to the PBX modem, use the following procedure:

1 Using either the 7-foot or the 14-foot cable with modular connectors on both ends which accompanied the Lock, insert one connector into the port on the back of the RPSD Lock device labeled **Subscriber.**

2 Insert the other modular connector into the appropriate port on the PBX modem.

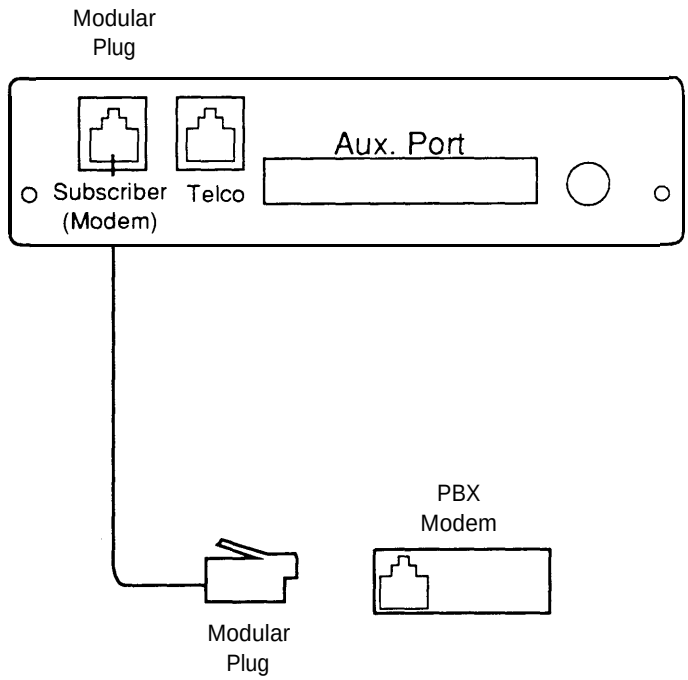


FIGURE 2-6
RPSD Lock to Modem

Connecting the RPSD Lock to the Administration Terminal or Printer

You will need the following hardware components to connect the RPSD Lock device to the administration terminal, printer, or modem:

- RPSD Lock device
- administration terminal or printer (printer is optional but recommended)
- one cable with one DB25 connector on one end and the appropriate connector for the serial printer or administration terminal on the other end
- RS-232 cable

Note: It is advised that you install an A/B switch if you are going to connect two pieces of equipment to the Aux. Port (meaning both a terminal and a printer). This will enable the administrator to change equipment without having to go to the trouble of disconnecting and reconnecting the plugs. Follow the directions for connecting a terminal to the Aux. Port to install the A/B switch.

To connect the RPSD Lock device to the administration terminal or printer, use the following procedure:

1. Using Table 2-1, make up a DB25 connector with EIA-RS232 cable for the Aux. Port of the RPSD Lock.
2. Make up the appropriate connector for the terminal or printer according to the pin descriptions in Table 2-1.
3. Connect the first DB25 connector to the Aux. Port on the back of the RPSD Lock.
4. Connect the other end of the cable you just made up to the terminal or printer, as appropriate.

Table 2-1 describes the pinout for the Aux. Port connection.

TABLE 2-1
Aux. Port, Terminal, and Printer Pinouts

RPSD Pin	Signal	To DTE Pin	To DCE Pin
1	Not used		
2	TXD (input)	2	3
3	RXD (output)	3	2
4	RTS (input)	4	6
5	CTS (output)	5	5
6	DSR (output)	6	4
7	Ground	7	7
8	CD (output)	8	20
9	Positive Test Voltage		
10-19	Not used		
20	DTR (input)	20	8
21	Not used		
22	RI (output)	22	22
23-25	Not used		

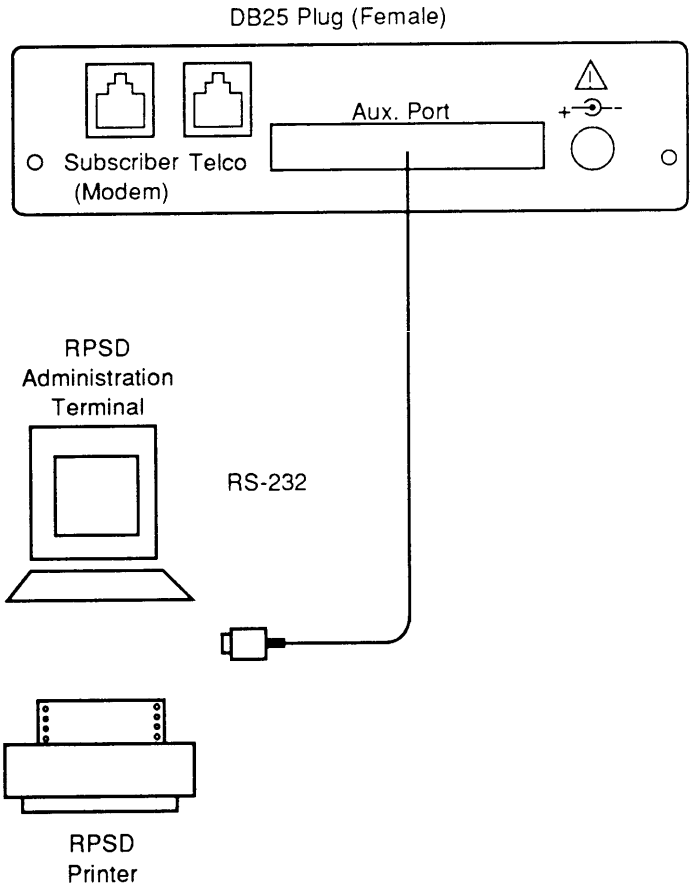


FIGURE 2-7
RPSD Lock to Administratlon Terminal or Printer

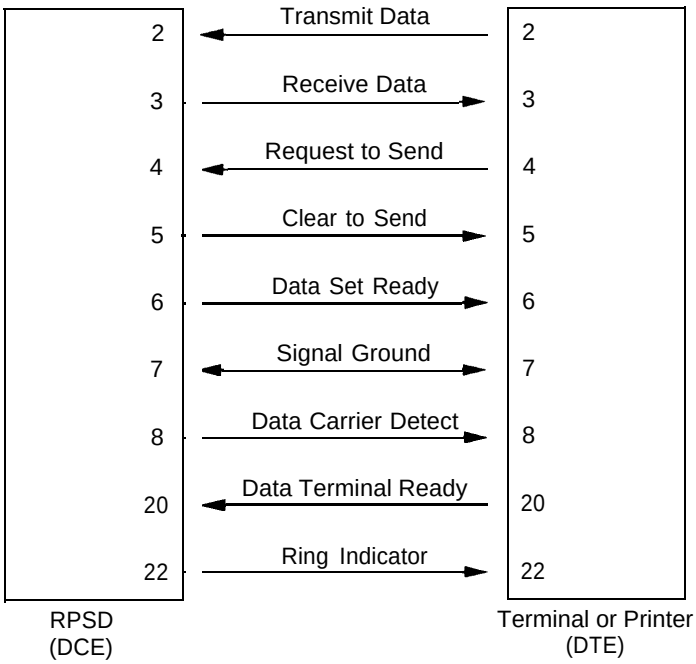


FIGURE 2-8
DB25 Connections From RPSD Lock or Key to Data Terminal Equipment

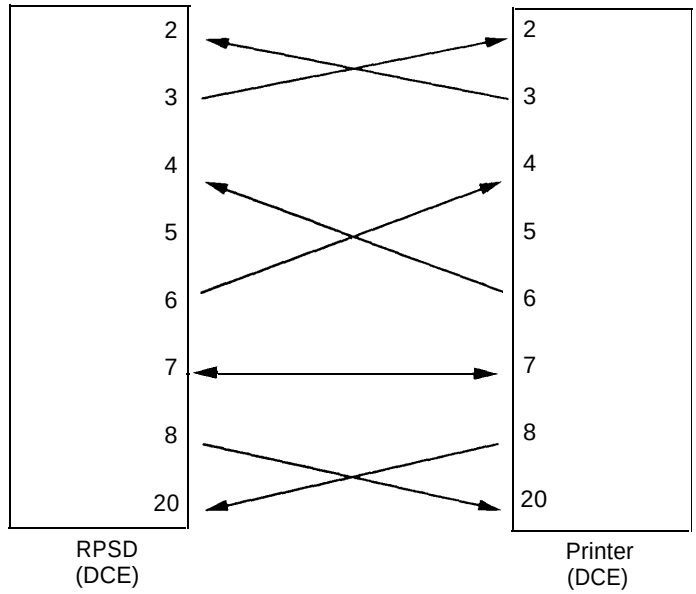


FIGURE 2-9
DB25 Connections From RPSD Lock or Key to Data Communications Equipment

Obtain further information for the specific terminal or printer in use from the documentation accompanying them.

Powering Up the RPSD Lock

To power the RPSD Lock, you need:

- the RPSD Lock Power Supply
- an AC wall outlet or an available AC outlet on the UPS. (With a System 85 or DEFINITY Generic 2, the modem is external to the PBX and should also be powered from the UPS.)

Plug one end of the power supply into the appropriate port on the back of the RPSD Lock and the other end into an AC wall outlet or an available outlet on the UPS. (See Figure 2-10.) The red Power LED on the front panel of the RPSD Lock will go on and remain on permanently while the other LEDs on the front panel of the RPSD Lock should blink three times and then settle into an Idle/Locked condition. If there is any failure of the LEDs (for example, they do not blink three times or the Power light does not come on), the Lock is defective and must be replaced. If you need to replace the Lock, see Chapter 5. A full explanation of the LEDs for both the RPSD Lock and Key is in Appendix B, *Front Panel LEDs.*

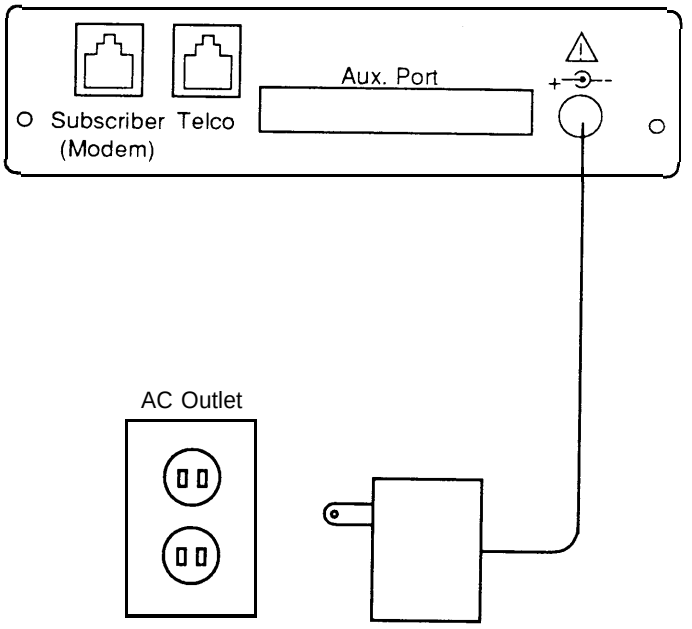


FIGURE 2-10
RPSD Lock Power Supply

Installing the RPSD Key

The RPSD Key is installed between the user's terminal and modem. To install an RPSD Key device, you need:

- RPSD Key
- Terminal
- Modem
- two modular connectors
- 6 position wire
- one RS-232 connectors
- one DB25 connector (male)
- RS-232 cable
- AC outlet

Note: The RPSD PMA may be used to provide Alarm Lead connections to alarming RPSD key failures. Refer to the Power Monitor Adapter documentation.

