US e-Mail™

Multi-Function Gateway (MFG) Security Policy Selection Table (SPST)/ Security Policy Translation Table (SPTT) Toolset

User's Guide

Document Part #: /cpe/mfg/SPTT/002

COMM
POWER

Document Part Number and Revision:

MFG SPST/SPTT Toolset User's Guide
Document Part Number: /cpe/mfg/SPTT/002

Revision History:

Date	Document Revision
April 2000	001
August 2000	002

This document describes the procedures for using the MFG SPST/SPTT Toolset.

Copyright Notice:

COMM POWER

CommPower, Inc.
1040 Flynn Road
Camarillo, CA 93012-8016
Telephone: 1 805 389 7414
Fax: 1 805 389 7419
e-Mail: Internet (info@commpower.com)

MFG SPST/SPTT TOOLSET
USER'S GUIDE
TABLE OF CONTENTS

COMM
POWER

Chapter 1.
OVERVIEW

This document describes how to use the US e-Mail Multi-Function Gateway (MFG) Security Policy Selection Table (SPST)/Security Policy Translation Table (SPTT) Toolset.

PRODUCT OVERVIEW

The Security Policy Information File (SPIF) is a key element of the access control mechanism used within the X.400 electronic messaging community. The SPIF defines the security policy and how the policy maps to the security label contained within the security header of the X.400 message.

Coupled with each SPIF, is a set of Security Policy Translation Tables (SPTTs) which define the security label translations between X.400 and legacy formats within that given security policy. For example, within the U.S. GENSER security policy, there will be one SPTT for X.400 to/from JANAP128 translations; another SPTT for X.400 to/from ACP127; another SPTT for X.400 to/from DOI-103, etc.

Selection of the appropriate SPTT within a given policy set is accomplished via the Security Policy Selection Table (SPST). This table specifies the applicable SPTT based upon received message criteria such as format and content keywords. For example, the SPST may specify that JANAP messages with the keyword “NATO” in Format Line 12a use the NATO-JANAP-SPTT, whereas all other JANAP messages would use the GENSER-JANAP-SPTT.

Although the SPIF is used by all messaging products that support the corresponding security policy, the SPST and SPTT are used only by the MFG, since the MFG is the only component that performs message format/label translations. For this reason, the generation tools for these various tables have been split into two sets: the SPIF Toolset, which is under Government control, and the SPST/SPTT Toolset, which is bundled with the MFG product. This document addresses the SPST/SPTT Toolset only.

The SPST/SPTT Toolset consists of the following tools, each of which is described in detail within this manual:

- **SPST Editor:** This tool allows the creation, modification, and display of the SPST. Using this tool, the user can specify the message criteria (format and content keywords) for each supported SPTT.
- **SPTT Editor:** This tool allows the creation, modification, and display of the SPTT. Using this tool, the user can specify the label translation rules for a given policy. The translation rules include mappings for classifications, categories, special handling designators, and privacy marks

as well as automatic default handling actions (i.e., automatically add a specified category to the label under certain conditions).

- **SPTT Simulator:** This tool provides security label translation simulation capabilities in support of SPTT content validation. Using this tool, the user can create a message security label and perform a sample translation using a specified SPTT. Output from this tool includes the translated label and a detailed trace log, listing the SPTT matching and decision making actions performed during the translation process.

DOCUMENT OVERVIEW

This document describes the operation of the SPST/SPTT Toolset in the following chapters:

Chapter 1, Overview: This chapter provides an overview description of the SPST/SPTT Toolset and this document.

Chapter 2, SPST/SPTT Toolset Installation: This chapter describes how to install the SPST/SPTT Toolset. It also describes SPST/SPTT Toolset Security Setup.

Chapter 3, SPST Editor Operations: This chapter describes how to start up the SPST Editor, how to use the editor to create, modify, and display SPSTs, and how to use the editor to digitally sign the SPST. It also provides an overview of the SPST Editor Main Window, as well as a discussion on SPST Editor Logging.

Chapter 4, SPTT Editor Operations: This chapter describes how to start up the SPTT Editor, how to use the editor to create, modify, display, verify, and print SPTTs, and how to use the editor to digitally sign the SPTT. It also provides an overview of the SPTT Editor Main Window, as well as a discussion on SPTT Editor Logging.

Chapter 5, SPTT Simulator Operations: This chapter describes how to start up the SPTT Simulator and how to use the simulator to validate newly created/modified SPTTs. It also provides an overview of the SPTT Simulator Main Window.

Chapter 2. SPST/SPTT TOOLSET INSTALLATION

This chapter describes how to install the SPST/SPTT Toolset. These procedures vary somewhat depending on the platform (UNIX or Windows-NT) on which the toolset is to be used.

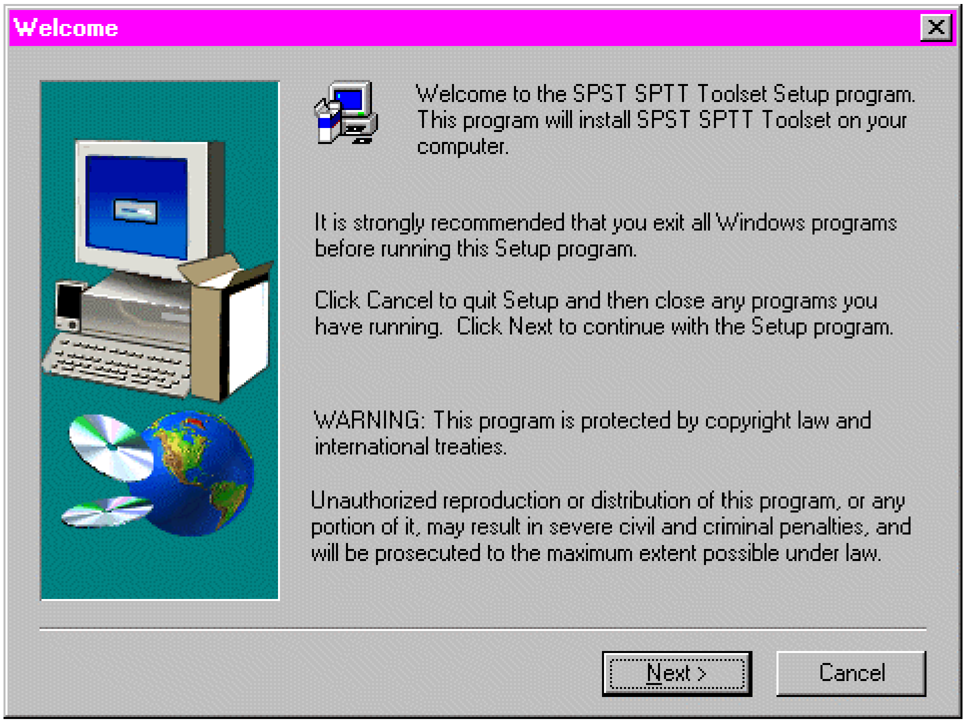
UNIX SPST/SPTT TOOLSET INSTALLATION

*****TBS*****

WINDOWS-NT SPST/SPTT TOOLSET INSTALLATION

To load the Windows-NT version of the SPST/SPTT Toolset, perform the following procedures:

1. Insert the CommPower SPST/SPTT Toolset CD in your CD-ROM drive.
2. Execute the *Setup.exe* file from the CD. The InstallShield® script is loaded and the Welcome dialog is displayed:



Welcome to the SPST SPTT Toolset Setup program. This program will install SPST SPTT Toolset on your computer.

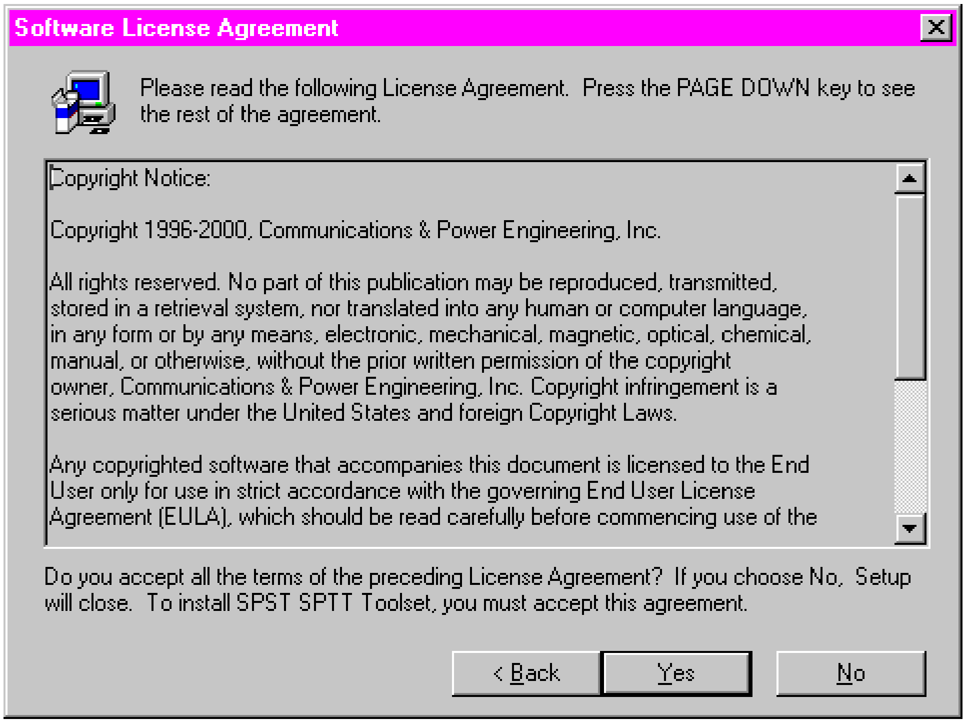
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

3. Select the **Next>** button. The Software License Agreement dialog is displayed:



Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.

