

Print Services Facility for z/OS
Version 4.7

Security Guide



Note

Before using this information and the product it supports, read the information in [“Notices” on page 31.](#)

This edition applies to the IBM® Print Services Facility Version 4 Release 8 Modification 0 for z/OS, Program Number 5655-M32, and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces S550-0434-05.

© **Copyright International Business Machines Corporation 1989, 2019.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures.....	v
Tables.....	vii
About this publication.....	ix
Who should read this publication.....	ix
How this publication is organized.....	ix
Fast path.....	ix
Understanding the syntax notation used in this publication.....	ix
Related information.....	x
How to send your comments to IBM.....	xi
If you have a technical problem.....	xi
Summary of Changes.....	xiii
PSF for z/OS Version 4 Release 7.....	xiii
Chapter 1. Introducing the print labeling function.....	1
Understanding print labeling.....	1
User-printable area.....	2
Distributing secure PSF output.....	2
Auditing PSF output for security.....	3
Introducing trusted computing base components.....	3
Trusted software.....	4
Trusted hardware.....	5
Users.....	5
Choosing from a list of security-related PSF tasks.....	5
Chapter 2. Using print labeling.....	7
Installing PSF.....	7
Printer support in PSF.....	7
Designing pages for print labeling.....	7
Creating security overlays.....	8
Allocating the security definitions library.....	8
Security definitions library attributes.....	8
Defining a security definitions library.....	9
Syntax for a security definitions member.....	9
Rules for defining a security definitions member.....	11
Sample security definitions member.....	11
Defining security resource libraries.....	12
Defining a security console.....	13
Assembling separator pages.....	13
Enabling print labeling.....	14
Using RACF with PSF for z/OS.....	14
PSF processing differences with the print labeling function.....	15
Updating initialization parameters.....	15
Updating print labeling parameters.....	16
Defining data definition names in the PRINTDEV statement.....	18
Submitting a print job that includes identification labels.....	18

Overriding print labeling defaults.....	19
Maintaining PSF for z/OS with print labeling enabled.....	19
Auditing PSF printing.....	19
Interpreting security-related messages.....	20
Diagnosing print labeling problems.....	20
Appendix A. Security page layout.....	25
Appendix B. PAPERNAME table for system-defined paper names.....	27
Appendix C. Accessibility.....	29
Notices.....	31
Terms and conditions for product documentation.....	32
IBM Online Privacy Statement.....	33
Policy for unsupported hardware.....	33
Minimum supported hardware.....	33
Trademarks.....	34
Glossary.....	35
Bibliography.....	41
Advanced Function Presentation (AFP).....	41
Index.....	43

Figures

1. Print labeling.....	1
2. Placing identification labels on the physical page.....	2
3. Random numbering of printed output.....	3
4. Typical components of a trusted computing base.....	4
5. Library attributes for the security definitions library.....	8
6. Syntax for a security definitions library member.....	9
7. Sample coding of a member.....	11
8. Page layout for a cut-sheet page.....	12
9. Page layout for a continuous form.....	12
10. ROUTCODE option for routing messages.....	13
11. ROUTCODE option for stopping messages.....	13
12. Activating SECLABEL.....	14
13. Using the RACF SETROPTS and RDEFINE commands.....	14
14. Adding a user ID to a RACF profile.....	14
15. Refreshing RACF.....	14
16. Sample PSF startup procedure with comments for security-related parameters.....	16
17. Sample JCL job card.....	19
18. Sample JCL output statement.....	19
19. Security page layout.....	25

Tables

1. SYS1.SAMPLIB members for PSF documentation updates..... x

2. Security tasks and the people who do them..... 5

3. Library attributes for a security resource library..... 13

4. PSF exit routines in SYS1.SAMPLIB..... 13

5. Parameters for enabling print labeling..... 17

6. Print labeling diagnosis..... 21

7. PAPERNAME parameter values..... 27

8. AFP publications available from the AFP Consortium..... 41

9. AFP publications available from the IBM Documentation and the IBM Publications Center..... 41

10. AFP publications available from the IBM Publications Center..... 41

About this publication

This publication is designed to help programmers, analysts, and administrators who install, customize, or maintain Print Services Facility (PSF) for z/OS® (referred to as PSF) as a component of a trusted computing base.¹

This publication describes the PSF function that is called *print labeling*. This function can be used to produce printed output that contains special labels. These labels can be used for security purposes or other installation-defined purposes.

Note: Print labeling can be done with PSF even if PSF is not a part of a trusted computing base.

Who should read this publication

You use this publication if you are a system programmer, a system analyst, a security administrator, a security auditor, or an application programmer who is responsible for data security.

You must be familiar with the material that is contained in *PSF for z/OS: Customization* and *PSF for z/OS: User's Guide* before you attempt any of the procedures that are described in this publication.

How this publication is organized

This publication is intended to help you do the tasks in [Table 2 on page 5](#). The information in this publication must not be used for programming purposes.

This publication is organized so that you can read it sequentially or refer directly to individual tasks.

- Use [Chapter 1, “Introducing the print labeling function,” on page 1](#) for an overview of the PSF print labeling function and how PSF operates within a trusted computing base.
- Use [Chapter 2, “Using print labeling,” on page 7](#) when you are working with an operating system that supports print labeling.
- Use [Appendix A, “Security page layout,” on page 25](#) when you are designing pages for printing with the print labeling function of PSF.
- Use [Appendix B, “PAPERNAME table for system-defined paper names,” on page 27](#) to find a list of system-defined paper names that are used when you are establishing a security definitions library.
- Use [Appendix C, “Accessibility,” on page 29](#) to obtain information about the accessibility features available in z/OS.

A notices section, glossary, bibliography, and index are included. The bibliography lists the publications that contain additional information about the system, hardware, or software used by PSF, or about installation and maintenance.

Fast path

For a list of security-related tasks, see [Table 2 on page 5](#). This fast path is provided so that you can quickly access task information if you are already familiar with the PSF print labeling function.

Understanding the syntax notation used in this publication

The following rules apply to syntax examples and coding illustrations throughout this publication:

- The uppercase letters are to be entered as shown; however, you do not need to type them in uppercase.

¹ A trusted computing base consists of components that together enforce a unified security policy over a computing environment. For more information, see [“Introducing trusted computing base components” on page 3](#).

- The variable data that you must provide is printed in *italics*. Enter specific data to replace the characters in *italics*; for example, for *PRTnnnn* you can enter PRT2.
- Do not enter any of the following symbols as part of a parameter or an option:
 - Vertical Bar |
 - Underscore ____
 - Braces { }
 - Brackets []
- A vertical bar between two values means that you are to select only one of the values.
- If one value in a set of values is underscored, that value is the default—that is, the value that PSF uses if no option is specified.
- If values are enclosed in braces {_s}, one or the other of the values in the braces must be selected.
- If a value is enclosed in brackets [_s], you do not have to select that value.

Related information

Publications that are referred to in this document or that contain more information about AFP and related products are listed in the “Bibliography” on page 41. For information about all z/OS product publications, see *z/OS Information Roadmap*.

For more information about z/OS and PSF for z/OS, see these web pages:

- IBM z/OS (www.ibm.com/products/zos)
- IBM Documentation (www.ibm.com/docs/en)

To obtain the latest documentation updates for PSF for z/OS, see the appropriate SYS1.SAMPLIB members in Table 1 on page x.

Table 1. SYS1.SAMPLIB members for PSF documentation updates	
Member	Publication
APSGADP8	<i>PSF for z/OS: AFP Download Plus</i>
APSGCUS8	<i>PSF for z/OS: Customization</i>
APSGDGN8	<i>PSF for z/OS: Diagnosis</i>
APSGDLG8	<i>PSF for z/OS: Download for z/OS</i>
APSGMAC8	<i>PSF for z/OS: Messages and Codes</i>
APSGSEC8	<i>PSF for z/OS: Security Guide</i>
APSGUSR8	<i>PSF for z/OS: User's Guide</i>

How to send your comments to IBM

We invite you to submit comments about the z/OS product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead [“If you have a technical problem”](#) on page xi.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function

If your comment or question is about z/OS itself, submit a request through the [IBM RFE Community](http://www.ibm.developerworks/ref) (<http://www.ibm.developerworks/ref>).

Feedback on IBM Documentation function

If your comment or question is about the IBM Documentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdoc@us.ibm.com.

Feedback on the z/OS product documentation and content

If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: *PSF for z/OS: Security Guide*, S550-0434
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the [IBM Support](http://www.ibm.com/mysupport/s) (www.ibm.com/mysupport/s).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of Changes

PSF for z/OS Version 4 Release 7

This information contains no technical changes for either PSF for z/OS® Version 4 Release 7 or PSF for z/OS Version 4 Release 6.

Chapter 1. Introducing the print labeling function

This information introduces the concept of print labeling and explains how PSF for z/OS operates within a secure computing environment.

Understanding print labeling

You can place identification labels on each page of printed output with the PSF function called print labeling. An identification label can be composed of text, graphics, or a combination of both. Identification labels can be used for security information, such as a TOP SECRET security level, or for other installation-defined purposes. Identification labels can be placed on the top, bottom, or sides of all pages within a job. Up to eight labels can be defined to print on every page of the job.

An identification label is positioned on the page by using a resource that is called a security overlay. The overlays and the resources used by the overlays, such as fonts and page segments, are stored in special security libraries.

Print labeling can be applied to data pages and to separator pages. Figure 1 on page 1 shows labeling applied to a data page from one job and a separator page from another job.

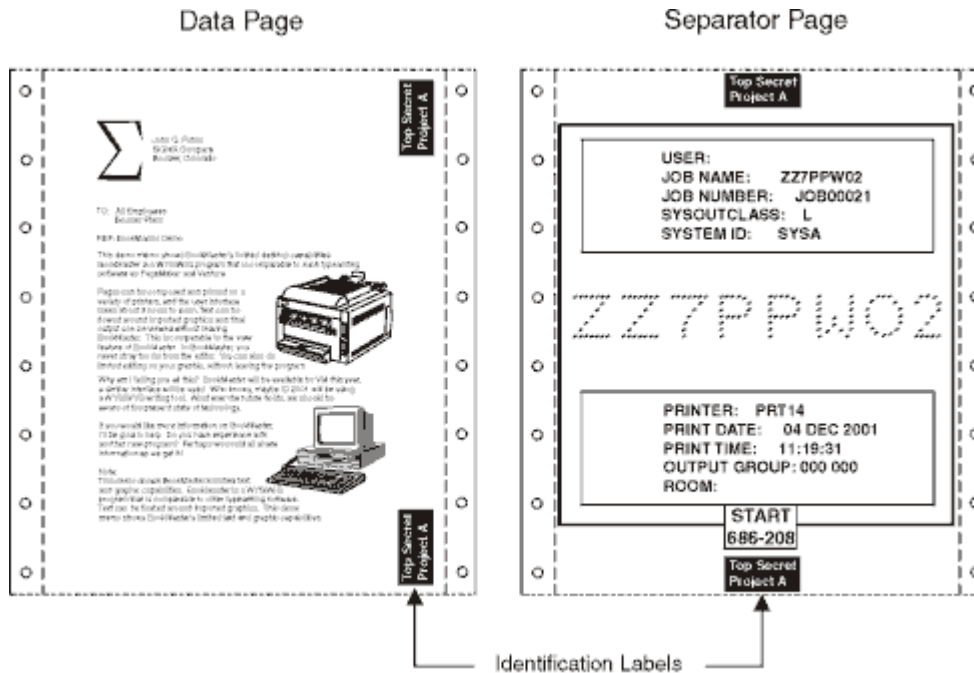


Figure 1. Print labeling

The two types of print labeling are *guaranteed print labeling* and *nonguaranteed print labeling*. Guaranteed print labeling works with a subset of Advanced Function Presentation (AFP) printers and ensures the integrity of the identification label by preventing the user from changing the label. Nonguaranteed print labeling works on most AFP printers, but the integrity of the identification labels cannot be guaranteed. For a list of printers that support print labeling, see [“Printer support in PSF” on page 7](#).