Connecting the RPSD Key to the Terminal

The RPSD Key is connected to the terminal via the Aux. Port on the back of the RPSD Key device and the terminal's RS-232 port. Obtain or make up a cable with the RS-232 wire, the RS-232 connector on one end, and the DB25 connector (male) on the other end. Connect the DB25 connector to the Aux. Port on the RPSD Key and connect the RS-232 connector to the RS-232 port on the back of the terminal.

See Table 2-1 for the pinout for the Aux. Port connection. The Aux. Port for the RPSD Key is connected in the same manner as the Aux .Port for the RPSD Lock. Figure 2-7 also applies equally to the Key as well as to the Lock.

The RPSD Key must be ordered by the customer separately from the RPSD Lock. In addition, all cabling and connectors must be ordered separately and are not supplied with the Key. Only the power pack comes with the Key.

Connecting the RPSD Key to the Modem

The RPSD Key is connected to the modem via the RJ11 port on the back of the Key device. Obtain or make up a cable using the 6 position wire and the two modular connectors. Plug one modular connector into the port on the back of the Key and the other into the appropriate port on the back of the modem.

Figure 2-6 applies equally to the RPSD Key as it does to the RPSD Lock.

Powering Up the RPSD Key

The RPSD Key may be in one of two conditions upon power-up: initialized or uninitialized. The response of the Key upon power-up is different depending on which condition it is in. Both conditions are described below.

To power the RPSD Key, you need:

- the RPSD Key Power Supply
- an AC wall outlet

Plug one end of the power supply into the appropriate port on the back of the RPSD Key and the other end into an AC wall outlet.

Power-Up Behavior of Initialized Key

With an initialized Key, the red Power LED on the front panel of the RPSD Key will go on and remain on permanently while the other LEDs on the front panel of the RPSD Key should blink three times and then settle into an Idle condition. If there is any failure of the LEDs (for example, they do not blink three times or the power light does not come on), the Key is defective and must be replaced.

Power-Up Behavior of Uninitialized Key

With an uninitialized Key, the left four LEDs will all light up upon power-up. If any other behavior occurs, there is a firmware error and the Key should be replaced.

Testing an Uninitialized Key

Test an RPSD Key that has not been initialized by connecting either a telephone or a terminal to the **Subscriber** port on the back panel of the Key, then dial the associated RPSD Lock, either directly via the telephone or via an application on the terminal. If the connection is good, the yellow Verify light comes on frost, followed by the green Connection light. This should occur in less than 30 seconds. The connection light will remain lit until the call is ended. If the connection fails, the red Idle light comes on.

Cables, Connectors, and Ports Table

Table 2-2 shows the cables, connectors, and ports required to install the RPSD system. This table includes optional connections as well as the basic configuration.

TABLE 2-2
Cables, Connectors, and Ports

Part	From	To
modular connector	PBX	RJ11 at modem
6 position wire	RJ11 at PBX	RJ11 at modem
modular connector[1]	Cable from PBX	modem
7 ft. cable with modular connector on each end	RPSD Lock	CO line or modem
14 ft. cable with modular connector on each end	RPSD Lock	CO line or modem
RJ11 wall jack[2]	RJ11 to RPSD	CO line
EIA-RS-232 cable[3]	DB25 at RPSD Lock	DB25 at admin. terminal or printer or A/B switch
DB25 connector[3]	RPSD Lock	Cable to admin. terminal or printer or A/B switch
DB25 connector[3]	Admin. terminal or printer or A/B switch	Cable to RPSD Lock

1 The 212A modem uses a DB25 connection. See Figures 2-8 and 2-9 for the details on making up the appropriate connector.

2 If RJ11 receptacle is not present on CO line, install one.

3 The RPSD Lock may be connected to the administration terminal, printer, or A/B switch (to allow connection to both the terminal and printer).

Software Components

The software for the RPSD system is contained within the hardware components and does not need to be loaded separately. Additionally, if you are not installing an RPSD Key or Keys, you need only set the date and time for the RPSD Lock and, in the case of multiple Locks, a Lock ID. If you are installing RPSD Keys, you will need to do some additional initialization on the Lock(s). The initialization procedures for RPSD Locks and RPSD Keys follow.

Initialization of the RPSD Lock is the responsibility of the RPSD system administrator. The technician who installs the RPSD Lock will test the system to make sure it is running properly, but will not set any additional parameters or make any changes to the system defaults.

Initializing the RPSD Lock

To initialize the RPSD Lock where no additional RPSD Keys are being installed, use the:

- Date Set command
- Clock Set command

If more than one RPSD Lock is being installed, use the ID Set command to allow identification of the Lock when viewing system activity messages. Each Lock's ID will be prepended to each system activity message.

If RPSD Keys are being installed, the Lock must be administered with the Add User command. This step is necessary to permit the Key to access the Lock. The Test User command should also be employed to make sure that the addition of the new Key worked properly.

The commands and their use are described in Chapter 3, *System Administrator Command Set.*

Note: The installer will not have an administration terminal to use for initialization. This must be supplied by the customer and must be ready for use when initialization takes place.

Aux. Port Settings

You will also need to set the link speed, character length, and parity on whichever equipment (administration terminal or printer) you have attached to the Aux. Port. The default for the Aux. Port is 9600 baud, 8 bit, no parity. See Chapter 3, *RPSD System Administration* for the use of the Set Communications Parameters command to change the default settings, if desired, on the RPSD Lock. See Chapter 4, *RPSD Key Use* for the use of the Set Communications Parameters command to change the default settings, if desired, on the RPSD Key.

Initializing an RPSD Key

Initialization of an RPSD Key involves both the Key and the RPSD Lock. On the Lock, the Key User ID in question must be added using the Add User command. See Chapter 3, *System Administrator Command Set* for the procedure for using the Add User command.

On the Key, the following commands are used for initializing the device:

- Set User ID
- Set Secret Key
- Sets Device Number
- Date Set
- Clock Set
- Set Log ID (optional)

All of these commands must be used when initializing the RPSD Key device. A description of the commands and the procedures for their use appear in Chapter 4, *RPSD Key Use.*

Note: The installer will not have an administration terminal to use for initialization. This must be supplied by the customer and must be ready for use when initialization takes place.

Test RPSD Lock Installation

The Self Check tests the health of the RPSD Lock. If the correct response is received when the test is run, the RPSD Lock is functioning properly.

To perform the Self Check, dial the RMATS channel from a touch-tone telephone. When the call is answered, you hear a short tone (indicating a connection to the RPSD Lock). Press *1* ✶ on the telephone pad.

If the response is 3 quick tones, followed by the RPSD Lock disconnecting, the Lock is functioning properly.

Finally, have the technical support center call the RMATS channel. If access is successful, the installation is working properly. If access is unsuccessful, refer to Chapter 5, *Troubleshooting.*

After a successful access of the port has shown the Lock to be working properly, try dialing out through the RMATS channel via the Lock. If you have trouble with making an outgoing call, the likeliest scenario is that the tip and ring leads are reversed. Reverse the current connection of the tip and ring leads from the CO line to the RPSD Lock and try dialing out again. A failure at this juncture indicates something is wrong with the Lock. See Chapter 5, *Troubleshooting.* If the Lock does not work properly, it must be replaced.

If all tests are passed successfully, installation is complete for the technician. Lock initialization can now be performed by the RPSD system administrator.

3 RPSD System Administration

RPSD System Administration

The RPSD Lock device prevents unauthorized access to the RMATS channel on your PBX. In administering the RPSD, keep in mind that access via telephone lines is not the only means of breaching the security of your system. A system can be breached, for example, by physically intercepting lines and adding unauthorized equipment. RPSD users may take many actions to enhance overall telecommunications security. These actions include, but are not limited to, providing physical security for RPSD installation sites (locked rooms, cabinets, etc.) and wiring room sites. The RPSD System Activity Log should be monitored for patterns of activity, such as repeated denied call attempts. Contact your computer security group for assistance.

In addition, you should save the seed value for the authentication algorithm in a protected place, in case equipment needs to be replaced at a later date.

Note: **The Remote Port Security Device, if properly installed and managed, clearly provides a significant and substantial barrier to unauthorized access to a dial up communication port.**

Note that the Remote Port Security Device cannot be assumed to be impregnable, but needs to be viewed as an important addition to the tools and measures used by system managers to prevent unauthorized access to dial up ports.

Time of Day Access

The RPSD Lock device can be administered to prevent access from a specified Key or from all Keys during specified times of the day. You may, as an example, instruct the Lock to block all attempts at access from 18:00 hours (using the 24 hour clock format) until 08:00 hours for user X. You might, for example, use this feature to prevent any administration of the PBX from being performed while a system administrator is not present to oversee the administration.

The default setting is no blockage of access for any Key user at any time.

The administerable parameters are time, date, and user ID. Up to 14 separate time restrictions (periods of no access) maybe set for any one user ID. Time restrictions may also be overlapped.

To specify Time of Day Access, see the Change Restriction, List Restrictions, and User Restrictions commands in the *System Administrator Command Set* section of this chapter.

System Activity Log

The System Activity Log retains a log history of the last 60 status messages generated by the RPSD Lock. As a new message is generated, the oldest message in the buffer is deleted. The most recent twenty messages are sent to the RPSD Lock administration terminal or printer and displayed or printed in real-time. That is, the oldest message scrolls off the screen on the administration terminal as the new message is added at the bottom. With the printer the new message is simply printed at the bottom of the page as it is received from the RPSD Lock. The printer can therefore be used to create a more permanent, hard copy record of these messages.

The messages are numbered consecutively from 000 to 999. If a printer is used, any breaks in this sequence indicate an interruption of log printing.