Copyright Notice:

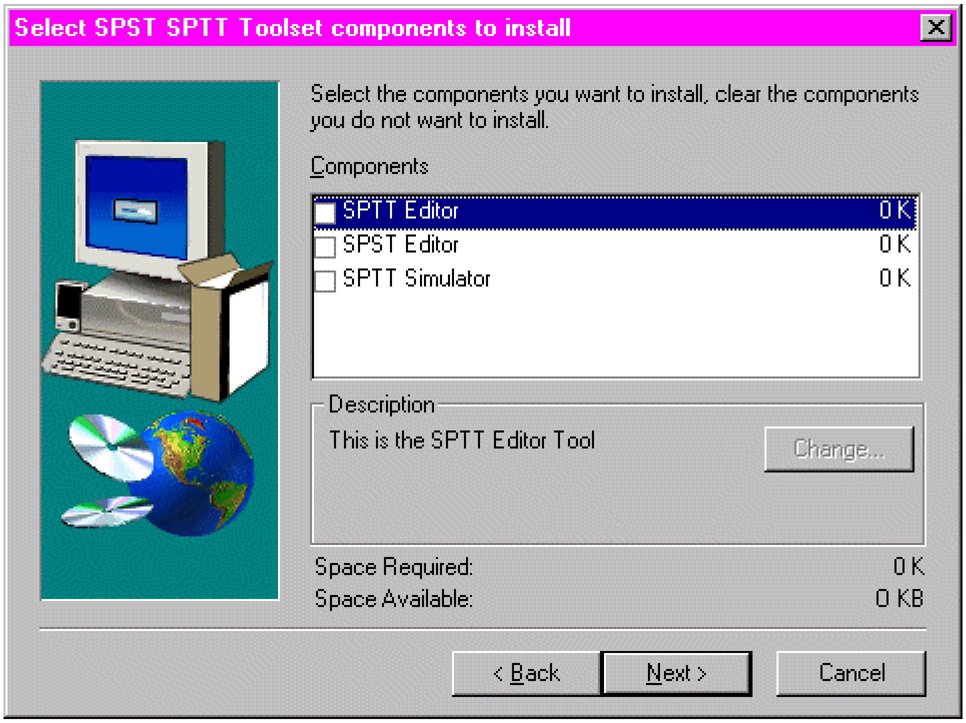
Copyright 1996-2000, Communications & Power Engineering, Inc.

All rights reserved. No part of this publication may be reproduced, transmitted, stored in a retrieval system, nor translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of the copyright owner, Communications & Power Engineering, Inc. Copyright infringement is a serious matter under the United States and foreign Copyright Laws.

Any copyrighted software that accompanies this document is licensed to the End User only for use in strict accordance with the governing End User License Agreement (EULA), which should be read carefully before commencing use of the

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install SPST SPTT Toolset, you must accept this agreement.

4. Select the **Yes** button to accept the license terms. The Select SPST/SPTT Toolset Components to Install dialog is displayed:



Select SPST SPTT Toolset components to install

Select the components you want to install, clear the components you do not want to install.

Components

□ SPTT Editor	0 K
□ SPST Editor	0 K
□ SPTT Simulator	0 K

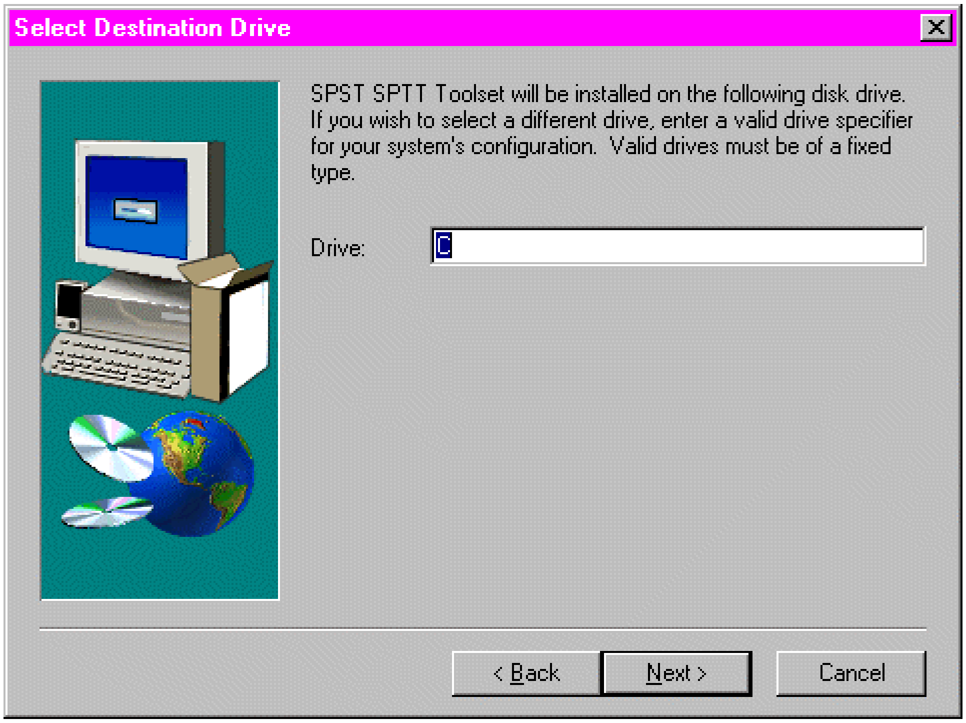
Description

This is the SPTT Editor Tool

Space Required: 0 K

Space Available: 0 KB

5. Select the desired SPST/SPTT Toolset components and then select the **Next>** button. The Select Destination Drive dialog is displayed:

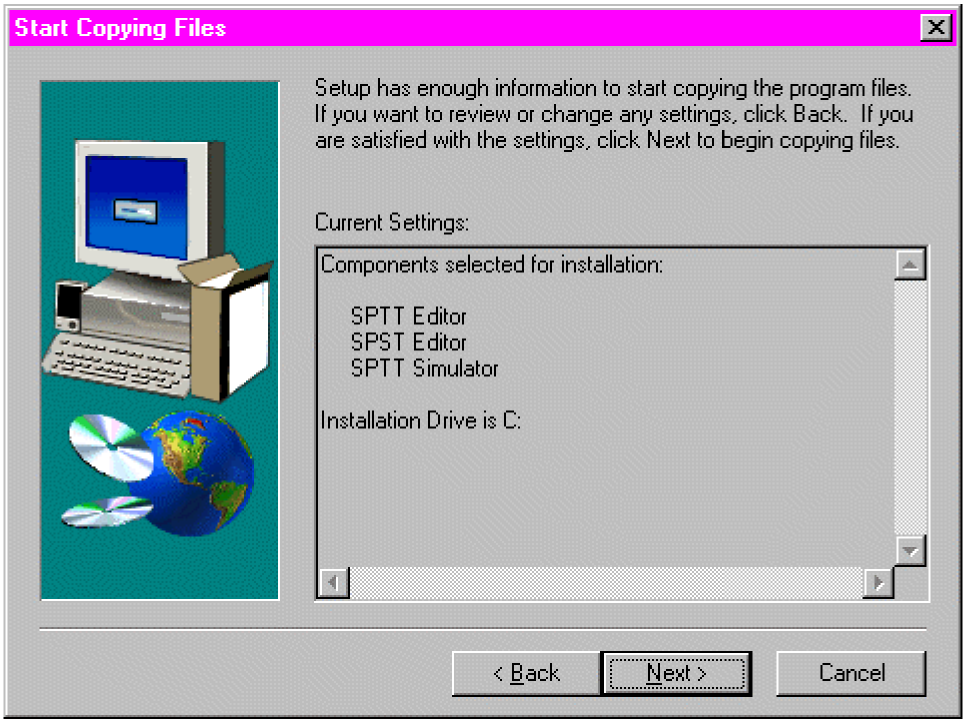


Select Destination Drive

SPST SPTT Toolset will be installed on the following disk drive. If you wish to select a different drive, enter a valid drive specifier for your system's configuration. Valid drives must be of a fixed type.