The following steps describe how print labeling works:

1. The user submits a print request that uses data and resources from host libraries. A security label is associated to the print request. The label is a combination of both the security level and the security class.

2. Resource Access Control Facility (RACF®), a component of z/OS Security Server, checks to ensure that the user's security label matches the security labels of all requested user data or user resources. If the labels match, the data is placed on the spool.
3. PSF formats the data and resources by using the security label of the print job to apply the appropriate security overlays to all pages of the printed output.

The integrity of the identification label is ensured by the positioning of the label in an area of the page where user data cannot be placed. To enforce this positioning, the valid printable area of a form for user data is reduced by the definition of a user-printable area.

User-printable area

The user-printable area (UPA) is the area on the page that contains all user-generated data. If an attempt is made to print user-generated data outside the UPA, an exception condition occurs. Identification labels are placed outside of the UPA, but within the valid printable area of the form. [Figure 2 on page 2](#) shows a layout of where an identification label can be placed.

When guaranteed print labeling is enabled, an appropriate UPA must be defined by the system programmer for each paper size that can be used to print data with a particular identification label. Different UPAs can be defined for the same paper size when different identification labels are used.

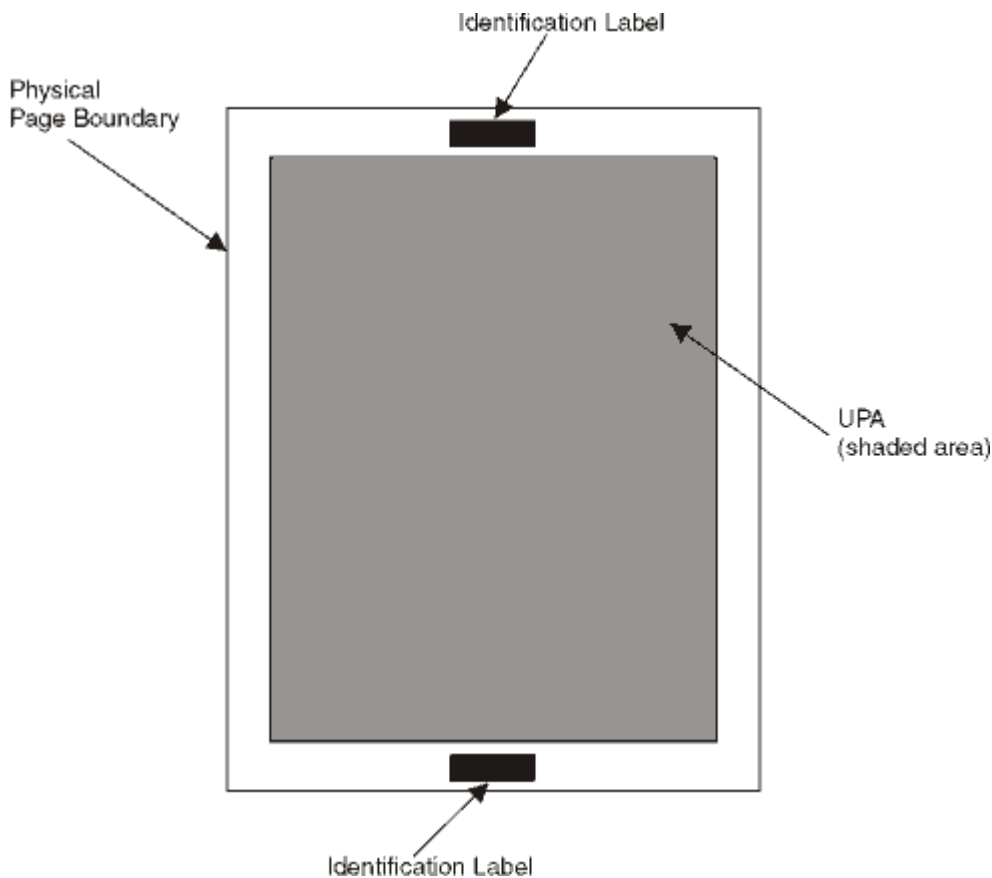


Figure 2. Placing identification labels on the physical page

For a template that you can use to lay out your pages and define the UPA, see [Appendix A, "Security page layout,"](#) on page 25.

Distributing secure PSF output

PSF prints a randomly generated number for each job on the header and the trailer pages of the job if guaranteed print labeling is being done. The printer operator matches the number on the header page to

the number on the trailer page before the job output is distributed. By ensuring that the numbers match, the printer operator ensures output security. Figure 3 on page 3 illustrates the printed numbers.

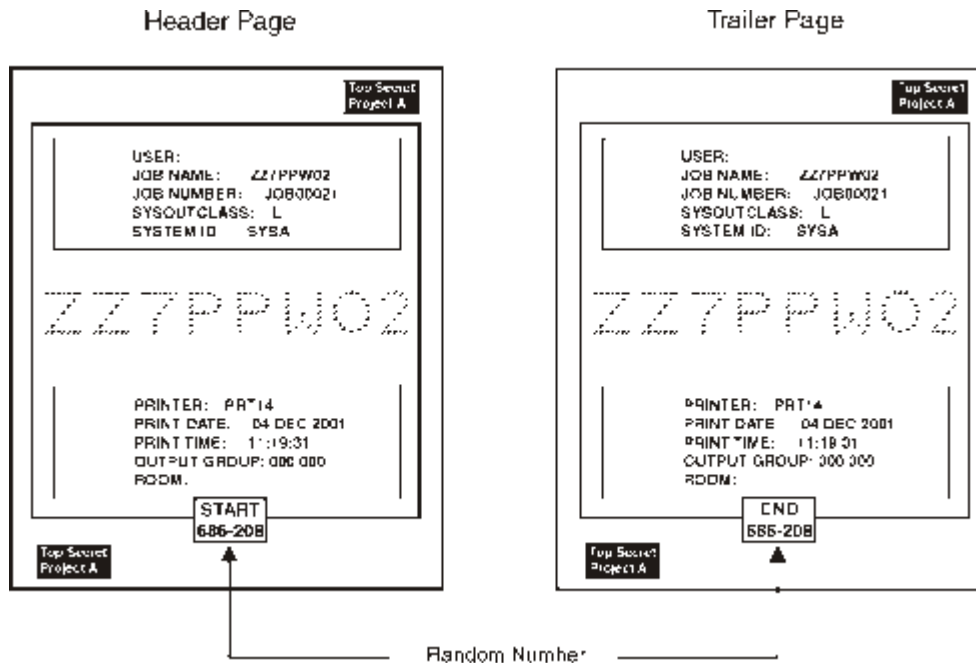


Figure 3. Random numbering of printed output

Auditing PSF output for security

PSF and RACF record security exceptions and help the security administrator audit PSF activity. For more information about auditable conditions, see “Auditing PSF printing” on page 19.

Introducing trusted computing base components

A *trusted computing base* consists of components that together enforce a unified security policy over a computer environment. Components of a trusted computing base include hardware and software. PSF is a software component that is used with hardware and other software components to provide a trusted computing base. Figure 4 on page 4 illustrates a sample trusted computing base.

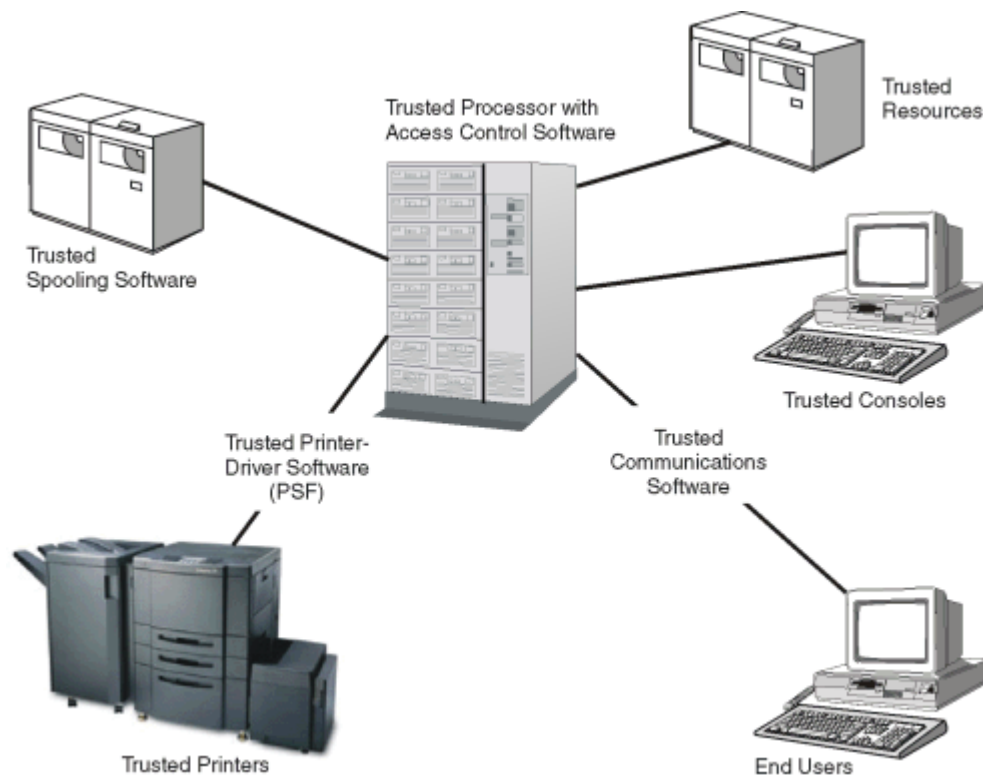


Figure 4. Typical components of a trusted computing base

Trusted software

Trusted software is the software portion of the trusted computing base. It includes:

Access control software

Access control is regulated by RACF, which:

- Authorizes user sessions based on user ID.
- Authorizes resource access.
- Ensures that only users who are identified to RACF can access the processor or resources.

For more information about how to protect processing with RACF, see [z/OS Security Server RACF Security Administrator's Guide](#).

Trusted spooling software

In a trusted computing base, spool files are protected through RACF and your spooling software. For example, in z/OS, the Job Entry Subsystem (JES) spool is protected by activating the RACF JESSPOOL security class and by defining RACF profiles. For information about defining PSF-related RACF profiles, see [“Using RACF with PSF for z/OS”](#) on page 14.

Trusted printer-driver software

In a trusted computing base, secure printed output is controlled through PSF (the printer-driver software) and RACF. Output from a trusted printer contains identification labels that are printed on each page.

Trusted communications software

In a trusted computing base, communications software is used to connect input and output devices to the main processor. For example, Communications Server: IP Services can be used to connect user terminals to the main processor so users communicate with one another.

In a trusted computing base, communication through networking software is controlled through RACF, and communication between users can be restricted or prohibited based on defined security clearances. See your networking software documentation for more information about controlling network access with RACF and for defining security clearances for user terminals.