The following is a sample log history:

```
--- Log History ---
JPLock01  531  07/12/90  13:23:18  KEY20 -- User Removed OK
JPLock01  532  07/12/90  13:23:51  KEY19 -- User Added OK
JPLock01  533  07/12/90  13:24:12  KEY20 -- User Added OK
JPLock01  534  07/12/90  13:26:51  Call Received
JPLock01  535  07/12/90  13:26:59  Attempt by KEY20 [#4321] Failed (4) Blocked User
JPLock01  536  07/12/90  13:27:00  KEY20 [#4321] Disconnected
JPLock01  537  07/12/90  13:27:06  AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01  538  07/12/90  13:27:45  KEY20 -- User Unblocked OK --
JPLock01  539  07/12/90  13:27:55  Call Received
JPLock01  540  07/12/90  13:28:04  KEY20 [#4321] Connected
JPLock01  541  07/12/90  13:32:13  KEY20 [#4321] Disconnected
JPLock01  542  07/12/90  13:32:15  AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01  543  07/12/90  13:32:50  Call Received
JPLock01  544  07/12/90  13:33:02  Attempt by KEY20 [#8765] Failed
                                   (5) Invalid Response
JPLock01 545 07/12/90  13:32:12  KEY20 [#8765] Disconnected
JPLock01 546 07/12/90  13:32:17  AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01 547 07/12/90  13:34:59  Date Changed OK
JPLock01 548 07/12/90  13:43:55  Call Received
JPLock01 549 07/12/90  13:44:04  KEY20 [#4321] Connected
JPLock01 550 07/12/90  13:49:13  KEY20 [#4321] Disconnected

>
```

The fields of the System Activity Log entries are:

Log ID provides the ID of the Lock associated with the system activity message.

Sequence Number numbers each message in sequence. The sequence goes from 000 to999 and then restarts at 000.

Date provides the date of the message.

Time provides the time the message was generated in 24 hour clock format.

Message contains the status message.

In the example, **KEY20** is a user ID. Where the user ID is followed by information in square brackets, the information is the RPSD User ID number (as in the fifth message in the sample screen above). Users can be assigned the same user ID; the user ID number provides a second means of identifying the calling party.

Additionally, calls may generate an access failure form of the status message. This type of message tells you the reason for an access failure. There are nine such messages, as listed in Table 3-1.

TABLE 3-1
Access Failure Messages

Code Number	Status Message	Meaning
1	No RPSD/Key Detected	No RPSD Key was detected on the caller's line.
2	No Response	No response was returned from the RPSD Key when the RPSD Lock sent the challenge.
3	Invalid User ID	The RPSD Key user's ID is not in the table of users on the RPSD Lock.
4	Blocked User	The RPSD Key user was deliberately blocked by the administrator on the RPSD Lock.
5	Invalid Response	The RPSD Key responded to the RPSD Lock's challenge, but the response was incorrect.
6	Outgoing Call	An outgoing call is being placed. The Lock forces a disconnect in order to make an outgoing call
7	Ring - No Answer	The RPSD Lock rang the modem, but the modem did not answer the call.
8	Force Disconnect	A Force Disconnect command was issued to the RPSD Lock.
9	Time Restriction	The call was received during a time of day when the Lock is restricted from taking any calls from that user.

This table is repeated in Chapter 5, *Troubleshooting,* along with the actions to be taken in response to the messages.

Single Point Administration

A single administration terminal or printer can be used to administer multiple Locks. To do so, you will need to either administer the Locks from tty ports via the UNIX® Operating System, or you can use, in the case of printers, a printer sharing device.

Where multiple Locks are used, a Lock ID should be assigned to each Lock. The ID will be appended to any messages generated so that the source can be identified. To assign an ID to a Lock, use the ID Set command described in the *System Administrator Command Set* section of this chapter.

Enable/Disable (Block) AT&T and Other Key Users

You may wish to block one or more Key users from accessing the RPSD Lock. This can be done by using the Block User command. You do not need to inform the Key user that the Key has been blocked. If a blocked Key user attempts access, the RPSD Lock will block the attempt and send a message to Lock administration terminal or printer explaining the cause of the failed access. An example of the message follows:

```
JPLock01 334 07/24/90 09:33:01 Attempt by KEY20 [#1234] Failed (4) Blocked User
```

The following message is sent to the Key user's administration terminal:

```
KEY20 07/24/90 09:33:01 Attempt Failed (4) Blocked User
```

To block a Key user or Key users, use the Block User command described in the *System Administrator Command Set* section of this chapter.

Force Connect/Disconnect

The RPSD Lock can be forced to connect an incoming call from any source or to disconnect a call in progress. A connection can be forced or a call disconnected whether the caller is using an RPSD Key or not.

To use Force Connect or Force Disconnect, see the Force Connect and Force Disconnect commands described in the *System Administrator Command Set* section of this chapter.

Note: **Use of Force Connect command bypasses RPSD Lock security. Use only with extreme caution!**

Authorized Keys

You may have up to twenty-five RPSD Key user IDs on the RPSD Lock. Ten RPSD Key user IDs are reserved as permanent for AT&T personnel to administer and maintain the PBX, peripheral, or adjunct via the RMATS port. These user IDs cannot be deleted. The permanent user IDs can, however, be blocked by issuing a block command on the RPSD Lock, or by time restrictions if they attempt access during a restricted time.

The ten permanent AT&T RPSD Key user IDs are:

- ATT-INADS1
- ATT-INADS2
- ATT-INADS3
- ATT-INADS4
- ATT-TSC001
- ATT-TSC002
- ATT-PECC01
- ATT-LABS01
- ATT-LABS02
- ATT-LABS03

The ATT-INADS1, ATT-INADS2, ATT-INADS3, and ATT-INADS4 user IDs are for users of INADS systems. ATT-TSC001 and ATT-TSC002 are key users and Engineers at the Technical Services Center in Englewood, CO (all products). ATT-PECC01 is the Tier 3 location at the Denver Works Factory. ATT-LABS01 is provided for the use of Bell Laboratories field support for System 85 and DEFINITY Generic 2. ATT-LABS02 is for Bell Laboratories field support for System 75 and DEFINITY Generic 1. ATT-LABS03 is for Bell Laboratories field support for AUDIX®.

In addition to the ten AT&T Key user IDs, there is support for up to fifteen additional user IDs for your own applications. These can be added to or removed from the RPSD Lock by the Lock administrator as necessary. They can also be blocked or restricted in the same ways as the permanent user IDs. Each of the non-permanent user IDs requires a separate RPSD Key device. Please note, however, that a single RPSD Key can be used to access multiple Locks.

See the Add User command for the procedure for adding users and the Remove User command for the procedure for removing users, both described in the *System Administrator Command Set* section of this chapter.

RPSD System Administrator Command Set

This section describes the commands available on the RPSD Lock and their syntax. The procedures in which the commands are used have been described earlier in this chapter. This material is provided as a quick reference.

Also described in this section is the method of accessing the help screens that accompany the Menu of Commands.

The Menu of Commands available to the system administrator is as follows:

```
- Menu of Commands ---

A  - Add User              LH - Log History        D  - Date Set
B  - Block User            AH - Access History     C  - Clock Set
U  - Unblock User          FH - Failure History    I  - ID Set
T  - Test User                                     SC - Set Comms.  Params
R  - Remove User           ST - Status Display
L  - List User Table       LS - List Statistics
                           RS - Reset Statistics
CR - Change  Restriction
LR - List  Restrictions    FC - Force Connect
UR - User  Restrictions    FD - Force Disconnect

 -- For Help Type '?' Followed By Command --

>
```

Note: The Menu of Commands is available at any time by pressing [RETURN] on the RPSD administration terminal. The commands are not case sensitive.

A - Add User

Syntax:

a <user_id>,[secret_key] [RETURN]

Adds an RPSD Key user to the list of users on the RPSD Lock. The total number of RPSD Key users at any one time is limited to twenty-five. Of the twenty-five users, ten are permanent users and cannot be removed.

The **[secret_key]** can be specified by the system administrator or randomly assigned by the Lock. If this field is omitted, it is randomly generated by the Lock.

Optionally, a single Key can be used to access multiple Locks. This is done by entering the **[secret_key]** information when adding that Key. The same **[secret_key]** information is then used when adding that Key to other Locks. The information is then used to generate the test responce. The secret key chosen by the administrator is the key information to be added to the RPSD Key. If this option is not used, the RPSD Lock generates the secret key information randomly.

In any situation where the RPSD Key is already initialized (meaning from another Lock), the existing **[secret_key]** should be specified when adding the user.

In the syntax line above, **a** is the command and **<user_id>** is a unique identifier selected by the administrator. The user ID may be up to ten characters long and is not case sensitive. The **[secret_key]** is the pre-defined number of up to 14 hexadecimal digits used for administering multiple Locks with a single Key.

The RPSD Lock returns secret information and a test response when a user is added. This information is then used to initialize the RPSD Key, so make sure to note the information. Also, be careful to maintain the security of the information. The user ID will always be associated with that particular Key and its secret information and test response. A new RPSD Key must be initialized after the addition has been made to the Lock in order to gain access. See Chapter 2, *Initializing an RPSD Key* for the procedure.

Sample Command and Response Without Optional Secret Key:

```
> a KEY20
JPLock01 443 08/12/90 13:14:22 KEY20 -- User Added OK --
>
Enter this secret key into the RPSD/Key unit
F37B 159D 6ABE 3E

Test Response is: 8119704

>
```

Sample Command and Response With Optional Secret Key:

```
> a KEY20, F37B159D6ABE3E
JPLock02 444 08/14/90 01:57:43 KEY21 -- User Added OK --
>
Enter this secret key into the RPSD/Key unit
F37B 159D  6ABE 3E

Test Response is: 4296425

>
```

B - Block User

Syntax:

b <user_id> [RETURN]

Blocks an RPSD Key user from access to the RMATS channel. Both permanent and non-permanent users may be blocked. In the syntax line above, **b** is the command and **<user_id>** is the user ID. To determine whether a user is already blocked, or to check the user IDs, use the List User Table command. See *List User Table* in this section.

Sample Command and Response:

```
> b KEY20
JPLock01 445 08/12/90 13:14:22 KEY20 -- User Blocked OK --
>
```

U - Unblock User

Syntax:

u <user_id> [RETURN]

Removes the block placed on an RPSD Key user's access to the RPSD Lock. Both permanent and non-permanent users may be unblocked. In the syntax line above, **u** is the command and **<user_id>** is the user ID. To determine whether a user is blocked, or to check the user IDs, use the List User Table command. See *List User Table* in this section.

Sample Command and Response:

```
> u KEY20
JPLock01 446 08/12/90 13:19:22 KEY20 -- User Unblocked OK --
>
```

T - Test User

Syntax:

t <user_id> [RETURN]

Returns a seven-digit, pseudo-random code to be matched by a code from the specified RPSD Key user. This is used to check whether the RPSD Key has been seeded properly with the secret information. The Test Response on the RPSD Key is obtained by using the List User Information command on the RPSD Key user's terminal. See Chapter 4, *RPSD Key Use* for details on the Key user command.

In the syntax line above, **t** is the command and **<user_id>** is the user ID. To check the user IDs, use the List User Table command. See *List User Table* in this section.