Drive: C

6. Select the **Next>** button to accept the default C:\ drive; otherwise, change the destination drive as desired and then select the **Next>** button. The Start Copying Files dialog is displayed:



Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

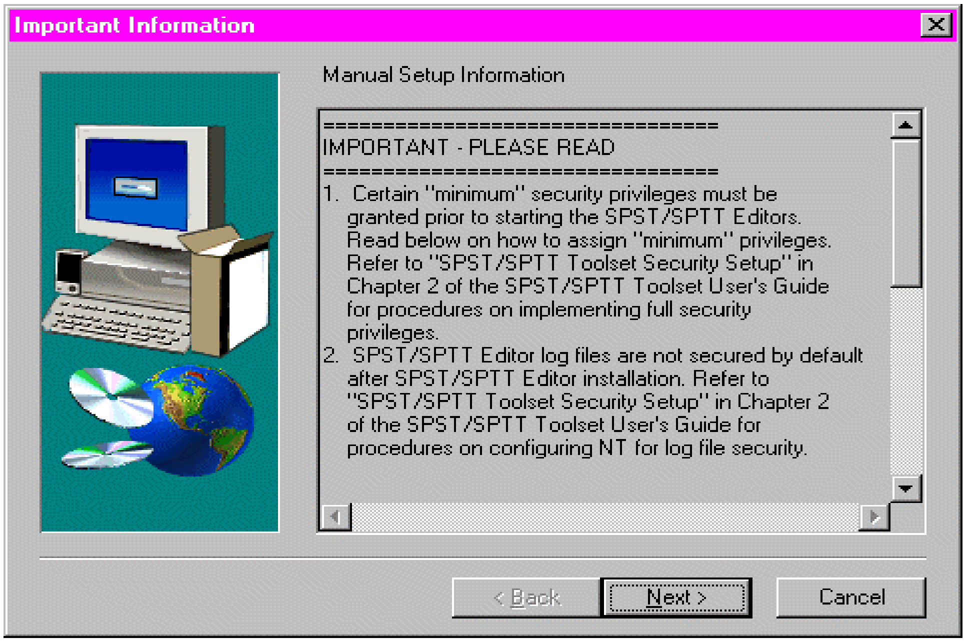
Current Settings:

```
Components selected for installation:

    SPTT Editor
    SPST Editor
    SPTT Simulator

Installation Drive is C:
```

7. Select the **Next>** button and the installation then begins. When finished, the Important Information dialog is displayed:

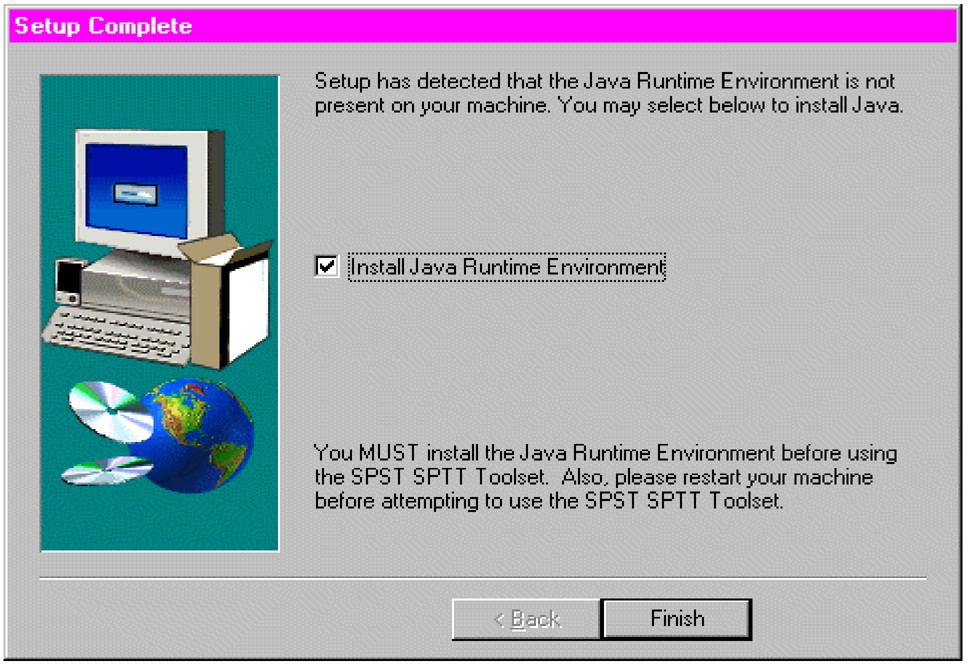


Manual Setup Information

```
================================
IMPORTANT - PLEASE READ
================================
1.  Certain "minimum" security privileges must be
    granted prior to starting the SPST/SPTT Editors.
    Read below on how to assign "minimum" privileges.
    Refer to "SPST/SPTT Toolset Security Setup" in
    Chapter 2 of the SPST/SPTT Toolset User's Guide
    for procedures on implementing full security
    privileges.
2.  SPST/SPTT Editor log files are not secured by default
    after SPST/SPTT Editor installation. Refer to
    "SPST/SPTT Toolset Security Setup" in Chapter 2
    of the SPST/SPTT Toolset User's Guide for
    procedures on configuring NT for log file security.
```

☒ **NOTE:** As emphasized in this dialog, certain minimum security privileges must be granted prior to starting either of the editors. Thus, when finished with the installation, please refer below to “SPST/SPTT Toolset Security Setup” for the procedures for implementing toolset security requirements.

8. After reading the information contained in the Important Information dialog, select the **Next>** button. The Setup Complete dialog is displayed:



Setup Complete

Setup has detected that the Java Runtime Environment is not present on your machine. You may select below to install Java.

☑ Install Java Runtime Environment

You MUST install the Java Runtime Environment before using the SPST SPTT Toolset. Also, please restart your machine before attempting to use the SPST SPTT Toolset.

9. If you haven't previously installed the Java Runtime Environment, which is required in order to run the SPST/SPTT Editors, the Setup Complete dialog will indicate this fact (as shown above) and you will be able to commence this additional software load at this point. To do this, select the **Finish** button and the InstallShield® script (for the Java Runtime Environment) will then be loaded, allowing you to complete the Java installation using dialogs and procedures similar to those used when installing the SPST/SPTT Toolset. When finished installing Java, you must then perform the security-related measures described below in "SPST/SPTT Toolset Security Setup". If you've already installed Java, then select the **Finish** button and perform these security measures directly. Once you have completed the installation and security setup, you must restart your computer before attempting to use the SPST/SPTT Editors.

SPST/SPTT Toolset Security Setup

Upon installing the SPST/SPTT Toolset, it is essential that you execute a number of security-related measures in order to (1) enable toolset startup and (2) ensure an environment in which only authorized users may use the toolset. This entails assigning intended toolset users to NT security groups and tailoring the access list of certain NT objects (i.e., folders and files), thereby differentiating between both the types of users and the operations they can perform.

For the SPST/SPTT Toolset, there are three recommended classes of users: Administrators, SPST/SPTT Editor operators, and Non-authorized personnel. Non-authorized personnel can neither run the SPST/SPTT Editors nor access the associated log files[1]. SPST/SPTT Editor operators can run the SPST/SPTT Editors but can only create (not access) log files (i.e., when running the editors). Administrators can run the SPST/SPTT Editors and can access the log files.

The following table summarizes the level of access by user class and recommends the appropriate (or "equivalent") NT security group:

User Class	Run SPST/SPTT Editors	Log File Access	Recommended NT Group
Administrators	Yes	Full Access	Administrators
SPST/SPTT Editor Operators	Yes	Write Only	Users
Non-authorized Personnel	No	No	Guests

ASSIGN USERS TO SECURITY GROUPS

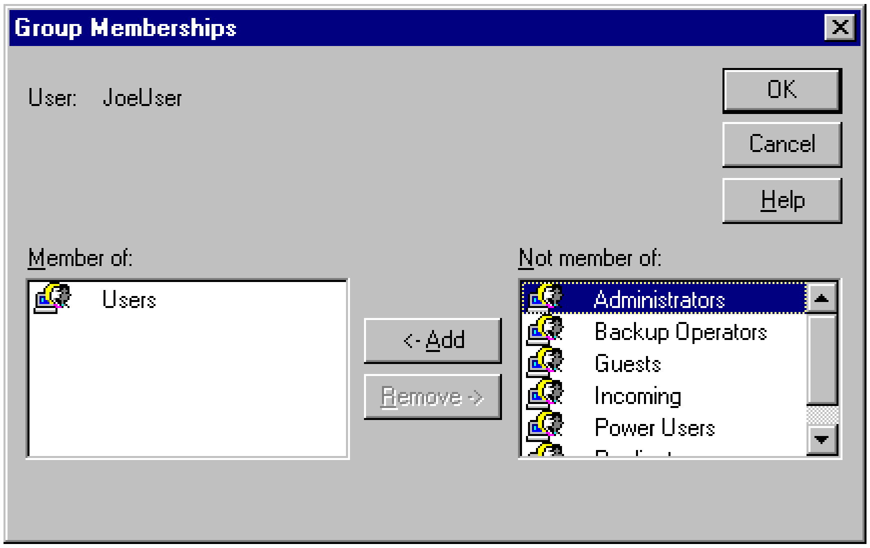
As stated (and illustrated) above, it is recommended that all intended SPST/SPTT Editor users be categorized into one of three user classes, i.e., Administrators, SPST/SPTT Editor operators, and Non-authorized personnel, and then assigned to equivalent NT security groups, i.e., Administrators, Users, and Guests.