Trusted resources

In a trusted computing base, some resources are defined as security resources and are managed differently from other resources. For example, fonts, overlays, and page segments that are used to print identification labels are stored in secure libraries, and only the printer driver can access these resources for printing.

Trusted hardware

Trusted hardware is the set of equipment that is protected through RACF in the trusted computing base. It includes:

Trusted processor

In a trusted computing base, the main processor provides access control for admittance to all resources and user processing. Communication between trusted and nontrusted processors is restricted.

Trusted printers

In a trusted computing base, a trusted printer is one that supports guaranteed print labeling. For more information about guaranteed print labeling and printers that support guaranteed print labeling, see [“Printer support in PSF” on page 7](#).

In addition, a trusted printer is located in a controlled area. Only the printer operator is allowed to distribute output to the user.

Trusted console

In a trusted computing base, a trusted console is a computer terminal that is defined to RACF with a security label. In addition, a trusted console is located in a controlled area where only authorized personnel are allowed to access the console.

A trusted console, or *security console*, can still be restricted from accepting certain console operator commands. For example, in z/OS, JES3 commands are grouped into command authority levels, and consoles can be defined to accept only certain levels of JES3 commands from the console operator. For more information about defining a console to RACF, see the RACF documentation for your operating system.

For information about diverting PSF messages from a master console to a security console, see [“Defining a security console” on page 13](#).

Users

In a trusted computing base, the user must be defined to RACF by using a security level and a security class. Both the security level and the security class make up the *security label* of the user. Only users with a security label that is assigned to the user terminal can use the trusted computing base.

Choosing from a list of security-related PSF tasks

Table 2 on [page 5](#) matches personnel with security-related tasks that are described here. You can use this table as a fast path that directs you to security-related tasks contained in this information.

Note: Your installation might or might not have the unique personnel that are listed in the table.

Table 2. Security tasks and the people who do them		
Security-Related Tasks	Personnel	See
Install PSF	System programmer	“Installing PSF” on page 7
Determine how your printer supports print labeling	System programmer and security administrator	“Printer support in PSF” on page 7
Allocate security definitions libraries	System programmer and security administrator	“Allocating the security definitions library” on page 8

<i>Table 2. Security tasks and the people who do them (continued)</i>		
Security-Related Tasks	Personnel	See
Define security definitions library	System programmer and security administrator	“Defining a security definitions library” on page 9
Define security resource libraries	System programmer and security administrator	“Defining security resource libraries” on page 12
Design page layouts for each size of paper	System programmer, security administrator, and application programmer	Appendix A, “Security page layout,” on page 25
Create security overlays	System programmer, security administrator, and application programmer	“Creating security overlays” on page 8
Define security consoles	System programmer and security administrator	“Defining a security console” on page 13
Update the PSF startup procedure	System programmer and security administrator	“Updating initialization parameters” on page 15
Enable print labeling	System programmer and security administrator	“Enabling print labeling” on page 14
Activate separator page content (random numbering)	System programmer or security administrator	“Assembling separator pages” on page 13
Submit a print job that requires identification labels	User who is RACF authorized	“Submitting a print job that includes identification labels” on page 18
Check PSF output for security	Printer operator	“Distributing secure PSF output” on page 2
Diagnose print-labeling problems	System programmer and security administrator	“Diagnosing print labeling problems” on page 20
Interpret security-related error messages	Console operator, system programmer, security administrator, and application programmers	“Interpreting security-related messages” on page 20
Perform security audits	Security administrator and installation auditor	“Auditing PSF printing” on page 19

Chapter 2. Using print labeling

This information describes how to enable, customize, and maintain the print labeling function of PSF for z/OS. The procedures, examples, and parameters described here apply only to a z/OS operating system.

You can find more information in these publications:

- *PSF for z/OS: Customization*
- *PSF for z/OS: User's Guide*
- *Overlay Generation Language/370 User's Guide and Reference*

You must be familiar with PSF customization before you enable the print labeling function.

The tasks that are described in this information can be done in the following sequence. Your installation might not require all tasks.

1. [“Installing PSF” on page 7](#)
2. [“Designing pages for print labeling” on page 7](#)
3. [“Allocating the security definitions library” on page 8](#)
4. [“Defining a security definitions library” on page 9](#)
5. [“Defining security resource libraries” on page 12](#)
6. [“Defining a security console” on page 13](#)
7. [“Assembling separator pages” on page 13](#)
8. [“Enabling print labeling” on page 14](#)
9. [“Updating initialization parameters” on page 15](#)
10. [“Submitting a print job that includes identification labels” on page 18](#)
11. [“Maintaining PSF for z/OS with print labeling enabled” on page 19](#)

Installing PSF

Install PSF as instructed in the *Program Directory for Print Services Facility for z/OS*, which is included with the PSF licensed program tapes. This directory contains information about the microcode levels for specific printers. You need to make sure that the appropriate level of microcode is installed on your printer before your printer can support guaranteed print labeling.

Printer support in PSF

AFP printers can support guaranteed print labeling or nonguaranteed print labeling. To determine the type of print labeling your printer supports in PSF for z/OS, use the display printer information function. If the Define User Area is listed in the DEVICE CONTROL COMMAND Set Vector of the Sense Type and Model (STM), the printer supports guaranteed print labeling; if it is not, the printer supports nonguaranteed print labeling. For more information about the display printer information function, see [PSF for z/OS: Customization](#).

For more information about guaranteed print labeling and nonguaranteed print labeling, see [“Enabling print labeling” on page 14](#).

Designing pages for print labeling

These steps are required to design pages for print labeling:

1. Identify any fonts or page segments that you want to use in the identification label. For information about identifying fonts and page segments, see [“Defining security resource libraries” on page 12](#) and [“Defining data definition names in the PRINTDEV statement” on page 18](#).

2. Construct a page layout. See Appendix A, “Security page layout,” on page 25 for a page layout tool.
3. Create security overlays as needed. See “Creating security overlays” on page 8.
4. Create a security definitions library (allocate and define members). Each combination of security label, paper size, and page top must be defined to PSF in a member of a security definitions library. To define members in a security definitions library, see “Defining a security definitions library” on page 9.

Creating security overlays

You must create at least one security overlay for each security label that you are using on your system. The same overlay can be used on different paper sizes and orientations but the overlay must be carefully designed, considering the media origin and the printable area differences. If you want, more than one security overlay can be created for each combination of security label, paper size, and orientation.

Security overlays are created as you would create other overlays, but RACF is used to protect overlays that are in a secure library from any unauthorized modification. For example, a user of Overlay Generation Language (OGL) needs to be RACF-authorized to access an overlay in a secure library. See your RACF documentation for more information about how users are authorized to access secure libraries. For more information about creating overlays, see *Overlay Generation Language/370 User's Guide and Reference*.

Printing with security overlays

Printing security overlays is not specified with a form definition but with the SECOVLY option. This option is coded in a member of the security definitions library. For more information, see “Defining a security definitions library” on page 9.

Allocating the security definitions library

The *security definitions library* is a partitioned data set or a series of concatenated partitioned data sets. A security definitions library contains separate definitions for each type of security label available on the system. A single member contains the definitions for one security label that is used with all paper sizes and page orientations. For example, a security definitions library that is called SECURE.SECDEFS contains two members, named TOPSEC and UNCL. The member SECURE.SECDEFS(TOPSEC) contains definitions for printing a top secret identification label. The member SECURE.SECDEFS(UNCL) contains definitions for printing an unclassified identification label.

A member of a security definitions library contains the size and origin of the user-printable area (UPA) for each paper size and page orientation that is used by the printer. The security definitions library can optionally contain the names of any security overlays.

You need to define the minimum number of paper sizes that are required for each security label. This definition reduces PSF search time. For example, you can create a security definitions library for all of your printers that use cut-sheet paper and another library for all of your printers that use continuous-forms paper.

Names that are used to identify the security definitions library are defined in a PSF startup procedure. The DD statement is used to associate a security definitions library name to the printer that uses that library. See Figure 16 on page 16 for an example of how a DD statement is used to refer to a security library name.

Security definitions library attributes

You allocate a security definitions library with the attributes that are listed in Figure 5 on page 8.

```
DSORG=PO
LRECL=80
BLKSIZE=multiple_of_80
RECFM={FB | F}
```

Figure 5. Library attributes for the security definitions library

Note: The security definitions library cannot have records that contain machine or American National Standards Institute (ANSI) control characters and cannot use the track overflow feature.

Defining a security definitions library

You define a member in the security definitions library for each security label.

Syntax for a security definitions member

Figure 6 on page 9 illustrates the syntax for a security definitions library member.

```
{PAPERNAME papername | PAPERSIZ width_value height_value }  
[ TOP { NARROW | WIDE } ]  
[ UPAORG xorg_value yorg_value ]  
[ UPADIM xlength_value ylength_value ]  
[ SECOVLY name1 name2...name8 ]
```

Figure 6. Syntax for a security definitions library member

The parameters and values for a security definitions library member are:

{PAPERNAME *papername* | PAPERSIZ *width_value height_value*}

Specifies the size of the paper. You must use either PAPERNAME or PAPERSIZ.

PAPERNAME specifies the system-defined paper names for each paper size. See [Appendix B, “PAPERNAME table for system-defined paper names,”](#) on page 27 for a list of valid names and the dimensions for each system-defined paper name.

PAPERSIZ specifies the width and height of the paper and the units of measurement, either in inches (IN) or in millimeters (MM). The PAPERSIZ parameter is used if the size of the paper that is loaded in the printer does not correspond to one of the PSF system-defined paper names.

The valid values for inches can be from 0 to 22.75. The valid values for millimeters can be from 0 to 577.97. The values do not need to be in the same units and are entered as follows (the decimal point is optional for integer values):

```
nnn.nn {IN | MM}
```

See [Figure 7 on page 11](#) for an example of this parameter.

Note: Make sure that you have a paper definition for every size of paper that might be installed on a printer.

[TOP { NARROW | WIDE }]

Specifies which edge of the paper is the top by identifying whether the media origin² is at the upper-left corner of a narrow or wide edge of the paper. The TOP parameter has two options:

- NARROW is the default and specifies that the security overlays and UPA in this security definition entry use the upper-left corner of a narrow edge of the paper as the media origin.
- WIDE specifies that the security overlays and UPA in this security definition entry use the upper-left corner of a wide edge of the paper as the media origin.

For continuous-forms printers, a security definitions member can contain both a NARROW and WIDE entry if:

- Both narrow and wide forms are used for the security label.³

² Media origin that is used by any security overlays or the media origin that is used by the UPA. For more information about media origins and the coordinate system that is used by AFP printers, see *Intelligent Printer Data Stream Reference*.

³ Narrow forms have perforations on the shorter edge of the paper and tractor holes on the longer edge. Wide forms have perforations on the longer edge of the paper and tractor holes on the shorter edge.

- The form definition contains page-presentation and print-direction controls that change the default media origin.

For cut-sheet printers, only one entry (NARROW) is needed. Because the media origin for cut sheets is always the upper-left corner of a narrow edge, the WIDE option is ignored for cut-sheet forms.

Determine whether to use the WIDE or NARROW entry for continuous-forms printers:

- WIDE for wide forms if the form definition contains LANDSCAPE ACROSS or PORTRAIT DOWN controls.
- WIDE for narrow forms if the form definition contains PORTRAIT ACROSS or LANDSCAPE DOWN controls.
- NARROW for narrow forms if the form definition contains PORTRAIT ACROSS or LANDSCAPE DOWN controls.
- NARROW for wide forms if the form definition contains LANDSCAPE ACROSS or PORTRAIT DOWN controls.