Sample Command and Response:

```
> t KEY20
Test Response is: 8119704
>
```

R - Remove User

Syntax:

r <user_id> [RETURN]

Removes a user from the user table. This prevents that user from accessing the RPSD Lock or the attendant RMATS channel. The ten permanent AT&T users cannot be removed. If the user is added again, the user must reinitialize the RPSD Key with new secret information. The user could also be re-entered if the secret key information was retained. In such a case, the Key would not need to be reinitialized. See Chapter 2, *Initializing an RPSD Key* for the procedure.

In the syntax line above, **r** is the command and **<user_id>** is the user ID. When a Remove User command is issued, the RPSD Lock requests a *y* or an *n* as confirmation of the removal. To check the user IDs or whether a user is permanent, use the List User Table command. See *List User Table* in this section.

Sample Command and Response:

```
> r KEY20
Are You Sure (Y/N) ? y
JPLock01 447 08/14/90 14:20:43 KEY20 -- User Removed OK --
>
```

L - List User Table

Syntax:

- l [RETURN]
  or
- l **<full_or_partial_user_id>** [RETURN]

The List User Table command lists information regarding all users if no user ID is specified. The command lists information regarding a specified user if the full user ID is given, or all users beginning with whichever characters are used, meaning it will list the information for all user IDs beginning with the letter “a” if you enter / *a* .

First Sample Command and Response:

The following is a sample of the output returned by using the first syntax example, which lists all users.

```
> l

User ID      Blocked?     Perm?     Restriction (s)
ATT-INADS1                  P       A B
ATT-INADS2                  P       B
ATT-INADS3                  P
ATT-INADS4                  P
ATT-NTSO01                  P
ATT-PECC01                  P
ATT-NCSC01                  P
ATT-TIER3G                  P
ATT-LABS01                  P
ATT-LABS02                  P
KEY11                               A
KEY12           B                   C
KEY13           B                   D
KEY14                               A B
KEY15                               D
KEY16                               A
KEY17                               A
KEY18           B                   A
KEY19                               A
KEY20                               A
 -- End of List --
```

The fields of the List User Table screen are:

User ID Provides the user ID.

Blocked? States whether a Block command has been issued for that user. The default is no block. If a user is not blocked, the field is left blank. Blocks can be issued on both permanent and non-permanent users.

Permanent? Tells whether the user is one of the AT&T permanent users. If the user is not permanent, the field is left blank.

Restrictions Provides the code letter for any time restrictions that have been placed on the user. The default is no restrictions. Restrictions can be placed on both permanent and non-permanent users. To find the meaning for the restrictions codes, use the List Restrictions command, which is explained in this section.

Second Sample Command and Response:

The following is a sample of the output returned by using the second syntax example, which lists only specified users.

```
> 1 KEY20

User ID      Blocked?     Perm?     Restriction(s)
KEY20                              A
-- End of List --
```

The fields of this screen are explained in the first sample, above.

Third Sample Command and Response:

The following is a sample of the output returned by using the second syntax example, which lists all users beginning with the same characters.

```
> l KEY

User ID       Blocked?      Perm?      Restriction(s)
KEY11                                  A
KEY12             B                    C
KEY13             B                    D
KEY14                                  A B
KEY15                                  D
KEY16                                  A
KEY17                                  A
KEY18             B                    A
KEY19                                  A
KEY20                                  A
 -- End of List --
```

The fields of this screen are explained in the first sample, above.

CR - Change Restriction

Syntax:

cr <restr_id,start(hh:mm),end(hh:mm),day_no.> [RETURN]

The Change Restriction command is used to set the list of time restrictions that may be placed on a user or users. Time restrictions block access to the RMATS channel for a specified portion of time on a specified day or days. That is, you can block access to the channel, for example, from 10:00AM to 3:00PM on Saturdays and Sundays.

The Change Restriction command is used to set the parameters of the restriction and to define to which code letter (restr_id) the restriction applies. The code is then applied to a specific user or users using the User Restriction command, which is explained in this section. To see which codes correspond to which restrictions, use the List Restrictions command, which is explained in this section.

Note: To set overnight time restrictions you will need to set two separate restrictions from time X until midnight (24:00) on one day and then from time 00:00 to time Y on the next day. For example, if you want to restrict access from 8:00PM on a Thursday until 8:00AM on a Friday, you will need to restrict access from 20:00 on Thursday until 24:00 on Thursday and then restrict access from 00:00 on Friday until 08:00 on Friday. You will also, when you use the User Restrictions command, need to assign both of these restrictions to the users you wish to restrict to prevent overnight access. The first sample below follows this example.

To clear the restrictions from a restriction ID (restr_id), the syntax is

cr <restr_id>, clear

Sample Command and Response:

```
> cr A,20:00,24:00,4
JPLock01 191 08/16/90 10:20:43 Restr. 'A' Set
> cr B,00:00,08:00,5
JPLock01 192 08/16/90 10:21:23 Restr. 'B' Set
>
```

The options for the Change Restriction command are:

restr_id A single character from A-N (a total of 14 possible separate restrictions) used as a code to identify a time restriction. The code is then assigned to the users you wish to restrict for that period using the User Restrictions command described in this section.

start(hh:mm) The beginning time of the restriction in 24 hour clock format. In the sample above, the beginning time for restriction IDA is **20:00,** which is 8:00PM.

Note: You must use the colon (:) as a separator between the hours and minutes or the entry will not work. You must also use a leading zero (0) to enter any time that is less than 10:00, for example, 08:00.

end(hh:mm) The ending time of the restriction in 24 hour clock format. In the sample above, the ending time is **24:00,** which is 12:00AM.

Note: You must use the colon (:) as a separator between the hours and minutes or the entry will not work. You must also use a zero (0) to enter any time that is less than 10:00, for example, 08:00.

day_no. The day or days of the week on which the restriction will be in effect. You enter the day(s) in ascending order, in any combination (for example, 367), as a number(s) from 1-7 as follows:

- 1 = Monday
- 2 = Tuesday
- 3 = Wednesday
- 4 = Thursday
- 5 = Friday
- 6 = Saturday
- 7 = Sunday

In the sample above, the days on which the restriction takes effect are Thursday and Friday.

LR - List Restrictions

Syntax:

lr [RETURN]

or

lr <restr_id> [RETURN]

The List Restrictions command is used to list the time restrictions that have been administered. Up to 14 separate restrictions maybe created (A-N).

The first syntax example above will list the time restrictions for all restriction IDs A to N. In the second example, entering a letter for the specific restriction ID will yield the time restrictions for that restriction ID only.

Sample Command and Response:

```
> lr

Restriction ID     Start Time     End Time     Days of the Week
       A             18:00          24:00      Sat, Sun
       B             12:00          15:00      Sat, Sun
       C             16:00          20:00      Mon
       D             01:00          08:00      Mon, Tues, Wed, Thu, Fri
       E             00:00          09:00      Thu
-- End of List --

>
```

The fields of the List Restrictions screen are:

Restriction ID	The letter code from A to N to be used to assign a restriction or set of restrictions to a user or users. To assign restrictions, see the User Restrictions command in this section.
Start Time	The time of day, in 24 hour clock format, when the restriction begins.
End Time	The time of day, in 24 hour clock format, when the restriction ends.
Days of the Week	The days on which the restricted times take effect.

UR - User Restrictions

Syntax:

ur <full_or_partial_user_id, restr_id(s)> [RETURN]

The User Restrictions command is used to assign time restrictions to a user or set of users. The command assigns restrictions to a specified user if the full user ID is given, or all users beginning with whichever characters are used, meaning it will assign the restriction(s) to all user IDs beginning with the letter "a" if you enter *ur a, <restr_id(s)>.* It will take as many restriction IDs as you enter, up to the full 14 from A to N.

To clear a user(s) restrictions, the syntax is

ur <full_or_partial_user_id, restr_id(s)>, clear

First Sample Command and Response:

```
> ur KEY20, abc
193 08/16/90 11:33:21 KEY20 Assigned Restr. 'ABC'
```

To check that the restrictions were assigned as desired, use the List User Table command described in this section. To check the parameters of the restriction IDs, use the List Restrictions command described in this section.

Second Sample Command and Response:

```
> ur KEY, abc
194 08/16/90 11:36:21 Restr.  KEY11 Assigned Restr.  'ABC'
195 08/16/90 11:36:23 Restr.  KEY12 Assigned Restr.  'ABC'
196 08/16/90 11:36:25 Restr.  KEY13 Assigned Restr.  'ABC'
197 08/16/90 11:36:27 Restr.  KEY14 Assigned Restr.  'ABC'
198 08/16/90 11:36:29 Restr.  KEY15 Assigned Restr.  'ABC'
199 08/16/90 11:36:31 Restr.  KEY16 Assigned Restr.  'ABC'
200 08/16/90 11:36:33 Restr.  KEY17 Assigned Restr.  'ABC'
201 08/16/90 11:36:35 Restr.  KEY18 Assigned Restr.  'ABC'
202 08/16/90 11:36:37 Restr.  KEY19 Assigned Restr.  'ABC'
203 08/16/90 11:36:39 Restr.  KEY20 Assigned Restr.  'ABC'
```

To check that the restrictions were assigned as desired, use the List User Table command described in this section. To check the parameters of the restriction IDs, use the List Restrictions command described in this section.

LH - Log History

Syntax:

lh [RETURN]

Displays the last sixty messages in the System Activity Log. The messages are displayed twenty to a page with a total of three pages. **– More to Come –** appears at the bottom of the first two pages and **– End of List –** appears at the bottom of the last (third) page. Press [RETURN] to move from the first to the second or second to the third page and press [RETURN] to return to the menu of commands when you have reached the third page.

Note: If AT&T Key users are undergoing unexplained access failures or are failing for reasons 2, 3, or 5 of Table 3-1, report it to AT&T.

A sample version of the display follows.

```
> lh

--- Log History ---
JPLock01 531 07/12/90 13:23:18 KEY20 -- User Removed OK
JPLock01 532 07/12/90 13:23:51 KEY19 -- User Added OK
JPLock01 533 07/12/90 13:24:12 KEY20 -- User Added OK
JPLock01 534 07/12/90 13:26:51 Call Received
JPLock01 535 07/12/90 13:26:59 Attempt by KEY20 [#4321] Failed (4) Blocked
                               User
JPLock01 536 07/12/90 13:27:00 KEY20 [#4321] Disconnected
JPLock01 537 07/12/90 13:27:06 AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01 538 07/12/90 13:27:45 KEY20 -- User Unblocked OK --
JPLock01 539 07/12/90 13:27:55 Call Received
JPLock01 540 07/12/90 13:28:04 KEY20 [#4321] Connected
JPLock01 541 07/12/90 13:32:13 KEY20 [#4321] Disconnected
JPLock01 542 07/12/90 13:32:15 AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01 543 07/12/90 13:32:50 Call Received
JPLock01 544 07/12/90 13:33:02 Attempt by KEY20 [#8765] Failed
                               (5) Invalid Response
JPLock01 545 07/12/90 13:32:12 KEY20 [#8765] Disconnected
JPLock01 546 07/12/90 13:32:17 AT&T RPSD Lock - V1.0 - Idle/Locked
JPLock01 547 07/12/90 13:34:59 Date Changed OK
JPLock01 548 07/12/90 13:43:55 Call Received
JPLock01 549 07/12/90 13:44:04 KEY20 [#4321] Connected
JPLock01 550 07/12/90 13:49:13 KEY20 [#4321] Disconnected

-- More to Come --
>
```

The fields of the Log History screen are:

Log ID	provides the ID of the Lock associated with the system activity message.
Sequence Number	numbers each message in sequence. The sequence goes from 000 to 999 and then restarts at 000.
Date	provides the date of the message.
Time	provides the time the message is generated in 24 hour clock format.
Message	contains the status message.