Enter New User Accounts

1. Enter new user accounts, as required. If the new user is a SPST/SPTT Editor operator, then assign that account to the Users security group as shown directly below.

   ☒ **NOTE:** If the target computer has a configuration that does not include Administrators and Users security groups, then the target computer administrator will have to manually choose what security groups to use.

[1] The SPST/SPTT Editors feature a logging function that monitors and logs all user activities associated with creating, editing, and displaying Security Policy Selection Tables (SPSTs) and Security Policy Translation Tables (SPTTs). Thus, whenever a user invokes either of the editors to perform any of these operations, a log file is automatically created and saved to the appropriate directory, i.e., *C:\cpe\csci\SecurityTranslationToolset\logs\SPSTEditor* for the SPST Editor and *C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor* for the SPTT Editor. (See "SPST Editor Logging" and "SPTT Editor Logging" in Chapters 3 and 4, respectively.) To properly maintain or ensure the integrity of these log files, it is imperative that only the system administrator (or other users with system administrative privileges) be given access to them (i.e., for the purpose of displaying, editing, or deleting).



User: JoeUser

Member of:
Users

Not member of:
Administrators
Backup Operators
Guests
Incoming
Power Users

Assign Security Properties to Log File Directory and Files

<u>Change Log File Directory Access to Administrators/Users</u>

1. Log onto the system as Administrator or other user with administrative privileges (i.e., if you haven't already done so).

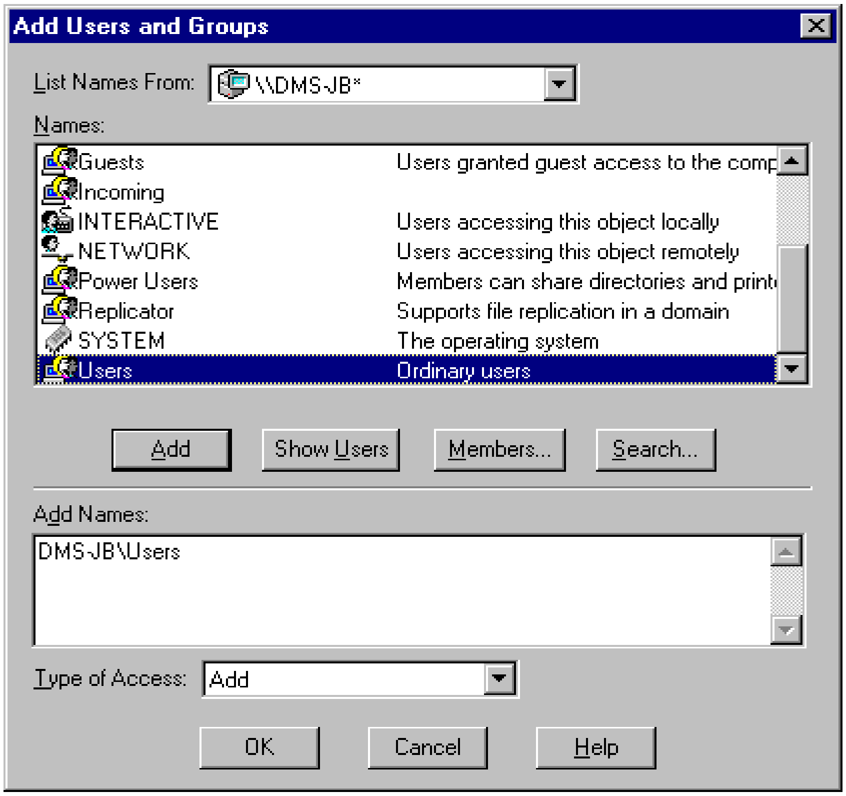
2. From Windows-NT Explorer, select the *C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor* folder and then select ***Properties*** from the File menu. The Log Properties dialog is displayed.

3. Select the **Security** tab and then the **Permissions** button. The Directory Permissions dialog is displayed.

4. Select all groups EXCEPT the Administrators group and then select the **Remove** button.

   ☒ **NOTE:** It is <u>crucial</u> that you leave the Administrators group in the Name list of the Directory Permissions dialog!

5. Select the **Add** button. The Add Users and Groups dialog is displayed. Choose the Users group from the Name List, select the **Add** button, and choose ***Add*** as the Type of Access. The dialog should look like the one shown below (except, of course, for the domain name "DMS-JB") before selecting the **OK** button.



Add Users and Groups

List Names From: \\DMS-JB*

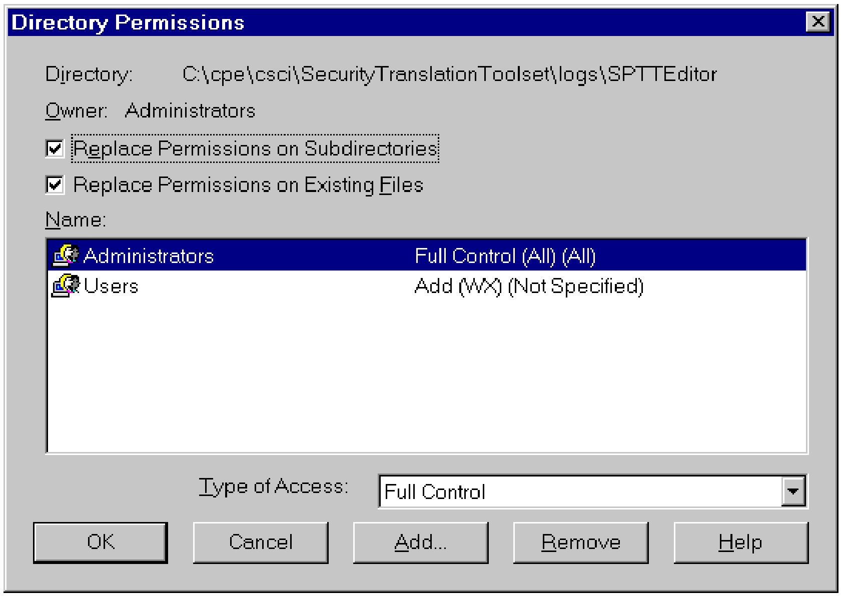
Names:

Guests	Users granted guest access to the comp
Incoming	
INTERACTIVE	Users accessing this object locally
NETWORK	Users accessing this object remotely
Power Users	Members can share directories and print
Replicator	Supports file replication in a domain
SYSTEM	The operating system
Users	Ordinary users

Add Names: DMS-JB\Users

Type of Access: Add

6. The Directory Permissions dialog should look like the following illustration prior to selecting the **OK** button.



Directory Permissions

Directory: C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor

Owner: Administrators

☑ Replace Permissions on Subdirectories

☑ Replace Permissions on Existing Files

Name:

Administrators	Full Control (All) (All)
Users	Add (WX) (Not Specified)

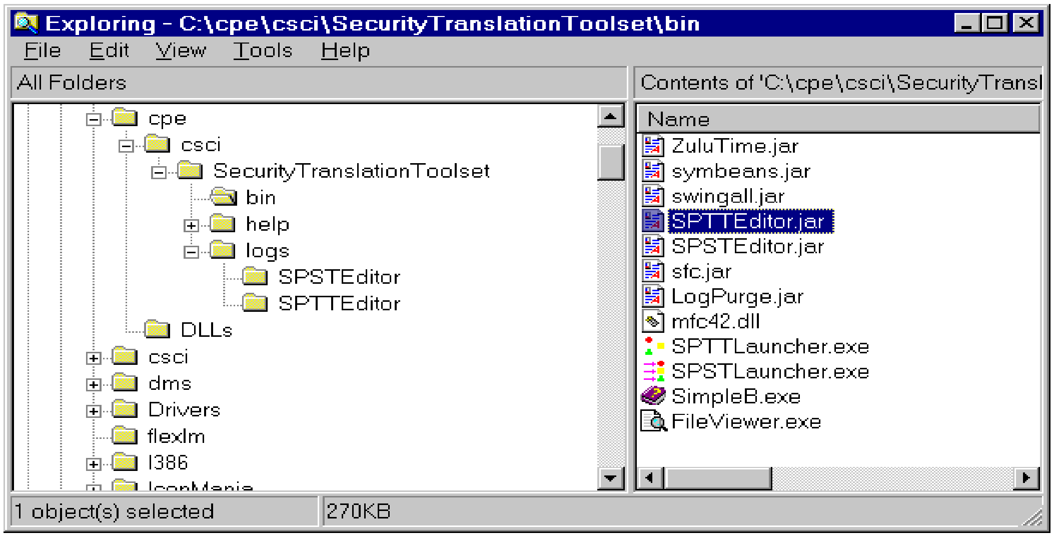
Type of Access: Full Control

7. Repeat Steps 2 through 6 above for the *C:\cpe\csci\SecurityTranslationToolset\logs\SPSTEditor* folder.

Change File Access to Administrators/Users

8. From Windows-NT Explorer, select the *C:\cpe\csci\SecurityTranslationToolset\bin* folder, select the *SPTTEditor.jar*

file (as shown in the following illustration), and then select ***Properties*** from the File menu.