For more information about the page-presentation and print-direction controls in a form definition, see *Page Printer Formatting Aid: User's Guide*. See [Figure 7 on page 11](#) for an example of this parameter.

[UPAORG *xorg_value yorg_value*]

Specifies the origin, in inches (IN) or millimeters (MM), of the UPA.

The origin is expressed as horizontal offsets (*xorg*) and vertical offsets (*yorg*) from the media origin for a particular page size and origin.

The valid values for inches can be from 0 to 22.75. The valid values for millimeters can be from 0 to 577.97. The values do not need to be in the same units and are entered as follows (the decimal point is optional for integer values):

```
nnn.nn {IN | MM}
```

See [Figure 7 on page 11](#) for an example of this parameter.

Note: This parameter is required if Restrict printable area=YES is specified (or is a default) in the Infoprint Server Printer Inventory, SYSAREA=YES is specified (or is a default) in the PRINTDEV statement for the data set, or UPADIM is specified.

[UPADIM *xlength_value ylength_value*]

Specifies the size, in inches (IN) or millimeters (MM), of the UPA.

The size of the UPA is expressed as horizontal (*xlength*) and vertical (*ylength*) dimensions of the UPA for a particular page size and origin.

The valid values for inches can be from 0 to 22.75. The valid values for millimeters can be from 0.1 to 577.97. The values do not need to be in the same units and are entered as follows (the decimal point is optional for integer values):

```
nnn.nn {IN | MM}
```

See [Figure 7 on page 11](#) for an example of this parameter.

Note: This parameter is required if Restrict printable area=YES is specified (or is a default) in the Infoprint Server Printer Inventory, SYSAREA=YES is specified (or is a default) in the PRINTDEV statement for the data set, or UPAORG is specified.

[SECOVLY *name1 name2...name8*]

Specifies the names of the overlays to be used for this security label on both the separator pages and the data pages.

One to eight overlays can be specified. These overlays must be in a security overlay library.

See [Figure 7 on page 11](#) for an example of this parameter.

Notes:

1. Overlay names are restricted to 6 characters; PSF appends a two-character prefix (O1).
2. If fonts or page segments are used in any of these overlays, the fonts must be in a security font library and the page segments must be in a security page-segment library.
3. This parameter is required if Label data pages=YES or Label separator pages=YES is specified in the Infoprint Server Printer Inventory, or DPAGELBL=YES or SPAGELBL=YES is specified in the PRINTDEV statement.

Rules for defining a security definitions member

This list describes the rules for defining a single member in a security definitions library:

- For each PAPERNAME or PAPERSIZ parameter, up to two sets of TOP, UPAORG, UPADIM, and SECOVLY parameters can be specified, one for the TOP WIDE parameter and one for the TOP NARROW parameter. If duplicate parameters within a set are specified, the last option for that parameter is used.
- The TOP parameter, if present, must be specified before the SECOVLY, UPAORG, and UPADIM parameters that correspond to the TOP parameter.
- The UPAORG, UPADIM, and SECOVLY parameters can be specified in any order. Either SECOVLY or both the UPAORG and the UPADIM parameter must be specified. All three can be used together.
- Multiple parameters and options can be specified in a single record.
- The delimiters that separate the parameters and options are one or more consecutive blanks, or the end of the line.
- Comments can be entered in the security member by entering an asterisk (*) as the first nonblank character in a line. The rest of the record is ignored. Comments cannot appear on the same line as the parameters or options.

Note: When the paper is to be cut after printing (for example, 2-up printing), you must take care to create secure overlays that appropriately label each of the subsheets.

Sample security definitions member

The member definition in [Figure 7 on page 11](#) is used when a SECLABEL of TOPSEC is specified in the print job JCL and can be used for two paper types.

```
* SECURE.SECDEFS(TOPSEC)
*** DEFINITION FOR CUT SHEET PAPER
PAPERSIZ 216      MM  11.00  IN
TOP      NARROW
UPAORG   0        IN   1      IN
UPADIM   8.5      IN  10.00  IN
SECOVLY  TOPSEC
*** DEFINITION FOR CONTINUOUS FORMS
PAPERNAME LISTING1
TOP      WIDE
UPAORG   0        IN   1      IN
UPADIM  13.88     IN  10.00  IN
SECOVLY  TOPSEC
* END SECURE.SECDEFS(TOPSEC)
```

Figure 7. Sample coding of a member

The coding for PAPERSIZ in [Figure 7 on page 11](#) produces a layout shown in [Figure 8 on page 12](#).

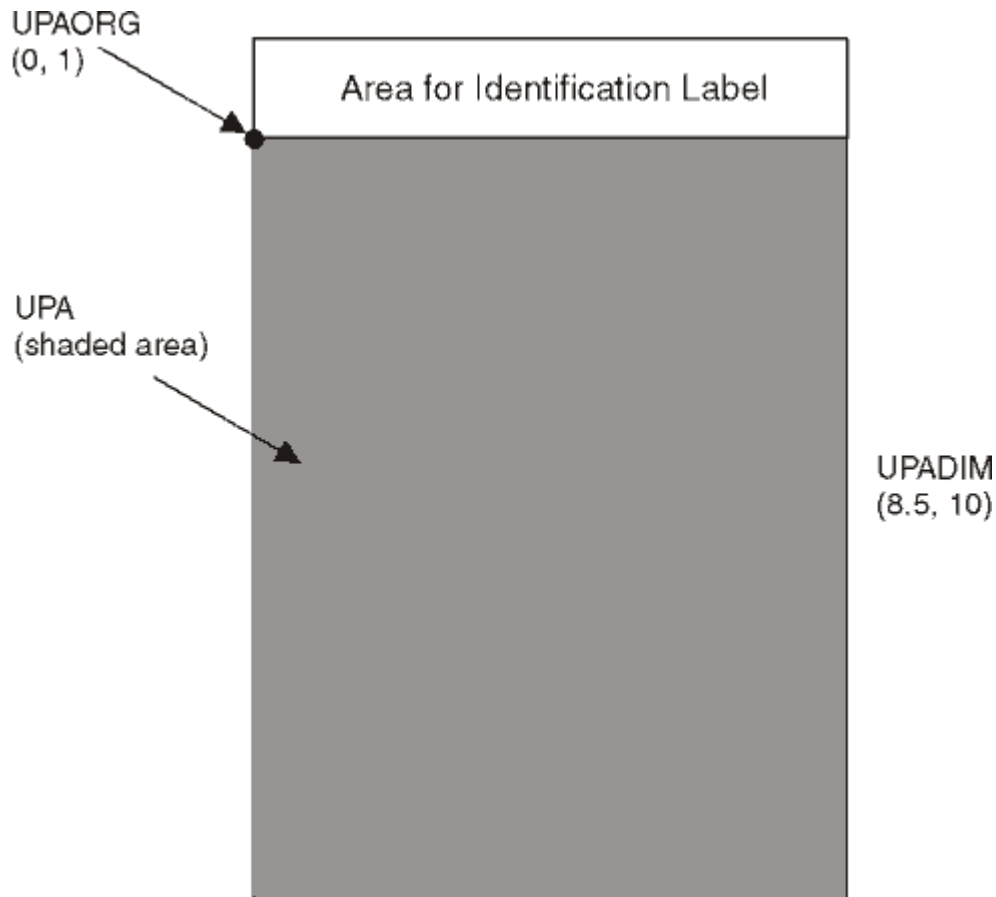


Figure 8. Page layout for a cut-sheet page

The coding for PAPERNAME LISTING1 in [Figure 7 on page 11](#) produces a layout as illustrated in [Figure 9 on page 12](#).

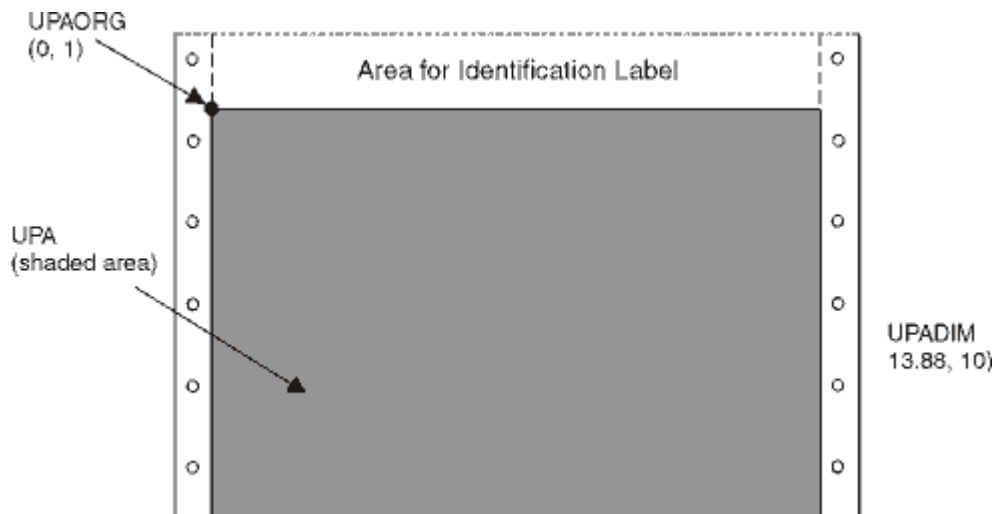


Figure 9. Page layout for a continuous form

Defining security resource libraries

The three types of security resources are overlays, page segments, and fonts. These types of resources are stored in a secure library, and they are managed differently from other resources that are stored on the system. You allocate a security resource library with the attributes that are listed in [Table 3 on page 13](#).

Table 3. Library attributes for a security resource library	
Overlays and Page Segments	Fonts
DSORG=PO LRECL=8205 BLKSIZE=8209 RECFM=VBM	DSORG=PO LRECL=12284 BLKSIZE=12288 RECFM=VBM

Security overlays are produced for each security label defined. One or more security overlays can be defined for each size paper and page orientation that is used. Security fonts and security page segments are used within the security overlay. Security resource libraries are named in the PRINTDEV statement of the PSF startup procedure. See [“Defining data definition names in the PRINTDEV statement” on page 18](#) for the syntax that is used in the PRINTDEV statement.

Defining a security console

You can optionally receive security-related PSF messages at a security console, and you can optionally elect not to receive PSF security-related messages at the master console.

To route messages to a security console, change the ROUTCODE in the SYS1.PARMLIB(CONSOLxx) as illustrated in [Figure 10 on page 13](#).

```
ROUTCODE(9)
```

Figure 10. ROUTCODE option for routing messages

To stop security-related PSF messages from reaching the master console, change the ROUTCODE in SYS1.PARMLIB(CONSOLxx) as shown in [Figure 11 on page 13](#). With this option, all messages except security-related messages reach the master console.

```
ROUTCODE(1-8,10-128)
```

Figure 11. ROUTCODE option for stopping messages

Assembling separator pages

Optional exits are provided if random numbering of separator pages is needed. For information about the exits that PSF provides, see [PSF for z/OS: Customization](#).

The installation exits in [Table 4 on page 13](#) must be modified, assembled, installed, or link-edited with the REPLACE option to print random numbers on job separator pages.

Table 4. PSF exit routines in SYS1.SAMPLIB	
Sample Routine	Description
APSUX01S	Source routine for security job headers.
APSUX02S	Source routine for security job trailers.