In the example, **KEY20** is a user ID. Where the user ID is followed by information in square brackets, the information is the RPSD User ID number.

Additionally, calls may generate an alarm form of the status message. This type of message tells you the reason for a call failure. Alarms are identified by a number from 1 to 9 in parentheses. Table 3-1 describes these alarms.

AH - Access History

Syntax:

ah [RETURN]

The Access History command displays details regarding the last twenty accesses of the RMATS channel for both incoming and outgoing calls. The command takes no arguments.

Sample Command and Response:

```
> ah

---Access  History  ---
  Date      Time       User ID       Device #     Duration
08/16/90  13:08:51    ATT-INADS1     12345         0: 0:20
08/16/90  13:09:42    ATT-INADS1     12345         1:20:33
08/16/90  15:12:06    <Outdial>                    0: 5:08
08/16/90  15:20:51    <Outdial>                    0: 2:14
08/16/90  15:24:19    ATT-INADS2     72333         0: 8:46
08/16/90  15:48:01    ATT-INADS2     72333         0: 1:59
08/16/90  15:58:23    KEY11          82545         0: 7:22
08/16/90  16:08:51    KEY11          82545         0: 3:20
08/17/90  08:08:18    <Outdial>                    0: 9:49
08/17/90  08:28:13    ATT-INADS1     12345         0:28:11
08/17/90  08:58:37    ATT-INADS1     12345         0: 1:02
08/17/90  14:03:32    <Outdial>                    0: 6:15
08/17/90  14:09:53    ATT-INADS1     12345         0: 3:38
08/17/90  14:18:10    KEY16          96549         0:24:22
08/17/90  14:44:44    KEY16          96549         0: 0:58
08/18/90  09:08:51    KEY12          37827         0:10:04
08/18/90  09:21:48    KEY12          37827         0: 0:47
08/18/90  11:31:25    <Outdial>                    0:13:03
08/18/90  11:48:11    <Outdial>                    0:29:34
08/18/90  13:28:31    ATT-INADS1     12345         2:56:05

>
```

The fields of the Access History screen are:

Date — Date on which the access took place.

Time — Time at which the access call came in.

User ID — The user ID of the RPSD Key used to access the channel. If the call was an outgoing call on the channel, no user ID is displayed but the call is identified as **<Outdial>** .

Device # — The device number of the RPSD Key used to access the channel. The device number is a number assigned to the Key by the Key user at initialization. No device number appears for an outgoing call.

Duration — The length of time that the call was corrected in hours, minutes, and seconds.

FH - Failure History

Syntax:

fh [RETURN]

The Failure History command displays a log of the last twenty failed access attempts and the details of those calls. The command takes no arguments.

Sample Command and Response:

```
> fh

 -- Failure History ---
  Date     Time       User ID      Device #    Reason
06/04/90  13:08:51    ATT-INADS1     12345      3
06/15/90  13:09:42    ATT-INADS1     12345      4
07/01/90  15:12:06    KEY20          76347      1
07/03/90  15:20:51    KEY20          76347      8
07/09/90  15:24:19    ATT-INADS2     72333      7
07/28/90  15:48:01    ATT-INADS2     72333      5
08/02/90  15:58:23    KEY11          82545      9
08/08/90  16:08:51    KEY11          82545      2
08/09/90  08:08:18    ATT-INADS4     66600      6
08/09/90  08:28:13    ATT-INADS1     12345      5
08/09/90  08:58:37    ATT-INADS1     12345      8
08/12/90  14:03:32    KEY16          45458      2
08/12/90  14:09:53    ATT-INADS1     12345      9
08/12/90  14:18:10    KEY16          96549      9
08/12/90  14:44:44    KEY16          96549      4
08/16/90  09:08:51    KEY12          37827      4
08/16/90  09:21:48    KEY12          37827      4
08/16/90  11:31:25    ATT-NCSC01     87654      5
08/16/90  11:48:11    ATT-NCSC01     87654      5
08/16/90  13:28:31    ATT-INADS1     12345      5

>
```

The fields of the Failure History screen are:

Date Date on which the access failure took place.

Time Time at which the access attempt failed.

User ID The user ID of the RPSD Key used to attempt to access the channel.

Device # The device number of the RPSD Key used to attempt to access the channel. The device number is a number assigned to the Key by the Key user at initialization.

Reason The call access failure code. The codes and their explanations are provided in Table 3-1. The LS command can also be used to get a very brief description of the meaning for each code.

ST - Status Display

Syntax:

st [RETURN]

The Status Display command displays the version, date, time, communications parameters, and current status of the RPSD Lock.

Sample Command and Response:

```
> st
AT&T  RPSD/JPLock01  - V1.1a Firmware V2.Ot     Init. Code: DR
Current Date: Mon 11/12/90 Time: 16:11:55   Log ID:
Comms.  Set to:  9600/8N
Current  Status:  Idle/Locked
```

The fields of the Status Display screen are:

AT&T RPSD/JPLock01	Gives the version number of the equipment.
Firmware	Gives the version number of the firmware.
Init Code	Tells where and when the device was initialized.
Current Date	Gives the current date. If the date is wrong, it can be corrected using the Date Set command described in this section.
Time	Gives the current time. If the time is wrong, it can be corrected using the Time Set command described in this section.
Log ID	Provides the Log ID of the RPSD Lock. To set a Log ID, use the Set Log ID command described in this section.
Comms Set to	Displays the setting of the communications parameters. To change the communications parameters, use the Set Communications Parameters command described in this section. The default setting is 9600 baud at 8 bits, no parity.
Current Status	Provides the current status of the Lock.

LS - List Statistics

Syntax:

ls [RETURN]

The List Statistics command displays a statistical summary of call attempts and failures, both cumulative and since the last time the statistical summary was reset. The summary is reset by the administrator using the Reset Statistics command, described in this section.

Sample Command and Response:

```
> ls

---RPSD/Lock Access Attempt Statistics - Last Reset: 08/14/90

                                Since Last Reset     Cumulative

Successful Authentications              19              142

Failed Attempts by Reason
   (1) No RPSD/Key Detected              1                1
   (2) No Response                       0                0
   (3) Invalid User ID                   0                0
   (4) Blocked User                      1                2
   (5) Invalid Response                  1                1
   (6) Outgoing Call                     3               14
   (7) Ring - No Answer                  1                1
   (8) Force Disconnect                  2                3
   (9) Restricted Time                   2                1
```

The fields of the List Statistics screen are:

Last Reset	Gives the date that the statistics kept in the Since Last Reset field were reset to 0. Cumulative statistics are never reset to 0.
Successful Authentications	Provides the number of times that a caller was successfully authenticated by the Lock since the last time the statistics were reset and also cumulatively since the Lock was installed.
Failed Attempts by Reason	Provides the number of times that a caller failed in an access attempt for each of the nine failure reasons. The statistics are broken down into the number of failures since the last reset and also the cumulative total since the Lock was installed. For a more detailed explanation of the causes of failure, see Table 3-1.

RS - Reset Statistics

Syntax:

rs [RETURN]

Entering *rs* resets the access attempts statistics to zero. This command does not reset cumulative totals. The access attempts statistics are obtained by using the List Statistics command.

FC - Force Connect

Syntax:

fc [RETURN]

If a call comes in that the administrator wants to go through regardless of whether the caller has a Key, the system administrator can issue the Force Connect command while the Lock is in Verify mode and force the connection to be made. There is a window of about sixty seconds in Verify mode during which the Force Connect command may be issued.

The Lock will request confirmation of a Force Connect command.

If the command is issued when there is no call coming in, an error message will be returned.

Sample Command and Response:

```
JPLock01 193 08/17/90 13:43:55 Call Received

> fc
Force Connect Current Call (Y/N) ? y
JPLock01 194 08/17/90 13:44:16 <Forc-Con> Connected
```

WARNING: Use of the FC command provides a call with connection to the protected resource, bypassing the security normally provided by the RPSD Lock. Use only to connect an authorized caller directly to the host resource.

FD - Force Disconnect

Syntax:

fd [RETURN]

The Force Disconnect command disconnects a call in progress. This might be used to clear the channel for a higher priority call. The Lock will request confirmation of a Force Disconnect command.

If a Force Disconnect command is issued when no call is in progress, an error message will be returned.

Sample Command and Response:

```
JPLock01 195 08/17/90 14:23:55  Call Received
JPLock01 196 08/17/90 14:24:04  KEY20 [#4321] Connected

> fd
Disconnect Current Call (Y/N) ? y
JPLock01 197 08/17/90  14:58:39 Force Disconnect
```

D - Date Set

Syntax:

d <mm/dd/yy> [RETURN]

Sets the date for the RPSD Lock. This must be done in order for the System Activity Log to be accurate. The date should be set upon installation of the Lock to be sure that it is correct.

In the above syntax, **d** is the command and **<mm/dd/yy>** is the date in month, day, and year format. Be certain to use two digits for each part of the date, including a zero at the beginning for months or days less than 10 (for example, 08/01/90). Only the last two digits are used for the year. Also be certain to separate the month, day, and year with the slash (/) character.

Sample Command and Response:

```
> d 08/14/90
JPLock01 198 08/17/90 15:14:13 Date Changed OK
```

C - Clock Set

Syntax:

c <hh:mm> [RETURN]

Set the clock to local time standards in 24 hour clock format (for example, 16:00 for 4:00 PM). The clock must be set in order to ensure the accuracy of the System Activity Log and also because the clock is used by the RPSD Lock for enabling and disabling time restrictions.

Be certain to use a colon (:) to separate the hours and minutes. Also be certain to use a leading zero if setting the time less than 10:00.

Sample Command and Response:

```
> c 13:15
JPLock01 199 08/17/90 15:15:00 Time Changed OK
```

I - ID Set

Syntax:

i <log_id> [RETURN]

The ID set command is used to set a unique identifier for the RPSD Lock. It is useful in the event that more than one RPSD Lock is in operation. The Lock's ID is added to the beginning of all message output so that the administrator can identify the Lock concerned.