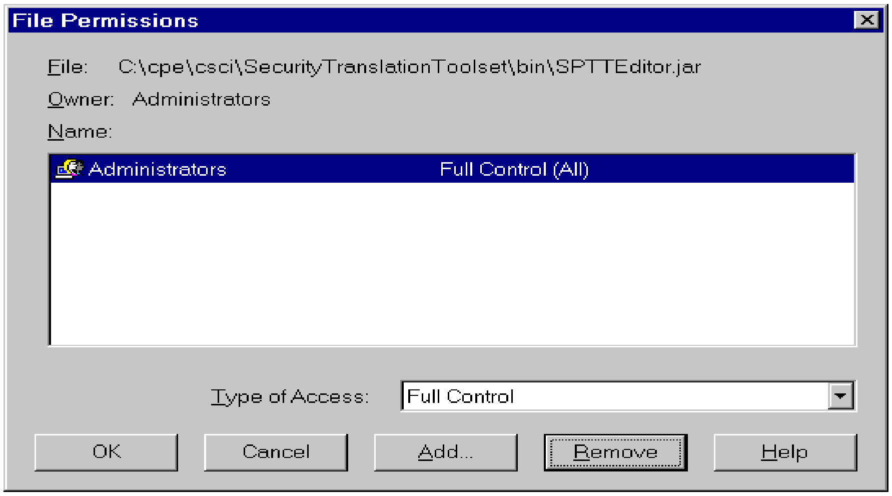


9. Select the **Security** tab and then the **Permissions** button (in the SPTTEditor.jar Properties dialog). The Directory Permissions dialog is displayed.

10. Select all groups EXCEPT the Administrators group and then select the **Remove** button.

☒ **NOTE:** Again, it is crucial that you leave the Administrators group in the Name list of the Directory Permissions dialog!

11. The File Permissions dialog should look like the following illustration:


File Permissions

File: C:\cpe\csci\SecurityTranslationToolset\bin\SPTTEditor.jar

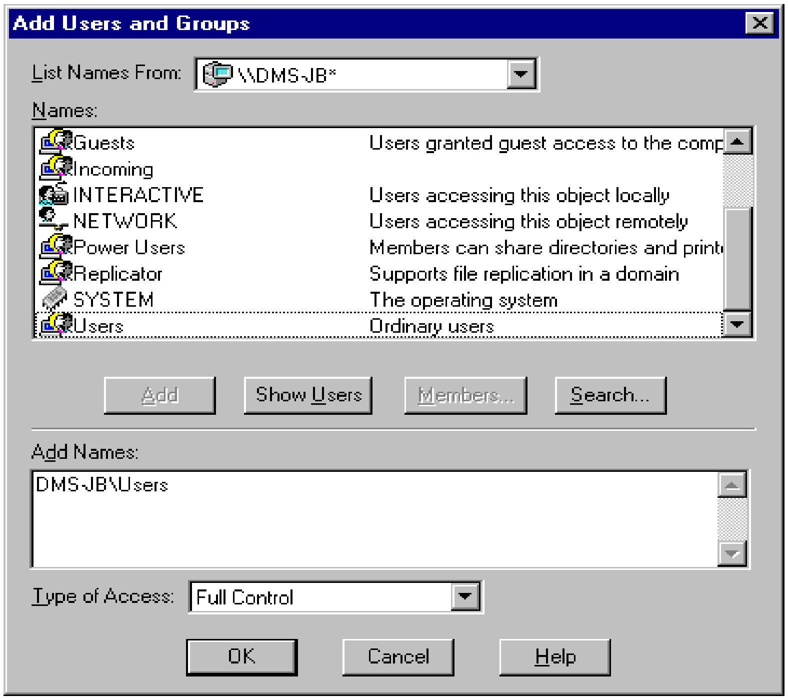
Owner: Administrators

Name:

Administrators Full Control (All)

Type of Access: Full Control

12. Select the **Add** button. The Add Users and Groups dialog is displayed. Choose the Users group from the Name List, select the **Add** button, and choose ***Full Control*** as the Type of Access. The dialog should look like the one shown below (except, of course, for the domain name "DMS-JB") before selecting the **OK** button.



Add Users and Groups

List Names From: \\DMS-JB*

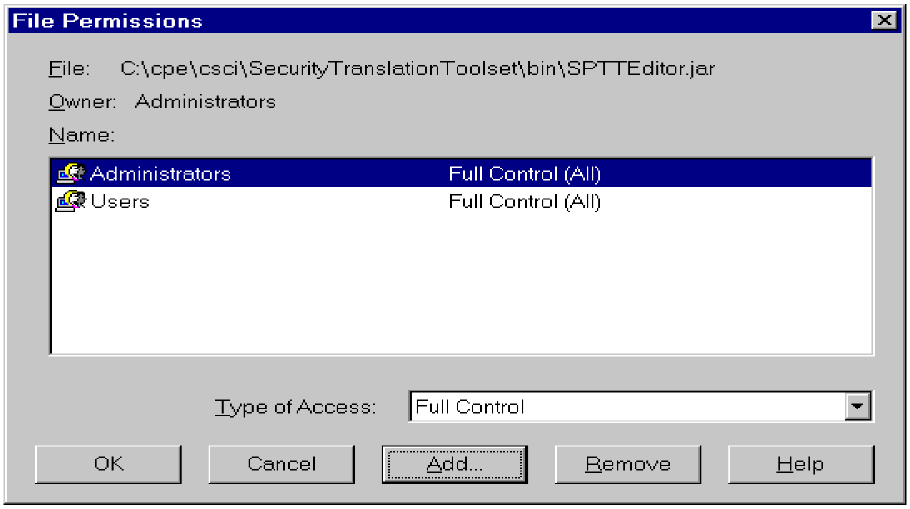
Names:

Guests	Users granted guest access to the comp
Incoming	
INTERACTIVE	Users accessing this object locally
NETWORK	Users accessing this object remotely
Power Users	Members can share directories and print
Replicator	Supports file replication in a domain
SYSTEM	The operating system
Users	Ordinary users

Add Names: DMS-JB\Users

Type of Access: Full Control

13. The Directory Permissions dialog should look like the following illustration prior to selecting the **OK** button.



File Permissions

File: C:\cpe\csci\SecurityTranslationToolset\bin\SPTTEditor.jar

Owner: Administrators

Name:

Administrators	Full Control (All)
Users	Full Control (All)

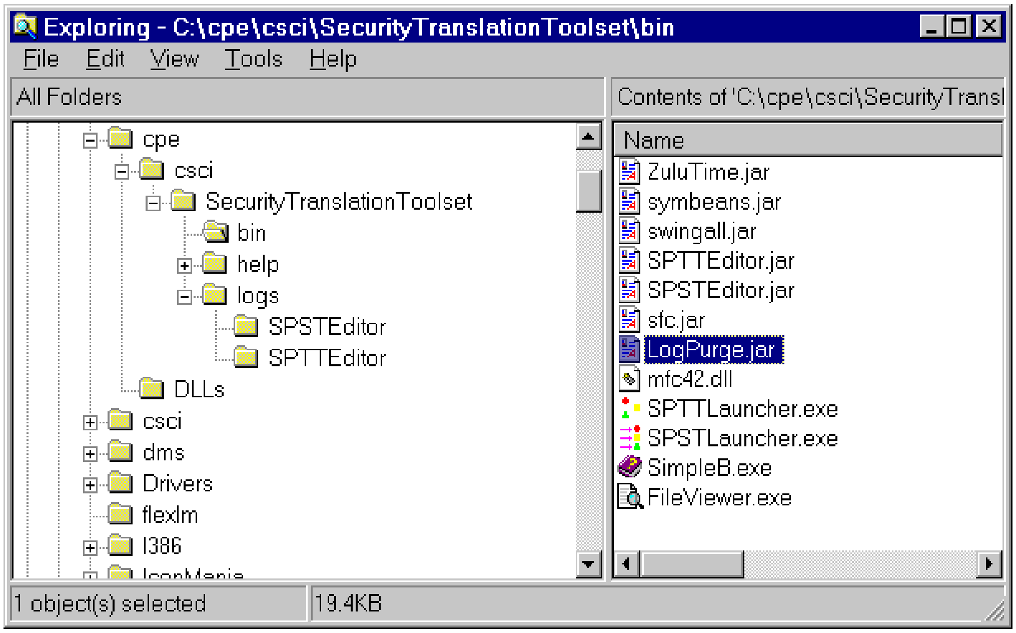
Type of Access: Full Control

14. Repeat Steps 8 through 13 above to change the security attributes of the following additional files:

- C:\cpe\csci\SecurityTranslationToolset\bin\SPSTEditor.jar
- C:\winnt\jrew.exe

Change File Access to Administrators Only

15. From Windows-NT Explorer, select the *C:\cpe\csci\SecurityTranslationToolset\bin* folder, select the *LogPurge.jar* file (as shown in the following illustration), and then select ***Properties*** from the File menu.