Either use the supplied source or modify the source to meet your needs. [Figure 3 on page 3](#) illustrates the IBM-supplied security header and trailer pages in a printed format.

Notes:

1. If APSUX01S and APSUX02S are used, they must replace APSUX01 and APSUX02. Ensure that APSUC01 and APSUC02 are not used. If they are, delete them because they override APSUX01 and APSUX02.
2. Separator pages do not have a UPA.

Enabling print labeling

PSF supports print labeling in two ways:

Guaranteed print labeling

Guaranteed print labeling ensures the integrity of the identification label by preventing the user from changing the label. (See “Printer support in PSF” on page 7 for information about determining whether a printer supports guaranteed print labeling.) Ensure that the RACF option PSFMPL is set according to [Figure 13 on page 14](#).

Nonguaranteed print labeling

Printers that do not support guaranteed print labeling can still print identification labels, but the integrity of the labels cannot be guaranteed. For nonguaranteed print labeling, you must:

1. Define the valid security labels to RACF as described in [z/OS Security Server RACF Security Administrator's Guide](#).
2. Activate security label checking through TSO commands as in [Figure 12 on page 14](#).

In addition, the RACF parameters that are shown in [Figure 13 on page 14](#) are optional for nonguaranteed print labeling. Other parameters in the PSF startup procedure are used to enable nonguaranteed print labeling. For more information, see “Updating initialization parameters” on page 15.

Note: PSF processing is different if print labeling is enabled. See “PSF processing differences with the print labeling function” on page 15 for a list of differences.

```
SETROPTS CLASSACT(SECLABEL)
SETROPTS RACLIST(SECLABEL) REFRESH
```

Figure 12. Activating SECLABEL

Using RACF with PSF for z/OS

Use RACF to activate PSFMPL and create RACF profiles.

Note: RACF CLASS PSFMPL must be refreshed after you activate PSFMPL or create new profiles.

- To activate print labeling, use SETROPTS. To set print labeling defaults to YES, use the RDEFINE command. RDEFINE creates RACF profiles. See [Figure 13 on page 14](#) for examples of using SETROPTS and RDEFINE.

```
SETROPTS CLASSACT(PSFMPL)
RDEFINE PSFMPL PSF.DPAGELBL UACC(NONE)
RDEFINE PSFMPL PSF.SYSAREA UACC(NONE)
```

Figure 13. Using the RACF SETROPTS and RDEFINE commands

- If you want to authorize a print job submitter to override printer defaults, issue the PERMIT commands in [Figure 14 on page 14](#) to add the user ID to the RACF profile.

```
PERMIT PSF.DPAGELBL CLASS(PSFMPL) ID(userid) ACCESS(READ)
PERMIT PSF.SYSAREA CLASS(PSFMPL) ID(userid) ACCESS(READ)
```

Figure 14. Adding a user ID to a RACF profile

- Whenever any of the commands that are shown in [Figure 13 on page 14](#) or [Figure 14 on page 14](#) are used, issue the REFRESH command that is illustrated in [Figure 15 on page 14](#) to refresh RACF.

```
SETROPTS RACLIST(PSFMPL) REFRESH
```

Figure 15. Refreshing RACF

For more information about RACF commands, see [z/OS Security Server RACF Security Administrator's Guide](#).

PSF processing differences with the print labeling function

When you are using the print labeling function, PSF processing is different. The differences include:

- Security resources are accessed only from security libraries. A resource that is loaded in the printer from a security library cannot be used to print user data.
- User resources are accessed only from user resource libraries. A resource that is loaded in the printer from a user library cannot be used to print identification labels.
- Security resources are loaded into the printer as required by the print data set. They typically are not deleted at the end of a data set, except when:
 - The resource deletion exit is used to delete the resources.
 - A job-trailer page is printed.

For more information about resource loading, deleting, and using installation exits, see [PSF for z/OS: Customization](#).

- Suppression of trailer pages by using JES operator commands can impact printer performance because printer storage can be exceeded.
- An audit is done whenever a data set is printed on a nonguaranteed printer.

Printable area considerations

If PSFMPL is active, the **Restrict printable area** parameter in the Infoprint Server Printer Inventory or the SYSAREA parameter in the PRINTDEV statement defaults to YES.

If PSFMPL is not active, the **Restrict printable area** parameter in the Printer Inventory or the SYSAREA parameter in the PRINTDEV statement defaults to NO.

If you are using a nonguaranteed printer, these parameters must be set to NO or an abend occurs. For more information, see [“Updating print labeling parameters” on page 16](#).

Updating initialization parameters

Before you start a PSF functional subsystem (FSS), you must have a cataloged PSF startup procedure in SYS1.PROCLIB or in a procedure library that is concatenated to the JES startup procedure. The PSF startup procedure specifies PSF initialization parameters that tell PSF where security resources and security definitions are located. [Figure 16 on page 16](#) lists a sample PSF startup procedure that includes parameters that are modified for print labeling.

```

//J2PSF00  PROC
//STEP01   EXEC PGM=APSPPIEP,REGION=4M,PARM=(,FULL)
//SYSABEND DD SYSOUT=A
//SYSUDUMP DD SYSOUT=A
//JOBHDR   OUTPUT PAGEDEF=A06462,
//          FORMDEF=A10110
//JOBTLR   OUTPUT PAGEDEF=A06462,
//          FORMDEF=A10110
//DSHDR    OUTPUT PAGEDEF=A06462,
//          FORMDEF=A10110
//MSGDS    OUTPUT PAGEDEF=A06462,
//          FORMDEF=A10110
//FONT01   DD DSN=TEST.FONTLIBB,DISP=SHR
//          DD DSN=SYS1.FONTLIBB,DISP=SHR
//PSEG01   DD DSN=TEST.SEGMENT,DISP=SHR
//          DD DSN=SYS1.SEGMENT,DISP=SHR
//OLAY01   DD DSN=TEST.OVERLAY,DISP=SHR
//          DD DSN=SYS1.OVERLAY,DISP=SHR
//FDEF01   DD DSN=TEST.FORMDEF,DISP=SHR
//          DD DSN=SYS1.FORMDEF,DISP=SHR
//PDEF01   DD DSN=TEST.PAGEDEF,DISP=SHR
//          DD DSN=SYS1.PAGEDEF,DISP=SHR
//SFONT1   DD DSN=SECURE.FONTLIBB,DISP=SHR /* DD statements used for print labeling. */
//SFONT2   DD DSN=SECURE.FONTL240,DISP=SHR /* */
//SFONT3   DD DSN=SECURE.FONTL300,DISP=SHR /* */
//SOLAY1   DD DSN=SECURE.OVERLAY,DISP=SHR /* */
//SPSEG1   DD DSN=SECURE.SEGMENT,DISP=SHR /* */
//SPSEG2   DD DSN=SECURE.SEGMT240,DISP=SHR /* */
//SPSEG3   DD DSN=SECURE.SEGMT300,DISP=SHR /* */
//SDEF1    DD DSN=SECURE.SECDEFS,DISP=SHR /* A member in SDEF1, SDEF2, or SDEF3 */
//SDEF2    DD DSN=SECURE.SECDF240,DISP=SHR /* matches the SECLABEL on the job card. */
//SDEF3    DD DSN=SECURE.SECDF300,DISP=SHR /* */
//PRT10    CNTL
//PRT10    PRINTDEV FONTDD=*.FONT01,
//          OVLYDD=*.OLAY01,
//          PSEGDD=*.PSEG01,
//          PDEFDD=*.PDEF01,
//          FDEFDD=*.FDEF01,
//          JOBHDR=*.JOBHDR,
//          JOBTRLR=*.JOBTLR,
//          DSHDR=*.DSHDR,
//          MESSAGE=*.MSGDS,
//          SFONTDD=*.SFONT1, /* These PRINTDEV statements correspond to */
//          SFONT240=*.SFONT2, /* the DD statements used for print labeling. */
//          SFONT300=*.SFONT3, /* */
//          SOVLY=*.SOLAY1, /* */
//          SPSEGDD=*.SPSEG1, /* */
//          SPSEG240=*.SPSEG2, /* */
//          SPSEG300=*.SPSEG3, /* */
//          SDEFDD=*.SDEF1, /* */
//          SDEF240=*.SDEF2, /* */
//          SDEF300=*.SDEF3, /* */
//          PAGEDEF=A06462,
//          FORMDEF=A10110,
//          CHARS=(60DB),
//          TRACE=YES,
//          DATAK=BLOCK,
//          BUFNO=5,
//          SPAGELBL=YES, /* These parameters enable print labeling if */
//          DPAGELBL=YES, /* PSFMPL is not active. */
//          SYSAREA=YES, /* */
//          PIMSG=YES
//PRT10    ENDCNTL

```

Figure 16. Sample PSF startup procedure with comments for security-related parameters

For more information about PSF initialization parameters, see [PSF for z/OS: Customization](#).

Updating print labeling parameters

You can use the Infoprint Server Printer Inventory, the PRINTDEV statement in the PSF startup procedure, or the OUTPUT JCL statement to enable print labeling. [Table 5 on page 17](#) lists the parameters that you can use.

Using the Printer Inventory is more efficient than using the PSF startup procedure because it avoids the need to restart all the printers in a startup procedure when you change parameters. Only the printer for which parameters are changed needs to be restarted.

Keep in mind:

1. Parameters available in the Printer Inventory are ignored in the PSF startup procedure when the Printer Inventory is used. Therefore, if you use the Printer Inventory, you must specify the parameters in the Printer Inventory instead of the startup procedure.
2. You can use the Printer Inventory component of Infoprint Server without licensing the Infoprint Server feature of z/OS. For more information, see [z/OS Infoprint Server Printer Inventory for PSF](#).

To use the Printer Inventory, you must specify the Printer Inventory name on the INV parameter in the PARM field of the EXEC statement for the startup procedure:

```
// EXEC PGM=APSPPIEP,PARM=('INV=piname')
```

where *piname* is the four-character name of the Printer Inventory that is specified in the Infoprint Server configuration file. For example, `// EXEC PGM=APSPPIEP,PARM=('INV=AOP1')` specifies the default name of the Printer Inventory.

You can use either the Printer Inventory Definition Utility (PIDU) or the Printer Inventory ISPF panels to enable print labeling in the Printer Inventory (for more information, see [PSF for z/OS: Customization](#)). When you are defining parameters on the ISPF panels, see the online help for information about each parameter.

Table 5. Parameters for enabling print labeling				
Printer Inventory		PRINTDEV	OUTPUT	Description
ISPF Panel	PIDU			
Label data pages Values: 1 = Yes 2 = No	label-data-pages Values: yes no	DPAGELBL Values: YES NO	DPAGELBL Values: YES NO	Indicates whether a label is printed on each data page.
Label separator pages Values: 1 = Yes 2 = No	label-separator-pages Values: yes no	SPAGELBL Values: YES NO		Indicates whether a label is printed on a separator page.
Restrict printable area Values: 1 = Yes 2 = No	restrict-printable-area Values: yes no	SYSAREA Values: YES NO	SYSAREA Values: YES NO	Indicates whether the printable area is restricted to the system-defined UPA. If the printable area is restricted, the area outside the UPA is reserved for a security label and any attempt to print in the reserved area results in error messages. If your printer does not support guaranteed print labeling, this parameter must be set to NO.
Note: In these parameters, the default is YES if PSFMPL is active; NO if PSFMPL is not active.				