In the syntax above, **i** is the command and **<log_id>** is the name selected by the system administrator to identify the Lock.

To clear the ID, enter *i*

The Log ID is limited to 8 alpha/numeric characters.

Sample Command and Response:

```
> i JPLock02
JPLock02 004 08/17/90 15:42:21 Log ID Changed OK

>
```

Note that in the sample the ID is appended to the beginning of the status message. This is where it will appear on all status messages once the ID is set.

SC - Set Communications Parameters

Syntax:

sc <speed,length_parity> [RETURN]

The Set Communications Parameters command is used to set the communications link speed, character length, and parity on the serial port. The default setting is 9600 baud, 8 bit, no parity. In the syntax above **sc** is the command, **speed** is the link speed, and **length_parity** are the character length and parity.

The options for **speed** and **length_parity** are:

- speed - 300, 600, 1200, 2400, 4800, 9600, or 19200 baud (trailing zeros may be omitted, meaning you may enter *sc 24* for 2400 baud)
- length_parity
  - 8N - 8 bits no parity
  - 7N - 7 bits no parity
  - 7E - 7 bits even parity
  - 7O - 7 bits odd parity

If either **speed** or **length_parity** are omitted, the current entry is left unchanged.

Sample Command and Response:

```
> sc 1200,7E
JPLock02 005 08/17/90 15:48:21 Comms Params Changed to 1200/7E
```

Help Screens

To obtain a help screen for any command, enter a question mark (?) followed by the command and [RETURN].

Sample Help Request and Help Response:

```
> ?i

Command:   I - ID Set
Function:  Set ID to precede all log messages from this device.
Format:    I log id
Example:  >I LOCK-A
To clear ID type: I ""
```

4 RPSD Key Use

RPSD Key Use

When the RPSD system is working correctly, Key use and authentication should be almost invisible to the RPSD Key user. The user dials the RMATS channel from the user's terminal, authentication takes place (during which time the LEDs on the front panel of the RPSD Key indicate the status of the call), and the RPSD Key user is corrected to the RMATS channel.

When access is successful, status messages like the following appear on the RPSD Key user's administration terminal (connected to via the RPSD Key Aux. Port):

```
07/12/90 13:58:27 Calling Out
07/12/90 13:58:37 Dialing Complete
07/12/90 13:59:07 Authentication Complete
07/12/90 14:05:41 AT&T RPSD/Key - V1.1 - Idle
```

However, access attempts may not always be successful. In such a case, the Key user can obtain an explanation for the failure in one of two ways:

- a status message on the RPSD Key user's terminal that is sent by the RPSD Lock
- the Last Call Status Test

In the case of a status message sent to the Key user's terminal, the message is sent automatically. The Last Call Status Test is explained in detail in this chapter in the section titled *Last Call Status Test.*

Access Failure Messages

Table 4-1 describes the access failure messages and their meanings. Access failure messages do not necessarily mean that an error has occurred. For example, if a Key user fails to gain access to the RMATS channel because the administrator has put a block on that Key, or because access has been restricted for that time of day, then the system is functioning properly.

TABLE 4-1
Access Failure Messages

Code Number	Access Failure Message	Meaning
1	No RPSD/Key Detected	The RPSD Lock and RPSD Key were unable to initiate a dialogue
2	No Response	The RPSD Key did not respond to the RPSD Lock's challenge. The probable explanation is that the Key was unable to receive the data from the Lock.
3	Invalid User ID	The RPSD Key user's ID is not in the table of users on the RPSD Lock.
4	Blocked User	The RPSD Key was administered as blocked on the RPSD Lock.
5	Invalid Response	The RPSD Key responded to the RPSD Lock's challenge, but the response was incorrect, probably due to an incorrect secret Key.
6	Outgoing Call	An outgoing call is being placed from the RPSD Lock, so the Lock terminated the session.
7	Ring - No Answer	The RPSD Lock rang the modem, but the modem did not pick up.
8	Force Disconnect	A Force Disconnect command was issued to the RPSD Lock.
9	Time Restriction	The call was placed during a time of day when the Lock is restricted from taking any calls from your user ID.

Last Call Status Test

To determine the cause of a failure to connect to the RMATS channel via the RPSD Lock, the Key user can obtain the last status message sent by the Lock by simply dialing the RMATS channel from a touch-tone telephone. When the Lock responds by sounding a tone, press *2*★ on the phone pad. You should hear a number of beeps equal to the number of the last status message. See Table 4-1 for an explanation of the status messages.

RPSD Key User Command Set

The RPSD Key device displays a different Menu of Commands to standard output depending on whether the device is in a virgin state. The following shows the Menu of Commands when the Key is in a virgin state:

```
--- Menu of Commands ---

L - List User Information
H - History Display
D - Date Set
C - Clock Set
I - Set Log ID
S - Status Display
SC - Set Comms. Params
W - Wipe Out (erase) User ID, Secret Key, and Device ID
------ Initialization Functions ------
U - Set User ID
K - Set Secret Key
N - Sets Device Number
 --------------------------------------

-- For Help Type '?' Followed by Command --
```

The following shows the Menu of Commands when the Key has been initialized:

```
--- Menu of Commands ---

L - List User Information
H - History Display
D - Date Set
C - Clock Set
I - Set Log ID
S - Status Display
SC - Set Comms. Params
W - Wipe Out (erase) User ID, Secret Key, and Device ID

-- For Help Type '?' Followed by Command --
```

As you can see, the last three commands displayed when the Key is in a virgin state are eliminated from an initialized Key. A description of the commands follows.

U - Set User ID

Syntax:

u <user_id> [RETURN]

The Set User ID command is used to enter a name that will identify the RPSD Key to the RPSD Lock. This command is only used when initializing a Key in the virgin state. See Chapter 2, *Initializing an RPSD Key* for a complete description of the procedure which uses this command.

To use this command, enter *u <user_id>* [RETURN], where *u* is the command and *<user_id>* is an alphanumeric identifier of up to ten characters. The user ID must match the user ID being used to identify the Key when adding a user to the RPSD Lock. If you assign the same user ID to more than one Key, be certain to assign different device numbers to those Keys.

Sample Command and Response:

```
> u KEY20
08/14/90 14:00:01 User ID set to KEY20
```

K - Set Secret Key

Syntax:

k <secret_key> [RETURN]

The Set Secret Key command is used to enter the secret key information supplied by the RPSD Lock when a new user is added to the list of authorized user's. This command is only used when initializing a Key in the virgin state. See Chapter 2, *Initializing an RPSD Key* for a complete description of the procedure which uses this command.

To use this command, enter *k <secret_key>* [RETURN], where *k* is the command and *<secret_key>* is the secret key information returned by the RPSD Lock device when you added a new user name. The response will include a Test Reply. The Test Reply should be matched against the one for your Key given by the RPSD Lock. If the replies match, the Key has been correctly seeded with the secret information. If the responses do not match, use the Wipe Out command described in this section to return the Key to a virgin state and initialize the Key again. If the tests again fail, there is a problem with the Key and it should be replaced.

Sample Command and Response:

```
> k f37b 159d 6abe 3e
08/14/90 14:01:09 Secret Key Loaded. Test Reply is 8119704
```

N - Set Device Number

Syntax:

n <number> [RETURN]

The Set Device Number command enters a number from 100 to 9999999 as an identifier for the RPSD Key device. Use this command when you have two or more RPSD Keys with the same user ID. The device number is associated with the Key for the purpose of identification by the RPSD Lock. This command is only used when initializing a Key in the virgin state. See Chapter 2, *Initializing an RPSD Key* for a complete description of the procedure which uses this command.

Enter *n <device_number>* [RETURN], where *n* is the command and *<device_number>* is an arbitrary number between 100 and 9999999 that you select to be used as an identifier for that particular RPSD Key device. Be certain not to duplicate existing device numbers. The last four digits of the RPSD Key AT&T serial number is recommended.

Sample Command and Response:

```
> n 12345
08/14/90 14:03:59 Device Number set to 12345
```

L - List User Information

Syntax:

l [RETURN]

The List User Information command will list the user ID, device number, and test response number for the Key.

To use the List User Information command, enter *l* [RETURN] at the > prompt of the Key user's terminal.

Sample Command and Response:

```
>l
User ID: KEY20
Device Number: 12345
Test Response: 8119704
```

H - History Display

Syntax:

h [RETURN]

The History Display command displays a log history of the last twenty messages generated by or sent to the RPSD Key device. See Table 4-1 for an explanation of the status messages sent to the Key by the RPSD Lock when a connection attempt fails.

Sample Command and Response:

```
> h

--- Log History ---
07/12/90 13:28:00 Dialing Complete
07/12/90 13:28:16 Attempt Failed (5) Invalid Response
07/12/90 13:28:16 Waiting for Subscriber to Go On-hook
07/12/90 13:28:26 AT&T RPSD/Key - V1.0 - Idle
07/12/90 13:32:44 Calling Out
07/12/90 13:32:55 Dialing Complete
07/12/90 13:33:15 Attempt Failed (5) Invalid Response
07/12/90 13:33:15 Waiting For Subscriber to Go On-hook
07/12/90 13:33:20 AT&T RPSD/Key - V1.0 - Idle
07/12/90 13:53:59 Wipe Out Complete
07/12/90 13:54:15 AT&T RPSD/Key - V1.0 - Reset
07/12/90 13:56:28 User ID set to KEY20
07/12/90 13:56:59 Secret Key Loaded. Test Reply is 8119704
07/12/90 13:57:46 Device Number set to 12345
07/12/90 13:57:46 Device Initialized OK
07/12/90 13:57:46 AT&T RPSD/Key - V1.0 - Idle
07/12/90 13:58:27 Calling Out
07/12/90 13:58:37 Dialing Complete
07/12/90 13:58:43 Authentication Complete
07/12/90 13:58:59 AT&T RPSD/Key - V1.0 - Idle
```

The fields of the History Display screen are:

Date Provides the date the message was generated.

Time The second field provides the time the message was generated in 24 hour clock format.

Message The last field contains the status message.

Failed attempts at access generate a message at the RPSD Lock that is sent to the RPSD Key. There are nine causes for such failure, as described in Table 4-1.

The rest of the messages are self-explanatory.

D - Date Set

Syntax:

d <mm/dd/yy> [RETURN]

The Date Set command is used to set the date for the RPSD Key's internal calendar. You should set the date when you begin using the Key just to be certain that it is correct. To check the date you can use the Status Display command described in this section.

In the above syntax, **d** is the command and **<mm/dd/yy>** is the date in month, day, and year format. Be certain to use two digits for each part of the date, including a zero at the beginning for months or days less than 10 (for example, 08/01/90). Only the last two digits are used for the year. Also be certain to separate the month, day, and year with the slash (/) character.