Exploring - C:\cpe\csci\SecurityTranslationToolset\bin

Contents of 'C:\cpe\csci\SecurityTransl

```
cpe
  csci
    SecurityTranslationToolset
      bin
      help
      logs
        SPSTEditor
        SPTTEditor
  DLLs
csci
dms
Drivers
flexlm
I386
IconMania
```

ZuluTime.jar
symbeans.jar
swingall.jar
SPTTEditor.jar
SPSTEditor.jar
sfc.jar
LogPurge.jar
mfc42.dll
SPTTLauncher.exe
SPSTLauncher.exe
SimpleB.exe
FileViewer.exe

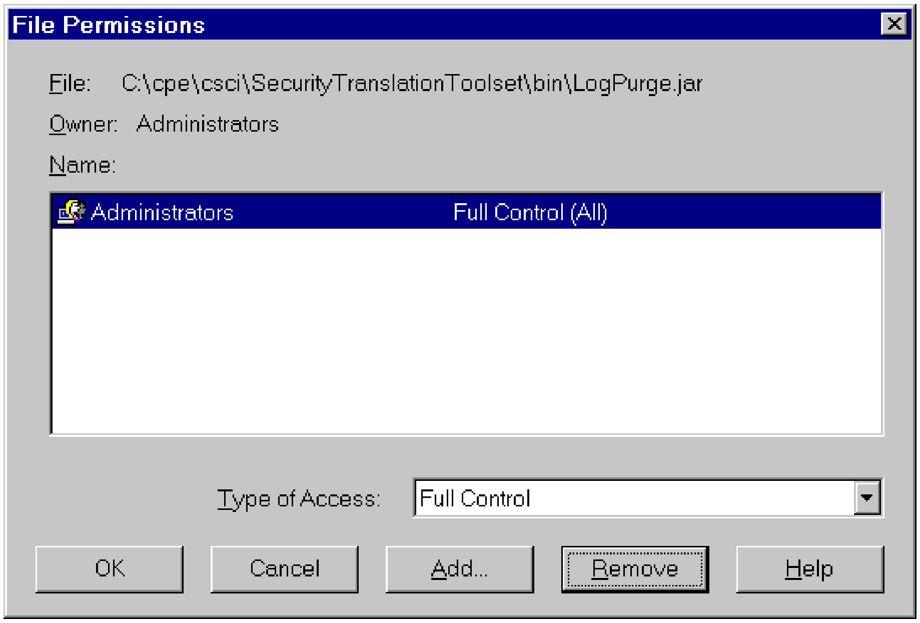
1 object(s) selected | 19.4KB

16. Select the **Security** tab and then the **Permissions** button (in the LogPurge.jar Properties dialog). The Directory Permissions dialog is displayed.

17. Select all groups EXCEPT the Administrators group and then select the **Remove** button.

    ☒ **NOTE:** Again, it is crucial that you leave the Administrators group in the Name list of the Directory Permissions dialog!

    The File Permissions dialog should look like the following illustration:



File: C:\cpe\csci\SecurityTranslationToolset\bin\LogPurge.jar

Owner: Administrators

Name:

Administrators Full Control (All)

Type of Access: Full Control

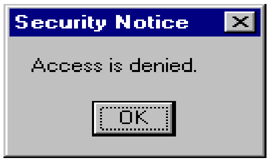
18. Select the **OK** button.

19. Repeat Steps 15 through 18 above to change the security attributes of the following additional files:
    - C:\cpe\csci\SecurityTranslationToolset\bin\Fileviewer.exe
    - C:\winnt\jre.exe
20. Exit the User Manager dialog and from the desktop select ***Start>>Shut Down>>Restart the Computer***.

Validate Security Requirements

After assigning privileges and users to NT security groups (as described above), you should perform the following additional steps in order to validate the correct implementation of these security-related measures.

1. Log onto the system as a SPTT Editor operator, i.e., a user without administrative privileges.
2. From Windows-NT Explorer, attempt to select the *C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor* folder. An Access Denied dialog should be displayed.
3. While logged on as a SPTT Editor operator, run the SPTT Editor.
4. Attempt to select either ***View Logs*** or ***Purge Logs*** from the File menu. A dialog box stating "Access Denied" should be displayed:



Security Notice

Access is denied.

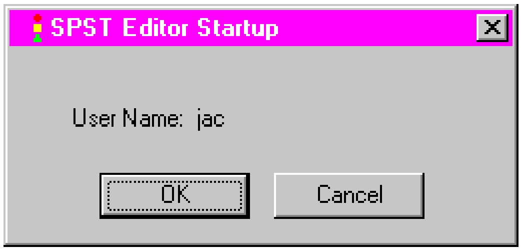
5. Log off and then back on as Administrator (or other user with administrative privileges). Repeat Step 2 above. You should see a log file created in the *C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor* folder from the just-completed SPTT Editor operator session.
6. Log off and then back on as Administrator and select ***View Logs*** or ***Purge Logs*** from the File menu. Both utilities should be available to you.
7. Repeat the above steps for the SPST Editor (substituting the directory given with *C:\cpe\csci\SecurityTranslationToolset\logs\SPSTEditor* where necessary).

Chapter 3.
SPST Editor Operations

This chapter describes how to start up the SPST Editor, how to use the editor to create, modify, or display Security Policy Selection Tables (SPSTs), and how to digitally sign the SPST via the editor. It also provides an overview of the SPST Editor Main Window (in the startup section), as well as a discussion on SPST Editor logging (specifically, how to view and purge the associated log files).

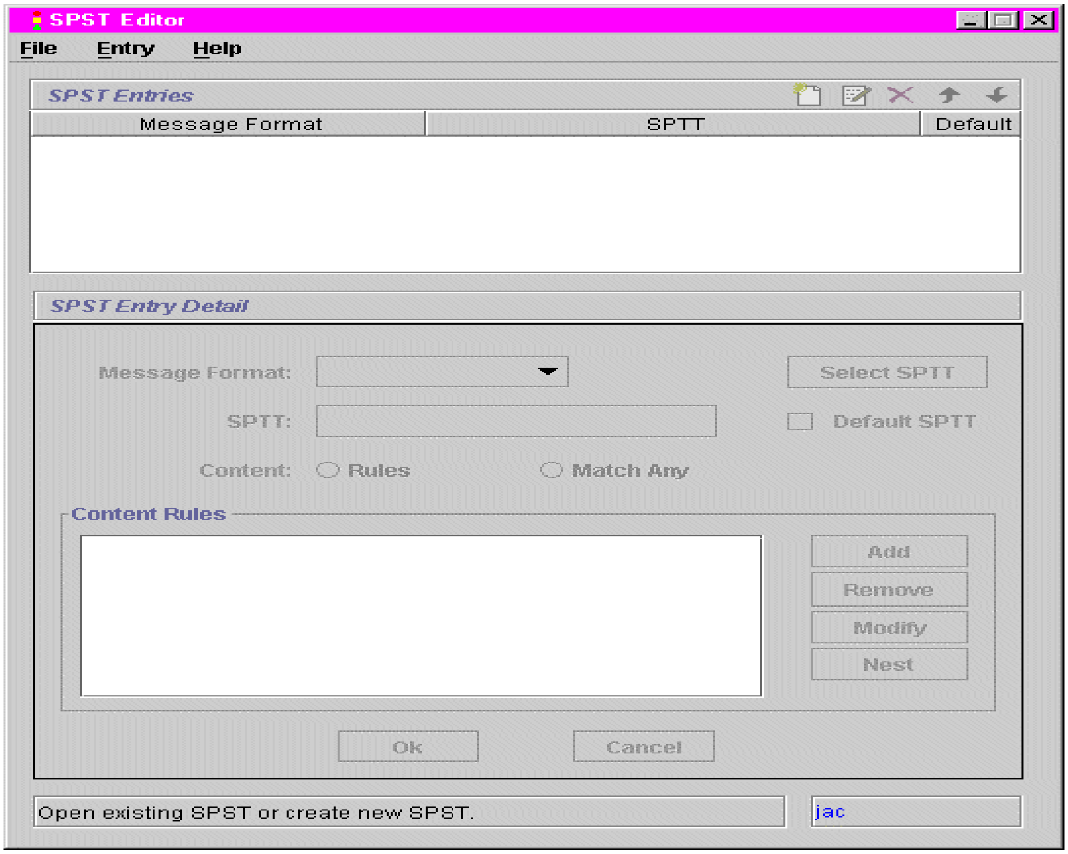
SPST EDITOR STARTUP

To start up the SPST Editor, select ***Start>>SPST-SPTT Toolset>>SPST Editor*** from the desktop. The SPST Editor Startup dialog is displayed:



User Name: jac

Select the **Ok** button. The SPST Editor Main Window is displayed:



Open existing SPST or create new SPST.