Defining data definition names in the PRINTDEV statement

These parameters are used to define security-related data definition names in the PRINTDEV statement:

SFONTDD=*.ddname

Defines the default secure font library. This ddname is required if a security overlay references a font.

SFONT240=*.ddname

Defines the secure font library for 240-pel fonts. This ddname is optional if all referenced 240-pel fonts are found in the default secure font library.

SFONT300=*.ddname

Defines the secure font library for 300-pel fonts. This ddname is optional if all referenced 300-pel fonts are found in the default secure font library.

SOVLYDD=*.ddname

Defines the default secure overlay library. This ddname is required if a security overlay is used to print identification labels.

SOVLY240=*.ddname

Defines the secure overlay library for overlays that print best at 240-pel resolution. This ddname is optional if all such overlays are found in the default secure overlay library.

SOVLY300=*.ddname

Defines the secure overlay library for overlays that print best at 300-pel resolution. This ddname is optional if all such overlays are found in the default secure overlay library.

SPSEGDD=*.ddname

Defines the default secure page segment library. This ddname is required if a security overlay references a page segment.

SPSEG240=*.ddname

Defines the secure page segment library for page segments that print best at 240-pel resolution. This ddname is optional if all such page segments are found in the default secure page segment library.

SPSEG300=*.ddname

Defines the secure page segment library for page segments that print best at 300-pel resolution. This ddname is optional if all such page segments are found in the default secure page segment library.

SDEFDD=*.ddname

Defines the default security definitions library. This ddname is required for print labeling.

SDEF240=*.ddname

Defines the security definitions library for printing at 240-pel resolution. This ddname is optional if all such page segments are found in the default security definitions library.

SDEF300=*.ddname

Defines the security definitions library for printing at 300-pel resolution. This ddname is optional if all such page segments are found in the default security definitions library.

These parameters refer to the libraries named in the startup procedure; see [Figure 16 on page 16](#).

Note: Even if you used the Printer Inventory to enable print labeling, you must still specify these parameters in the PRINTDEV statement.

Submitting a print job that includes identification labels

After you define a security definitions library, update PSF initialization parameters, and create security resources, you are ready to submit a print job. To submit a print job and have that job print with the correct identification label, follow this procedure to ensure that a member exists in the security definitions library with the same name as each SECLABEL that is defined to RACF by the security administrator:

1. The security administrator defines a set of security labels to be used by the installation.
2. The security administrator associates SECLABELs with every user on the system.

3. The print administrator creates a member in the security definitions library to match the name of every SECLABEL defined to the system.
4. The user submits the job, the user's SECLABEL is matched and the appropriate security labeling is printed on the user's output.

For example, if you want to print the identification label that is associated with the security label of TOPSEC, specify SECLABEL=TOPSEC in the job card. PSF uses the member that is named SECURE.SECDEFS(TOPSEC) to find the security overlay that is identified for the TOPSEC security label.

Figure 17 on page 19 shows an example of using the SECLABEL parameter in the job card. Figure 7 on page 11 shows an example of the definitions that are used in SECURE.SECDEF(TOPSEC).

```
//TESTER1 JOB (SYS10000),USER=TESTER1,  
// CLASS=A,MSGCLASS=T,MSGLEVEL=(1,1),REGION=4M,  
// SECLABEL=TOPSEC  
.  
.  
.
```

Figure 17. Sample JCL job card

Overriding print labeling defaults

If authorized by RACF, you can use these JCL keywords in the OUTPUT statement to change the definition of print labeling:

DPAGELBL=YES|NO

Indicates whether a label is printed on each data page.

SYSAREA=YES|NO

Indicates whether the printable area is restricted to the system-defined UPA.

If SYSAREA=YES is specified, any attempt to print outside the UPA results in error messages.

If your printer does not support guaranteed print labeling, use SYSAREA=NO. To determine whether your printer supports guaranteed print labeling, see “Printer support in PSF” on page 7.

Figure 18 on page 19 shows an example of the OUTPUT statement that is used to override PSF defaults.

```
.  
.  
.  
//OUTPUT1 OUTPUT FORMDEF=IPGP00,DATAACK=UNBLOCK,  
// DPAGELBL=YES,SYSAREA=NO  
//SYSUT1 DD SYSOUT=L,DCB=(RECL=VBA,BLKSIZE=8192),  
// OUTPUT=*.OUTPUT1
```

Figure 18. Sample JCL output statement

Maintaining PSF for z/OS with print labeling enabled

The following information is used to maintain PSF when print labeling is enabled.

Auditing PSF printing

PSF uses the SMF type 6 record to audit certain events that can indicate a security exception. Only one record is written per data set, but the record can contain numerous conditions.

The following information is included in the SMF type 6 record to support print labeling:

- Indicator that flags JCL keywords that are in effect during printing.
- Indicator that flags a successful print operation.
- Indicator that flags an error that occurred during overlay processing.
- Indicator that flags a hardware error that occurred.
- Indicator that flags printed job-trailer pages.

- Indicator that flags printed job-header pages.
- Indicator that flags that the user suppressed data-page labeling.
- Indicator that flags that the user suppressed UPA enforcement.
- Identifier for the job or group identifier for the data set.
- Identifier for the page definition name.
- Identifier for the form definition name.
- Identifier for the number of security overlays that are used.
- Identifier for the number of security fonts that are used.
- Identifier for the number of security page segments that are used.

For more information about the SMF type 6 record that PSF generates, see [*PSF for z/OS: Customization*](#).

Interpreting security-related messages

If you receive a PSF error message that relates to print labeling, see [*PSF for z/OS: Messages and Codes*](#) for more information.

PSF security-related messages are received at these locations:

- Within a print job
- At the security console
- At the master console

A PSF message number can be placed in these JES messages:

- HASP704
- IAT706I

Diagnosing print labeling problems

The problems in [Table 6 on page 21](#) can occur when you are using the print labeling function.

Table 6. Print labeling diagnosis

Problem	Possible Causes
<p>No identification label is printed on any page.</p>	<ul style="list-style-type: none"> • Security definitions library member does not name a security overlay or names an overlay that does not contain any labeling information. • PSFMPL is not active and: <ul style="list-style-type: none"> – Label data pages and Label separator pages are not specified in the Printer Inventory or DPAGELBL and SPAGELBL are not specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=NO and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but separator pages were suppressed by an operator command. – Label data pages=YES and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but separator pages were suppressed by an operator command and the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file. • PSFMPL is active and: <ul style="list-style-type: none"> – Label data pages=NO and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file and is RACF-authorized to override data page labeling. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but separator pages were suppressed by an operator command. – Label data pages=YES and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but separator pages were suppressed by an operator command and the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file and is RACF-authorized to override data page labeling.

Table 6. Print labeling diagnosis (continued)

Problem	Possible Causes
Identification label is printed on separator pages, but is not printed on data pages.	<ul style="list-style-type: none"> • PSFMPL is not active and: <ul style="list-style-type: none"> – Label separator pages=YES but Label data pages is not specified in the Printer Inventory, or SPAGELBL=YES but DPAGELBL is not specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file. • PSFMPL is active and: <ul style="list-style-type: none"> – Label data pages=NO but Label separator pages is not specified in the Printer Inventory, or DPAGELBL=NO but SPAGELBL is not specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=NO on the OUTPUT statement for the file and is RACF-authorized to override data page labeling.

Table 6. Print labeling diagnosis (continued)

Problem	Possible Causes
Identification label is printed on data pages, but is not printed on separator pages.	<ul style="list-style-type: none"> • PSFMPL is not active and: <ul style="list-style-type: none"> – Label data pages=YES but Label separator pages is not specified in the Printer Inventory, or DPAGELBL=YES but SPAGELBL is not specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=NO and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=YES on the OUTPUT statement for the file. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=YES on the OUTPUT statement for the file and separator pages were suppressed by an operator command. • PSFMPL is active and: <ul style="list-style-type: none"> – Label separator pages=NO but Label data pages is not specified in the Printer Inventory, or SPAGELBL=NO but DPAGELBL is not specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=YES and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=YES and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file. – Label data pages=NO and Label separator pages=NO are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=NO are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=YES on the OUTPUT statement for the file. – Label data pages=NO and Label separator pages=YES are specified in the Printer Inventory or DPAGELBL=NO and SPAGELBL=YES are specified in the PRINTDEV statement for the printer that printed the file, but the print-job submitter specified DPAGELBL=YES on the OUTPUT statement for the file and separator pages were suppressed by an operator command.
Wrong data in identification label.	<ul style="list-style-type: none"> • Print-job submitter specified wrong SECLABEL on job card. • Wrong security overlay is specified in the security definitions library member for the SECLABEL on the job card and the size of paper in the printer that printed the file. • Security definitions library member names an overlay that contains the wrong labeling information. • Overlay names were changed in the security overlay library.
Wrong page segment in identification label.	<ul style="list-style-type: none"> • Security overlay is named the wrong page segment. • Page segment names were changed in the security page segment library.

Table 6. Print labeling diagnosis (continued)

Problem	Possible Causes
Wrong overlay is used for identification label.	<ul style="list-style-type: none">• Print-job submitter specified wrong SECLABEL on job card.• Wrong security overlay is specified in the security definitions library member for the SECLABEL on the job card and the size of paper in the printer that printed the file.• Overlay names were changed in the security overlay library.

Appendix A. Security page layout

The template in [Figure 19 on page 25](#) is provided to help you determine the dimensions that you need when you design pages for the print labeling function. This template can be used to help define where identification label placement occurs and to help determine the dimensions of the user-printable area (UPA). For information about using these measurements to code a security definition, see [“Defining a security definitions library” on page 9](#). To determine the printable area dimensions your printer supports, see the documentation that is provided with the printer.