Sample Command and Response:

```
> d 08/14/90
08/14/90 13:14:13 Date Changed OK
```

C - Clock Set

Syntax:

c <hh:mm> [RETURN]

Set the clock to local time standards in 24 hour clock format (for example, 16:00 for 4:00 PM). The clock must be set in order to ensure the accuracy of the History Log.

Be certain to use a colon (:) to separate the hours and minutes. Also be certain to use a leading zero if setting the time less than 10:00.

Sample Command and Response:

```
> c 13:15
8/14/90 13:15:00 Time Changed OK
```

I - Set Log ID

Syntax:

i <log_id> [RETURN]

The Set Log ID command is used to identify which Key is associated with which status message. This is especially important where multiple devices share a single administration terminal. The command adds the ID to the beginning of each message generated by the Key.

In the syntax described above, **i** is the command and **log_id** is an identifier of up to 8 characters selected by you.

Sample Command and Response:

```
> i KEY11
KEY11 08/14/90 14:20:08 Log ID Changed OK
```

S - Status Display

Syntax:

s [RETURN]

The Status Display command displays the current status of the RPSD Key to the user's terminal.

To use this command, enter **s** [RETURN] at the **>** prompt.

Sample Command and Response:

```
>s
AT&T RPSD/KEY11 - V1.0     Firmware  V2.0x      Init Code:
Current Date: Mon 08/14/90   Time:  14:28:09   Log ID:  12345678
Comms Set to: 9600/8N
Current Status: Idle
```

The fields of the Status Display screen are:

AT&T RPSD/KEY11	Gives the version number of the equipment and the Key user ID.
Firmware	Gives the version number of the firmware.
Init Code	Tells where and when the device was initialized.
Current Date	Gives the current date. If the date is wrong, it can be corrected using the Date Set command described in this section.
Time	Gives the current time. If the time is wrong, it can be corrected using the Time Set command described in this section.
Log ID	Provides the Log ID of the RPSD Key. To set a Log ID, use the Set Log ID command described in this section.
Comms Set to	Displays the setting of the communications parameters. To change the communications parameters, use the Set Communications Parameters command described in this section. The default setting is 9600 baud at 8 bits, no parity.
Current Status	Provides the current status of the Key.

SC - Set Communications Parameters

Syntax:

sc <speed,length_parity> [RETURN]

The Set Communications Parameters command is used to set the communications link speed, character length, and parity on the serial port. The default setting is 9600 baud, 8 bit, no parity. In the syntax above, **sc** is the command, **speed** is the link speed, and **length_parity** are the character length and parity.

The options for **speed** and **length_parity** are:

- speed - 300, 600, 1200, 2400, 4800, 9600, or 19200 baud (trailing zeros maybe omitted, meaning you may enter *sc 24* for 2400 baud)
- length_parity
  - 8N - 8 bits no parity
  - 7N - 7 bits no parity
  - 7E - 7 bits even parity
  - 7O - 7 bits odd parity

If either **speed** or **length_parity** are omitted, the current entry is left unchanged.

Sample Command and Response:

```
> sc 1200,7E
08/14/90 13:48:21 Comms Params Changed to 1200/7E
```

W - Wipe Out

Syntax:

w [RETURN]

The Wipe Out command will erase the user ID, secret key information, and device ID of the RPSD Key and return it to a virgin state. If the Wipe Out command is used, the Key will be unable to access the RPSD Lock unless the entire initialization procedure is performed again. For this reason, you should be certain that you really want to return the Key to a virgin state before using this command.

You may wish to test the Key while it is in an uninitialized state. See Chapter 2, *Testing an Uninitialized Key* for the procedure.

The RPSD Key requests confirmation of the Wipe Out command.

Sample Command and Response:

```
> w

**** THIS FUNCTION RENDERS DEVICE UNABLE ****
****          TO ACCESS RPSD/LOCK          ****

Are You Sure You Want to Do This (Y/N) ? y
08/15/90 13:23:16 Wipe Out Complete

>
```

Help Screens

To obtain a help screen for any command, enter a question mark (?) followed by the command and [RETURN].

Sample Help Request and Help Response:

```
> ?i

Command:   I - ID Set
Function:  Set ID to precede all log messages from this device.
Format:    I log_id
Example:  >I KEY-A
To clear ID type: I ""
```

5 Troubleshooting

Troubleshooting

This chapter provides a basis for establishing the cause of trouble or access failure with your RPSD system. In the event that you are unable to determine the cause of the problem or resolve the matter to your satisfaction, contact the technical support center at:

1 800 242-2121

Note: The only solution to a hardware or firmware problem in the RPSD Lock or Key is to replace the malfunctioning equipment. Instructions for replacing the equipment are in the *Replacing the RPSD Lock or Key* section of this chapter.

Access Failure Messages

When calls to the RPSD Lock are disconnected without reaching the PBX modem, the Lock generates an access failure message that is sent to standard output and saved in the system activity log. The access failure message is also sent as a reply to the caller whose attempt failed (the message can only be received, however, if the caller has an RPSD Key with an administration terminal or printer attached to it). A dedicated printer connected to the Aux. Port on the Lock enables you to maintain a permanent record of access failure messages.

Note: These messages are not necessarily a sign of a malfunction or other problem. If the RPSD Lock fails to detect a Key, for example, on the caller's line, this is likely because there is no Key on the caller's line and the Lock is fulfilling its role properly by preventing unauthorized access. The actions suggest in Table 5-1 are only to be taken in the event that a known Key user who is supposed to have access to the RMATS channel is unable to gain access.

You can also obtain an access failure message for the most recent call attempt by using the Last Call Status Test. See *Last Call Status Test* in this chapter for a detailed explanation of the use and limitations of the Last Call Status Test.

There are nine codes that explain access failures. Table 5-1 explains the type of access failures and the appropriate action to take.

TABLE 5-1
Access Failure Messages

Code No.	Message	Meaning	Action
1	No RPSD/Key Detected	No RPSD Key was detected on the caller's line.	First test the RPSD Lock using the Self Check described in *Testing the RPSD Lock* in this chapter. If the Lock tests okay, and there is an RPSD Key on the line but the RPSD Lock failed to detect it, escalate the trouble to the next level of service.
2	No Response	No response was returned from the RPSD Key when the RPSD Lock sent the challenge.	First test the RPSD Lock using the Self Check described in *Testing the RPSD Lock* in this chapter. If the Lock tests okay, a touch-tone telephone should be substituted for the RPSD Lock and the Last Call Status Test described in *Testing the RPSD Lock* in this chapter should be run to obtain any status information the Lock may have generated and to determine of the problem is with the CO line. If the CO line is okay, escalate the trouble to the next level of service.
3	Invalid User ID	The RPSD Key user ID is not in the table of users on the RPSD Lock.	Add the Key user to the user table if it is someone you want to permit access to the RMATS channel. (Note that this message may indicate an unauthorized attempt at access.) See Chapter 3 for the procedure for adding users. Check the Test Responses to make sure the RPSD Lock and RPSD Key Test Responses match (see Chapters 3 and 4 for checking Test Responses). If access for this Key is desired, and the Test Responses do not match, you will need to use the Wipe Out command (see Chapter 4, *RPSD Key Use)* to return the Key to a virgin state. Then follow the directions for initializing the RPSD Key, also found in Chapter 4.

TABLE 5-1 (Continued)
Access Failure Messages

Code No.	Message	Meaning	Action
4	Blocked User	The administrator placed a block on the caller's RSPD Key user ID.	No action necessary. This is a deliberate Block command issued by the administrator.
5	Invalid Response	The RSPD Key responded to the RSPD Lock's challenge, but the response was incorrect.	Check the Test Responses to make sure the RSPD Lock and RSPD Key Test Responses match (see Chapters 3 and 4 for checking Test Responses). If access for this Key is desired, and the Test Responses do not match, you will need to use the Wipe Out command (see Chapter 4, *RSPD Key Use)* to return the Key to a virgin state. Then follow the directions for initializing the RSPD Key, also found in Chapter 4.
6	Outgoing Call	An outgoing call is being placed. If a call is connected, the Lock forces a disconnect in order to make the outgoing call.	No action necessary. This is not a call failure.
7	Ring - No Answer	The RSPD Lock rang the modem, but the modem did not pick up.	Run the Modem Ring Test described in this chapter and follow the directions for determining the cause of failure.
8	Force Disconnect	A Force Disconnect command was issued to the RSPD Lock.	No action necessary. This is a deliberate disconnect command issued by the administrator.

TABLE 5-1 (Continued)
Access Failure Messages

Code No.	Message	Meaning	Action
9	Time Restriction	The call was placed during a time of day when the Lock is restricted from taking any calls.	No action necessary. This is a deliberate restriction placed on access to the RSPD Lock by the administrator. If access must be permitted at this time, contact the system administrator. The administrator may bypass the time restriction in one of the following ways: ■ Removal of the time restriction on that Key user ■ Force Connect command The administrator should see Chapter 3 for instructions on removing time restrictions or using the Force Connect command.

Testing the RPSD Lock

There are two ways in which the RPSD Lock can be tested to determine the cause of access failures and whether the Lock or some associated piece of hardware is malfunctioning.

- Built-in diagnostics
- Hardware replacement

Note: In all cases where a connection fails, if it is important for the caller to get into the RMATs channel, the system administrator can permit the access by using the Force Connect command. See Chapter 4 for more information on the Force Connect command.

Both of these methods require a touch-tone telephone, the first to dial into the Lock and perform the diagnostics, the second to physically replace various pieces of hardware.

Built-in Diagnostics

The RPSD system provides three diagnostic tests which are used to determine the cause of access failures. These are:

- Self Check
- Last Call Status Test
- Modem Ring Test

All three tests are performed by dialing the RMATS channel from a touch-tone telephone and then entering a code for the test you want using the phone pad. The RPSD Lock responds to the code by issuing a tone or set of tones, which can then be interpreted to determine the cause of call failure.

Self Check

The Self Check tests the health of the RPSD Lock.

To perform the Self Check, dial the RMATS channel from a touch-tone telephone. When the call is answered, you hear a short tone (indicating a connection to the RPSD Lock). Press *1* ⋆ on the telephone pad.

If the response is 3 quick tones, followed by the RPSD Lock disconnecting, the Lock is functioning properly. The Lock will also generate a status message similar to the following:

```
999 08/14/90 16:21:34 Remote Test 1 (Self Check) Completed OK
```

If the response is anything but 3 quick tones, the Lock is not functioning properly.

You should run the Modem Ring Test next no matter what the Lock's response. In the case of a properly functioning Lock, the Modem Ring Test serves as a backup check on the Lock. In the case of a malfunctioning Lock, the Modem Ring Test will further diagnose the problem.