SPST Editor Main Window Overview

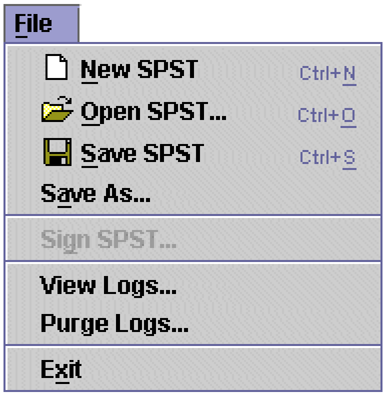
As shown above, the SPST Editor Main Window comprises the following features:

- Menu Bar (across the top)
- Main Display Windows/Work Areas (at the top and bottom)
- Function Buttons/Icons (above the SPST Entries Pane and to the right and bottom of the SPST Entry Detail Pane)
- Display Bars (across the bottom)

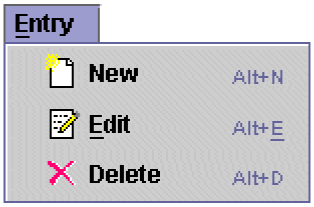
Menu Bar

The menu bar consists of three menus:

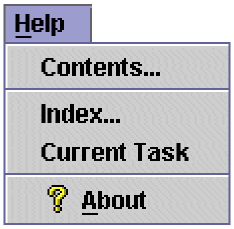
- **File Menu:** The File menu allows you to select standard file-related options including ***New SPST, Open SPST, Save SPST, Save As,*** and ***Exit***. It also allows you to select some application-specific ones including ***Sign SPST***, ***View Logs***, and ***Purge Logs***. These enable you to digitally sign an SPST, view SPST log files, and purge SPST log files.



- **Entry Menu:** The Entry menu allows you to select application-specific editing options including ***New***, ***Edit***, and ***Delete***. These enable you to create, edit, and delete security mappings.



- **Help Menu:** The Help menu allows you to select standard help-related options including ***Contents***, ***Index***, ***Current Task***, and ***About***. These enable you to display a table of contents (from which a topic can be selected); display an index (from which an index item can be selected); display context-sensitive help information; and display information about the current software release.



Main Display Windows/Work Areas

The main display windows/work areas consist of two primary panes:

- **SPST Entries:** This pane (located at the top) is used for displaying security policy "mappings" between message formats and Security Policy Translation Tables (SPTTs).
- **SPST Entry Detail:** This pane (located at the bottom) is used for specifying the mappings (or "rules') for the entries displayed in the SPST Entries pane.

Function Buttons/Icons

The function buttons/icons consist of the following:

- 🗋 The **New** button allows you to create a new security mapping. This function can also be executed by selecting ***New*** from the Entry menu.
- ✎The **Edit** button allows you to edit an entry in the SPST Entries pane. This function can also be executed by selecting ***Edit*** from the Entry menu.
- ✕ The **Delete** button allows you to delete a security mapping entry from the SPST Entries pane. This function can also be executed by selecting ***Delete*** from the Entry menu.
- ↑ The **Up Arrow** button allows you to move an entry up in the list of entries in the SPST Entries pane.
- ↓ The **Down Arrow** button allows you to move an entry down in the list of entries in the SPST Entries pane.
- Select SPTT The **Select SPTT** button allows you to select a SPTT upon which to base security policy mappings.
- Add The **Add** button allows you to add a rule to the Message Content Rules field (or sub-pane) in the SPST Entry Detail pane.
- Remove The **Remove** button allows you to remove a rule from the Message Content Rules field (or sub-pane) in the SPST Entry Detail pane.
- Modify The **Modify** button allows you to modify a rule in the Message Content Rules field (or sub-pane) in the SPST Entry Detail pane.
- Nest The **Nest** button allows you to nest (or subordinate) a rule under another rule in the Message Content Rules field (or sub-pane) in the SPST Entry Detail pane.
- Ok The **Ok** button allows you to complete (or "finalize") your ruleset for an SPST entry.
- Cancel The **Cancel** button allows you to remove all ruleset entries in the SPST Entry Detail pane.

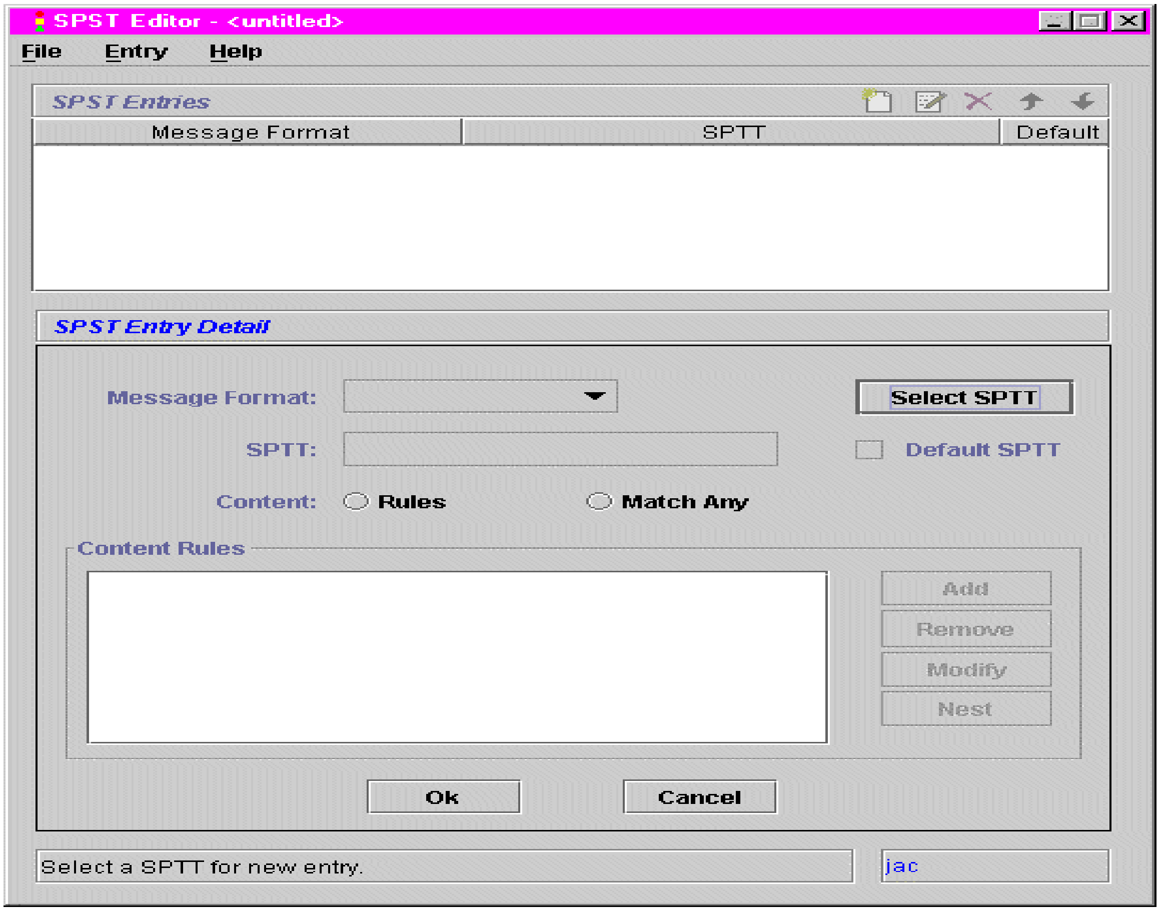
Display Bars

The display bars consist of two side-by-side horizontal bars (at the bottom), the first of which displays feedback relating to operator selections and the second of which displays the user name of the person currently logged onto the SPST Editor.