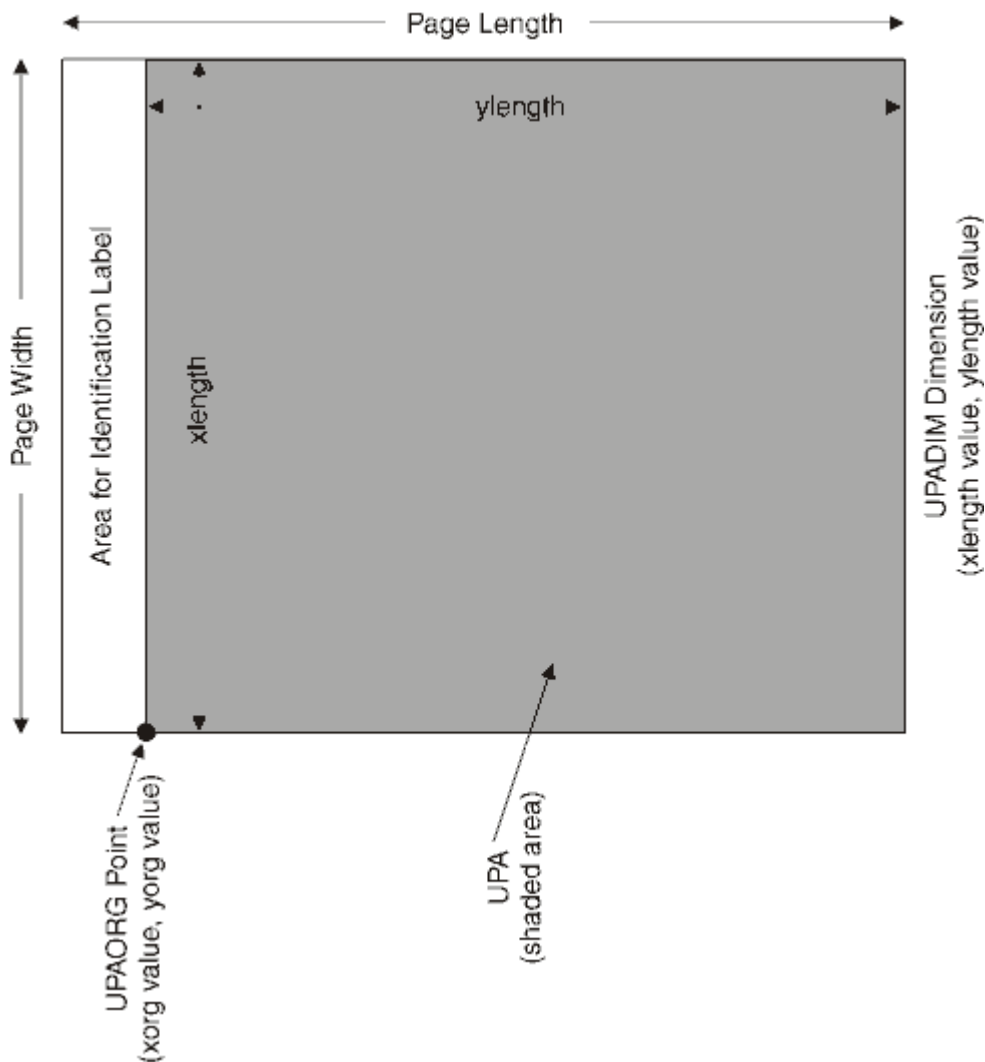


Figure 19. Security page layout

Appendix B. PAPERNAME table for system-defined paper names

Table 7 on page 27 lists the paper names that you can select for the PAPERNAME parameter.

Table 7. PAPERNAME parameter values		
Paper Name	Paper Size: Width by Height in Millimeters	Paper Size: Width by Height in Inches
A4	210 x 297	8.27 x 11.69
B4	257 x 364	10.12 x 14.33
B5	182 x 257	7.17 x 10.12
EXEC1	178 x 267	7.00 x 10.50
EXEC2	184 x 267	7.25 x 10.50
EXEC3	190 x 267	7.50 x 10.50
LEGAL	216 x 356	8.50 x 14.00
LETTER	216 x 279	8.50 x 11.00
LISTING1	378 x 279	14.88 x 11.00
LISTING2	305 x 216	12.00 x 8.50

Appendix C. Accessibility

Accessible publications for this product are offered through [IBM Documentation \(www.ibm.com/docs/en/zos\)](http://www.ibm.com/docs/en/zos).

If you experience difficulty with the accessibility of any z/OS documentation see [How to send feedback to IBM \(www.ibm.com/docs/zos/3.1.0?topic=how-send-feedback\)](http://www.ibm.com/docs/zos/3.1.0?topic=how-send-feedback) to leave documentation feedback.

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation
Site Counsel
2455 South Road*

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those

products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: [IBM Lifecycle Support for z/OS \(www.ibm.com/software/support/systemsz/lifecycle\)](http://www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at [Copyright and Trademark information \(www.ibm.com/legal/copytrade.shtml\)](http://www.ibm.com/legal/copytrade.shtml).

UNIX is a registered trademark of The Open Group in the United States and other countries.

Glossary

This glossary defines technical terms and abbreviations used in PSF for z/OS documentation.

These cross-references are used in this glossary:

See

Refers to preferred synonyms or to defined terms for acronyms and abbreviations.

See also

Refers to related terms that have similar, but not synonymous, meanings, or to contrasted terms that have opposite or substantively different meanings.

A

access control

The process of ensuring that users can access only those resources of a computer system for which they are authorized.

C

concatenated data set

A group of logically connected data sets that are treated as one data set for the duration of a job step. See also [data set](#), [partitioned data set](#), and [library](#).

console

A display station from which an operator can control and observe the system operation.

D

data set

The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access. See also [file](#), [concatenated data set](#), [partitioned data set](#), and [sequential data set](#).

data set header

A page in printed output that separates multiple data sets or multiple copies of a data set within a print job. See also [job header](#).

F

file

1. A collection of related data that is stored and retrieved by an assigned name. A file can include information that starts a program (program-file object), contains text or graphics (data-file object), or processes a series of commands (batch file).
2. See also [data set](#), [partitioned data set](#), [sequential data set](#), and [library](#).

font

1. A family or assortment of characters of a given size and style, for example, 9-point Bodoni modern. A font has a unique name and might have a registry number.
2. A particular type style (for example, Bodoni or Times Roman) that contains definitions of character sets, marker sets, and pattern sets.

form definition

An AFP resource object used by PSF that defines the characteristics of the form or printed media, including: overlays to be used, duplex printing, text suppression, the position of composed-text data on the form, and the number and modifications of a page.

FSA

See [functional subsystem application](#).

FSS

See [functional subsystem](#).

functional subsystem (FSS)

An extension of JES that runs in an address space separate from the JES address space. An FSS provides support for an auxiliary function to JES processing, such as a peripheral device or other component.

functional subsystem application (FSA)

1. An area within the functional subsystem (FSS) that drives and manages a single printer. FSAs are identified with JES printer definitions.
2. An application that uses the support facilities of the functional subsystem (FSS) to communicate with JES.

G

guaranteed print labeling

A method of print labeling that ensures the integrity of the identification label by preventing the user from changing the label. If attempts are made to override print labeling, printing is stopped, and an audit record is written. See also [nonguaranteed print labeling](#) and [identification label](#).

I

identification label

In PSF, a protected set of resources (fonts, overlays, and page segments) that are used to label PSF output for security purposes. See also [security label](#).

Infoprint Server

An element of z/OS that supports printing on local printers and remote printers in an Internet Protocol or SNA network. With Infoprint Server, users can submit print requests from remote workstations in an Internet Protocol network, from z/OS UNIX System Services applications, from batch applications, from VTAM® applications (such as CICS® or IMS), and from SAP R/3.

J

JCL

See [job control language](#).

JES

See [Job Entry Subsystem](#).

JES2

An MVS subsystem that receives jobs into the system, converts them to internal format, selects them for processing, processes their output, and purges them from the system. In an installation with more than one processor, each JES2 processor independently controls its job input, scheduling, and output processing. See also [Job Entry Subsystem](#) and [JES3](#).

JES3

An MVS subsystem that receives jobs into the system, converts them to internal format, selects them for processing, processes their output, and purges them from the system. In complexes that have several loosely coupled processing units, the JES3 program manages processors so that the global processor exercises centralized control over the local processors and distributes jobs to them by using a common job queue. See also [Job Entry Subsystem](#) and [JES2](#).

job

A separately executable unit of work.

job control language (JCL)

A command language that identifies a job to an operating system and describes the job's requirements.

Job Entry Subsystem (JES)

An IBM licensed program that receives jobs into the system and processes all output data that is produced by jobs. See also [JES2](#) and [JES3](#).

job header

A page in printed output that indicates the beginning of a user job. A user job can contain one or more data sets, or one or more copies of a print job. See also [data set header](#).

job separation

The ability to identify job boundaries by placing marks or sheets of paper between successive jobs.

job trailer

A page in the printed output that indicates the end of a user job.

L**library**

1. A system object that serves as a directory to other objects. A library groups related objects, and allows the user to find objects by name.
2. A data file that contains copies of a number of individual files and control information that allows them to be accessed individually.
3. A partitioned data set or a series of concatenated partitioned data sets.

licensed program

A separately priced program and its associated materials that bear a copyright and are offered to customers under the terms and conditions of a licensing agreement.

M**media origin**

The reference point from which the logical page origin is positioned by the medium map. This point is represented by $X_m=0$, $Y_m=0$ in the X_m , Y_m coordinate system. The media origin is defined relative to the upper-left corner of the form. See also [logical page origin](#). See also .

Multiple Virtual Storage (MVS)

An IBM operating system that accesses multiple address spaces in virtual storage.

N**nonguaranteed print labeling**

Some printers that do not support guaranteed print labeling can still print identification labels, but the integrity of the labels cannot be guaranteed by using PSF. See also [guaranteed print labeling](#).

O**OGL**

See [Overlay Generation Language](#).

operating system (OS)

A collection of system programs that control the overall operation of a computer system.

OS

See [operating system](#).

overlay

1. A resource object that contains predefined presentation data, such as text, image, graphics, and bar code data, that can be merged with variable data on a page or form while printing.
2. The final representation of a collection of predefined presentation data on a physical medium.

Overlay Generation Language (OGL)

An IBM licensed program used for designing objects (such as lines, boxes, shadings, and irregular shapes) for electronic overlays.

P

page definition

An AFP resource object used by PSF that defines the rules for transforming line data and XML data into MO:DCA data and text controls, such as width of margins and text orientation.

Page Printer Formatting Aid (PPFA)

An IBM licensed program with which to create and store form definitions and page definitions, which are resource objects used for print-job management. These stored objects are used to format printed output.

page segment

An AFP resource object containing text, image, graphics, or bar code data that can be positioned on any addressable point on a page or an electronic overlay.

parameter

A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

partitioned data set (PDS)

A data set in direct-access storage that is divided into partitions, called members, each of which can contain a program, part of a program, or data. See also [sequential data set](#).

PDS

See [partitioned data set](#).

physical page

A single surface (front or back) of a form.

PPFA

See [Page Printer Formatting Aid](#).

Printer Control Language (PCL)

The Hewlett Packard page description language that is used in laser and ink-jet printers.

Printer Inventory

In Infoprint Server, a set of files that contain information about printers. The Printer Inventory includes such objects as printer definitions, functional subsystem (FSS) definitions, and job selection rules for IP PrintWay.

print job

One or more documents submitted in the same job to be printed on the same printer.

print labeling

A controlled method of placing identification labels on each page of PSF printed output.

Print Services Facility (PSF)

An IBM licensed program that manages and controls the input data stream and output data stream required by supported page printers.

processor

In a computer, the part that interprets and processes instructions. Two typical components of a processor are a control unit and an arithmetic logic unit.

PSF

See [Print Services Facility](#).

R

RACF

See [Resource Access Control Facility](#).

record

1. In programming languages, an aggregate that consists of data objects, possibly with different attributes, that typically have identifiers attached to them. In some programming languages, records are called structures.

2. A group of related data, words, or fields treated as a unit, such as one name, address, and telephone number.

resource

A collection of printing instructions used, in addition to the print data set, to produce the printed output. Resources include coded fonts, font character sets, code pages, page segments, overlays, form definitions, and page definitions.

Resource Access Control Facility (RACF)

An IBM licensed program that provides for access control by identifying users to the system, verifying users of the system, authorizing access to protected resources, logging unauthorized attempts to enter the system, and logging accesses to protected resources.

S**security definition**

A member containing the definitions for one identification label. These definitions include instructions for the overlay name, and the size and origin of paper to be used.

security definitions library

A partitioned data set or a series of concatenated partitioned data sets that contain the security definitions for an entire system.

security label

In a trusted computing base, a label used to maintain multiple levels of security on a system. This label is a combination of a security class and a security level. See also [identification label](#).

security overlay

An overlay, such as one created by use of Overlay Generation Language, that resides in a secure library and is used to place security resources on a page.

separator page

An identifying sheet of paper between successive jobs. See also [job header](#) and [job trailer](#).

sequential data set

A data set whose records are organized on the basis of their successive physical positions, such as on magnetic tape. See also [partitioned data set](#).