Last Call Status Test

The Last Call Status Test provides the call outcome for the last call attempt to the RPSD Lock. The test responds either with slow beeps, the number of which correspond to the nine status messages explained in Table 5-1, or 3 fast beeps, which means that the last call attempt was successful.

To perform the Last Call Status Test, dial the RMATS channel from a touch-tone telephone. When the call is answered, you will hear a tone indicating a connection to the RPSD Lock. Press *2* ⋆ on the telephone pad.

As stated above, you will hear 3 fast beeps if the last call attempt was successful, or between one and nine slow beeps if the last call attempt was unsuccessful. Count the number of slow beeps. The number of slow beeps corresponds to the access failure message number. Table 5-1 explains each of the nine access failure messages and the appropriate action to take.

The RPSD Lock also generates a status message similar to the following:

```
103 08/14/90 16:21:34 Remote Test 2 (Last Call Status) Completed OK
```

Modem Ring Test

The Modem Ring Test tells you whether the call attempts are getting through to the modem. If there is a problem with the RPSD Lock, the PBX modem, or the cabling, the call will not reach the modem. The likeliest result, in the case of a problem, is a Ring No Answer.

To perform the Modem Ring Test, dial the RMATS channel from a touch-tone telephone. When the call is answered, you will hear a tone indicating a connection to the RPSD Lock. Press *3* ⋆ on the telephone pad.

The RPSD Lock responds to the command by ringing the modem. While the Lock rings the modem, you will hear a simulated ring on the telephone handset. When the modem picks up, you will hear the answer tone. The answer tone will not last long enough for the modem to perform handshaking. The Lock will then send 3 quick beeps to your telephone and disconnect the call.

The RPSD Lock also generates a status message similar to the following:

```
104 08/14/90 16:21:34 Remote Test 3 (Modem Ring) Completed OK
```

If you do not hear the answer tone, the problem may be the RPSD Lock, the PBX modem, or the cabling. Your next action should be to check the equipment by physically replacing the hardware. See *Hardware Replacement* in this chapter for procedures.

Hardware Replacement

The built-in diagnostics of the RPSD Lock may indicate that there is a hardware failure, but they will not necessarily determine whether that failure is in the CO line, RPSD Lock, PBX modem, or caller's equipment or lines. In such a situation, the best way to determine where the failure is occurring is to methodically replace individual components of the hardware with a touch-tone telephone. The following sections describe the procedure for such replacement in the order you should perform it.

Note: The modem for the System 75 and DEFINITY Generic 1 is internal to the PBX and located on the circuit board. The modem for the System 85 and DEFINITY Generic 2 is external to the PBX.

Replacing the PBX Modem

To test whether the problem diagnosed by the Modem Ring Test is in the PBX modem, perform the following procedure:

1. Disconnect the modular telephone plug from the PBX modem and connect a touch-tone telephone to the modem.
2. Call the RMATS channel from a touch-tone telephone and perform the Modem Ring Test described in this chapter.
3. If the phone you substituted for the modem rings, have someone answer it. If the connection is fine, the problem is in the modem.

   If the call fails to ring the telephone, or the connection is faulty, it is likely that the modem is fine. Go to the next step.
4. Remove the touch-tone telephone and reconnect the modem, but this time use a different cable between the RPSD Lock and the modem. Call the modem again from a telephone.
5. If the system functions properly, the problem is in the cable.

   If the system continues to malfunction, go to the next step.
6. Remove the substitute cable and put the original back in. Disconnect the RPSD Lock from the CO line and replace the Lock with a touch-tone telephone. Again, call the RMATS channel from a second telephone.
7. If the telephone you substituted for the Lock rings, answer it. If the phones work properly, the problem is in the RPSD Lock. Replace the Lock. See *Replacing the RPSD Lock* in this chapter.

Replacing the Lock or Key

If an RPSD Lock must be replaced, the service call is classified as the highest priority because a failed Lock prevents all access to or from the RMATS channel. The RPSD Lock may be removed from the line and, to maintain access to the RMATS channel, the modem may be connected directly to the CO line. (This is only if the Force Connect command fails as well. See Chapter 3 for further information on the Force Connect command.) Please note that without the Lock, the line is not secure.

AT&T technicians should consider a failed RPSD Lock or Key a Severity 4 trouble.

Customers can replace the unit themselves, if they want, by contacting the National Parts Sales Center (NPSC). The number for the NPSC is 1 800 ATT-PART.

Saving the Key Seed Value

All of the secret information used to initialize the RPSD Lock should be saved in a secure location. If a Lock needs to be replaced, you will want to initialize the replacement Lock with the same information as the original. However, it is important to remember that the secret information must be saved in a secure location so as to maintain the security of the system.

WARNING: If the security of the Seed Value is breached, RPSD security itself is lost. RPSD Lock and Key should be reinitialized with a new secret key.

The RPSD Secret Key Seed Value must be physically protected and secured. AT&T makes no claim or guaranty for protection or security provided by RPSD.

A Cables, Connectors, and Ports Table

Cables, Connectors, and Ports Table

Table A-1 shows the cables, connectors, and ports for installing the RPSD system. This table includes optional connections as well as the basic configuration.

TABLE A-1
Cables, Connectors, and Ports

Part	COMCODE	From	To
modular connector	XXXXXX	PBX	RJ11 at modem
6 position wire	XXXXXX	RJ11 at PBX	RJ11 at modem
modular connector[1]	XXXXXX	Cable from PBX	modem
7 ft. cable with modular connector on each end	Supplied with RPSD Lock	RPSD Lock	CO line or modem
14 ft. cable with modular connector on each end	Supplied with RPSD Lock	RPSD Lock	CO line or modem
RJ11 wall jack[2]	XXXXXX	RJ11 to RPSD	CO line
EIA-RS-232 cable[3]	XXXXXX	DB25 at RPSD Lock	DB25 at admin. terminal or printer or A/B switch
DB25 connector[3]	XXXXXX	RPSD Lock	Cable to admin. terminal or printer or A/B switch
DB25 connector[3]	XXXXXX	Admin. terminal or printer or A/B switch	Cable to RPSD Lock

1 The 212A modem uses a DB25 connection. See Figures 2-7 and 2-8 for the details on making up the appropriate connector.

2 If RJ11 receptacle is not present on CO line, install one.

3 The RPSD Lock maybe connected to the administration terminal, printer, or A/B switch (to allow connection to both the terminal and printer).

B Device LEDs

Front Panel LEDs

Both the RPSD Lock and the RPSD Key have seven LEDs each on their front panels. The following sections explain the meaning of each LED and their various states.

RPSD Lock

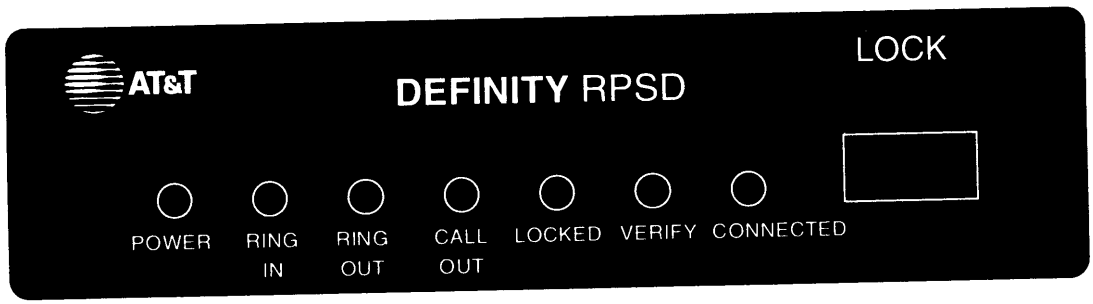


FIGURE B-1
RPSD Lock LEDs

The first LED on the left is the red Power light. This indicates that the power is on. This LED should remain lit whenever the RPSD Lock is plugged into an electrical outlet.

When first powered up, the LEDs should all blink on and off in unison three times, then settle into a Locked condition.

Table B-1 explains the status of the RPSD Lock when the different LEDs are lit.

TABLE B-1
RPSD Lock LEDs

LED							Meaning
1	2	3	4	5	6	7	
On	On	Off	Off	Off	Off	Off	An incoming call is being processed.
On	Off	On	Off	Off	Off	Off	The RPSD Lock is ringing the modem.
On	Off	Off	On	Off	Off	Off	An outgoing call is in progress from the modem.
On	Off	Off	Off	On	Off	Off	The Lock is idle and in a ready condition, able to accept incoming calls or process outgoing calls.
On	Off	Off	Off	Off	On	Off	An incoming call is being authenticated for permission to access the RPSD Lock.
On	Off	Off	Off	Off	Off	On	An incoming call has been authenticated, passed to the PBX, and is in progress.

RPSD Key

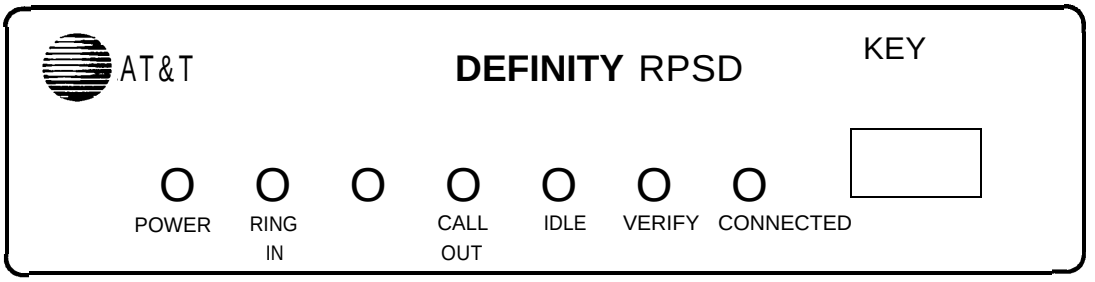


FIGURE B-2
RPSD Key LEDs

The first LED on the left is the red Power light. This indicates that the power is on. This LED should remain lit whenever the RPSD Lock is plugged into an electrical outlet.

When first powered up, the LEDs should all blink on and off in unison three times, then settle into a Locked condition.

Table B-2 explains the status of the RPSD Key when the different LEDs are lit.

TABLE B-2
RPSD Key LEDs

LED							Meaning
1	2	3	4	5	6	7	
On	On	Off	Off	Off	Off	Off	An incoming call is being processed.
On	Off	On	Off	Off	Off	Off	Should only light when it blinks on power-up.
On	Off	Off	On	Off	Off	Off	An outgoing call is in progress from the modem.
On	Off	Off	Off	On	Off	Off	The Key is idle and in a ready condition, able to place outgoing calls or process incoming calls.
On	Off	Off	Off	Off	On	Off	A call from the Key is being authenticated for permission to access an RPSD Lock.
On	Off	Off	Off	Off	Off	On	A call from the Key to an RPSD Lock has been authenticated, passed to the PBX, and is in progress.

Index

S

T

U

W