SMF

See [System Management Facilities](#).

SMF type 6 record

A record that PSF uses to record data for each print data set.

spool

The system function of putting files or jobs into disk storage for later processing or printing. An abbreviation for *simultaneous peripheral operations online*.

spool file

1. A file containing output that has been saved for later processing.
2. A file that is used in the transmission of data among devices.

spooling

The sending of data to auxiliary storage for later processing. The most common spooling application is print spooling.

statement

1. In programming languages, a language construct that represents a step in a sequence of actions or a set of declarations.
2. An instruction in a program or procedure.

System Management Facilities (SMF)

A component of z/OS that collects and records a variety of system and job-related information. Examples of information collected by SMF are statistics, accounting information, and performance data.

T

terminal

In data communication, a device, typically equipped with a keyboard and display device, capable of sending and receiving information.

trusted computing base

The part of the system that contains all the elements that support the security policy of the system. The trusted computing base includes all hardware, microcode, and software that protect information on the system.

U

UPA

See [user printable area](#).

user ID

See [user identifier](#).

user identifier

A string of characters that uniquely identifies a user to a system.

user printable area (UPA)

The area within the valid printable area (VPA) where user-generated data can print without causing an exception condition. See also [valid printable area](#).

V

valid printable area (VPA)

The intersection of the current logical page or current overlay with the physical page in which printing is allowed. See also [user printable area](#).

VPA

See [valid printable area](#).

X

Xm, Ym coordinate system

The media coordinate system.

Z

z/OS

An IBM mainframe operating system that uses 64-bit real storage.

Bibliography

This bibliography lists the titles of publications containing additional information about PSF, AFP, the z/OS operating system, and related products.

The titles and order numbers might change from time to time. To verify the current title or order number, consult your IBM marketing representative.

You can obtain many of the publications listed in this bibliography from the AFP Consortium Publications (afpcinc.org/publications), the IBM Documentation (www.ibm.com/docs/en), and the IBM Publications Center (www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss).

Advanced Function Presentation (AFP)

The AFP publications in [Table 8 on page 41](#) are available from [AFP Consortium Publications \(afpcinc.org/publications\)](http://afpcinc.org/publications).

<i>Table 8. AFP publications available from the AFP Consortium</i>	
Publication	Order Number
<i>Advanced Function Presentation: Programming Guide and Line Data Reference</i>	S544-3884
<i>AFP Consortium: AFP Color Management Architecture (ACMA)</i>	AFPC
<i>Bar Code Object Content Architecture Reference</i>	AFPC-0005
<i>Color Management Object Content Architecture Reference</i>	AFPC-0006
<i>Font Object Content Architecture Reference</i>	AFPC-0007
<i>Graphics Object Content Architecture for AFP Reference</i>	AFPC-0008
<i>Guide to Advanced Function Presentation</i>	G544-3876
<i>Image Object Content Architecture Reference</i>	AFPC-0003
<i>Intelligent Printer Data Stream Reference</i>	AFPC-0001
<i>Mixed Object Document Content Architecture Reference</i>	AFPC-0004
<i>Overlay Generation Language/370 User's Guide and Reference</i>	S544-3702
<i>Presentation Text Object Content Architecture Reference</i>	AFPC-0009

The AFP publications in [Table 9 on page 41](#) are available from the [IBM Documentation \(www.ibm.com/docs/en\)](http://www.ibm.com/docs/en) and the [IBM Publications Center \(www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss\)](http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss). For best results, search the IBM Publications Center by order number.

The AFP publications in [Table 10 on page 41](#) are available from the [IBM Publications Center \(www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss\)](http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss). For best results, search the IBM Publications Center by order number.

<i>Table 10. AFP publications available from the IBM Publications Center</i>	
Publication	Order Number
<i>AFP Toolbox User's Guide</i>	S544-5292
<i>Guide to Advanced Function Presentation</i>	G544-3876

Index

A

- accessibility
 - contact IBM [29](#)
- activating print labeling with RACF [14](#)
- activating security labeling checking [14](#)
- adding user IDs to RACF profiles [14](#)
- allocating security resource libraries [12](#)
- allocating the security definitions library [8](#)
- areas, physical page [2](#)
- assembling separator pages [13](#)
- assistive technologies [29](#)
- attributes for security definitions library [8](#)
- auditing printing [19](#)
- auditing PSF output for security [3](#)

C

- commands, RACF
 - PERMIT [14](#)
 - RDEFINE [14](#)
 - REFRESH [14](#)
 - SETOPTS [14](#)
- computing base, trusted [3](#)
- consoles, defining security [13](#)
- contact
 - z/OS [29](#)
- creating RACF profiles [14](#)
- creating security overlays [8](#)

D

- data definition names, defining [18](#)
- DD statements
 - SDEF240
 - SDEF300 [18](#)
 - SFONT300 [18](#)
 - SOVLY300 [18](#)
 - SPSEG300 [18](#)
 - SDEFDD [18](#)
 - SFONT240 [18](#)
 - SFONTDD [18](#)
 - SOVLY240 [18](#)
 - SOVLYDD [18](#)
 - SPSEG240 [18](#)
 - SPSEGDD [18](#)
- defaults, overriding print labeling [19](#)
- defining
 - security consoles [13](#)
 - security definitions library [9](#)
 - security resources [12](#)
 - security-related data definition names [18](#)
- deleting security resources [15](#)
- designing pages for print labeling [7](#)
- diagnosing print labeling problems [20](#)
- distributing secure PSF output [2](#)
- DPAGELBL parameter [16](#)

E

- enabling print labeling [14](#)
- error messages, interpreting [20](#)
- exits for assembling separator pages [13](#)

F

- feedback [xi](#)

G

- guaranteed print labeling [14](#)

H

- hardware, trusted [5](#)

I

- identification labels
 - description of [1](#)
 - layout for [2](#), [25](#)
 - printing correct [18](#)
- Infoprint Server Printer Inventory, specifying [16](#)
- initialization parameters, updating [15](#)
- installation exits for separator pages [13](#)
- installing PSF [7](#)
- interpreting error messages [20](#)

J

- JES messages, interpreting [20](#)

K

- keyboard
 - navigation [29](#)
 - PF keys [29](#)
 - shortcut keys [29](#)

L

- Label data pages parameter [16](#)
- Label separator pages parameter [16](#)
- label, security [1](#), [5](#)
- layout, security page [25](#)
- libraries
 - attributes for [8](#)
 - defining security definitions [9](#)
 - defining security resource [12](#)
- loading security resources [15](#)

M

maintaining PSF with print labeling enabled [19](#)
messages, interpreting [20](#)

N

names, system-defined paper [27](#)
navigation
 keyboard [29](#)
nonguaranteed print labeling [14](#)
numbering, random job [2](#)

O

OUTPUT statement for overriding defaults [19](#)
overlays, creating security [8](#)
overriding print labeling defaults [19](#)

P

page layout template [25](#)
pages, designing for print labeling [7](#)
paper names, system-defined [27](#)
PAPERNAME parameter [27](#)
parameters and options
 DD statement [18](#)
 PAPERNAME [27](#)
 PRINTDEV statement [16](#), [18](#)
 Printer Inventory [16](#)
 PSFMPL [14](#)
 SECLABEL [18](#)
 SECLABEL in RACF [14](#)
 security definitions library [8](#)
PERMIT command [14](#)
physical page, printable area [2](#)
print job, submitting secure [18](#)
print labeling function
 activating with PSFMPL [14](#)
 allocating the security definitions library [8](#)
 assembling separator pages [13](#)
 defining
 security consoles [13](#)
 security definitions library [9](#)
 security resource libraries [12](#)
 designing pages [7](#)
 diagnosing problems [20](#)
 enabling [14](#)
 guaranteed [14](#)
 installing PSF [7](#)
 maintaining PSF with print labeling enabled [19](#)
 nonguaranteed [14](#)
 overriding defaults [19](#)
 page template [25](#)
 printer support for [7](#)
 PSF processing differences [15](#)
 random numbering of printed output [2](#)
 security auditing of output [3](#)
 security-related PSF tasks [5](#)
 submitting secure print jobs [18](#)
 trusted computing base components [3](#)
 understanding [1](#)
 updating initialization parameters [15](#)

print labeling function (*continued*)
 using [7](#)
Print Services Facility (PSF)
 auditing printing [19](#)
 distributing secure output [2](#)
 error messages, interpreting [20](#)
 installing [7](#)
 maintaining with print labeling enabled [19](#), [20](#)
 printer support in [7](#)
 processing differences with print labeling [15](#)
 security auditing of output [3](#)
 security-related tasks [5](#)
 using print labeling [7](#)
printable area considerations [15](#)
printable areas on a physical page
 print labeling function
 UPA [2](#)
PRINTDEV statement parameters [16](#), [18](#)
Printer Inventory parameters [16](#)
printer support for print labeling [7](#)
problems, diagnosing print labeling [20](#)
processing differences with print labeling [15](#)
profiles, creating RACF [14](#)
PSFMPL option [14](#)
publications, related [41](#)

R

RACF
 adding user IDs to profiles [14](#)
 profiles, creating [14](#)
 refreshing [14](#)
random numbering for print labeling [2](#)
RDEFINE command [14](#)
refreshing RACF [14](#)
related publications [41](#)
resources
 defining security [12](#)
 loading and deleting security [15](#)
Restrict printable area parameter [16](#)
rules for defining a security definitions member [11](#)

S

sample security definitions member [11](#)
SDEF240 parameter [18](#)
SDEF300 parameter [18](#)
SDEFDD parameter [18](#)
SECLABEL option in RACF [14](#)
SECLABEL parameter [18](#)
secure print jobs, submitting [18](#)
secure PSF output, distributing [2](#)
security auditing of PSF output [3](#)
security consoles, defining [13](#)
security definitions library
 allocating [8](#)
 attributes [8](#)
 defining [9](#)
 rules for defining a member [11](#)
 sample member [11](#)
 syntax for members [9](#)
security label [1](#), [5](#)
security overlays, creating [8](#)

- security page layout [25](#)
- security resource library, allocating and defining [12](#)
- security resources, loading and deleting [15](#)
- security-related messages, interpreting [20](#)
- security-related tasks [5](#)
- sending to IBM
 - reader comments [xi](#)
- separator pages, assembling [13](#)
- SETRPTS command [14](#)
- SFONT240 parameter [18](#)
- SFONT300 parameter [18](#)
- SFONTDD parameter [18](#)
- shortcut keys [29](#)
- SMF type 6 record auditing [19](#)
- software, trusted [4](#)
- SOVLY240 parameter [18](#)
- SOVLY300 parameter [18](#)
- SOVLYDD parameter [18](#)
- SPAGELBL parameter [16](#)
- SPSEG240 parameter [18](#)
- SPSEG300 parameter [18](#)
- SPSEGDD parameter [18](#)
- submitting secure print jobs [18](#)
- syntax for security definitions member [9](#)
- SYSAREA parameter [16](#)
- system-defined paper names [27](#)

T

- tasks, security-related [5](#)
- trusted computing base
 - hardware [5](#)
 - software [4](#)
 - users [5](#)

U

- UPA [2](#)
- updating initialization parameters [15](#)
- user IDs, adding to RACF profiles [14](#)
- user interface
 - ISPF [29](#)
 - TSO/E [29](#)
- user security label [5](#)
- user-printable area [2](#)



Product Number: 5655-M32

S550-0434-05