CREATE/OPEN SPST

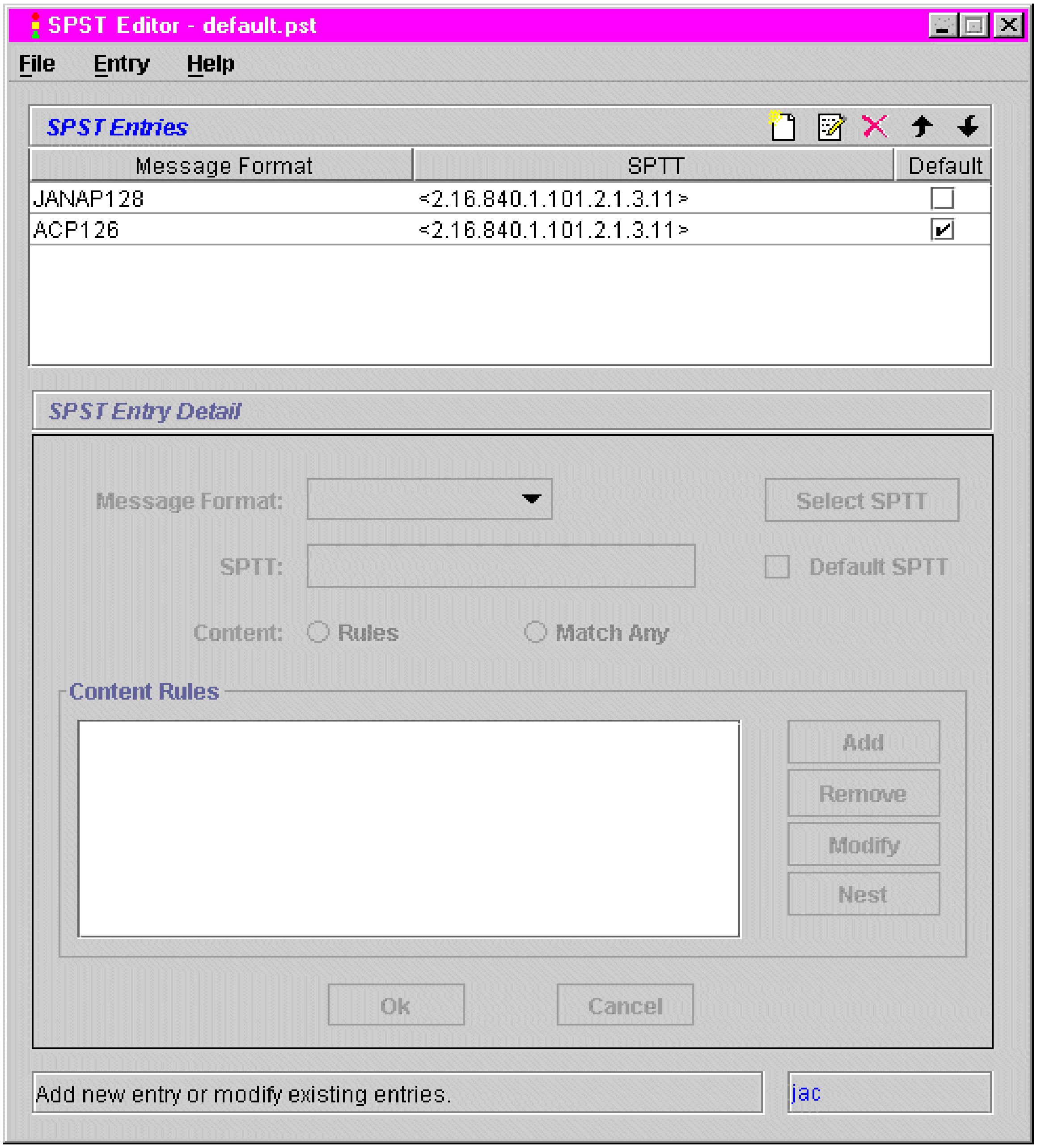
Upon invoking the SPST Editor via the Windows NT Start menu (as described above), you must choose to either create a new SPST or open an existing one. Do this as follows:

- Select ***New SPST*** or ***Open SPST*** from the File menu, depending on whether you wish to create a new SPST or edit a previously created one. If your intent is to create a new SPST, then after selecting ***New SPST*** from the File menu you must select either ***New*** from the Entry menu or the **New** (or 1st) button in the upper right-hand corner of the SPST Entries pane. The SPST Entry Detail pane and the associated buttons (i.e., **Select SPTT**, **Add**, **Remove**, **Modify**, **Nest**, **Ok**, and **Cancel**) are then enabled:



Select a SPTT for new entry.

If, on the other hand, your intent is to modify/display an existing SPST, you must supply the location and name of the SPST file when prompted. After doing so, the SPST data is displayed in the SPST Entries pane:



Message Format	SPTT	Default
JANAP128	<2.16.840.1.101.2.1.3.11>	□
ACP126	<2.16.840.1.101.2.1.3.11>	☑

Add new entry or modify existing entries.

jac

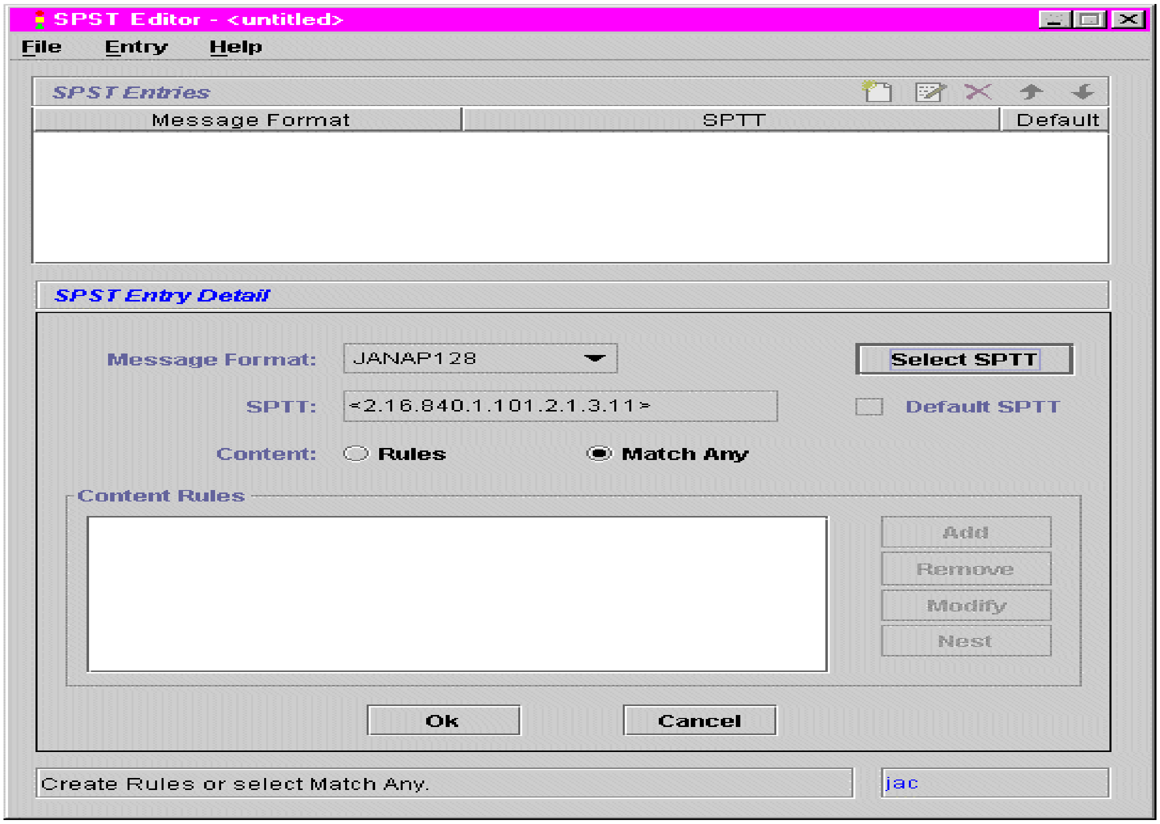
You are now free to add, modify, remove, and reposition SPST entries by performing the procedures described below in the respective paragraphs.

Add, Modify, Remove, & Reposition SPST Entry

Add SPST Entry

To add an SPST entry to a new or an existing SPST, you must first choose whether you want to map the entry to a "regular" SPTT or a "default" SPTT and then perform "1" or "2" below depending upon your choice. *Basically speaking, a default SPTT is one that maps Security Policy Information File (SPIF)* *classification values to MFI Local Classification values. Since it (unlike a regular SPTT) does not contain any other classification/category translation data, it can be thought of as an "abbreviated" SPTT. An SPST entry based on a default SPTT can also be thought of as "abbreviated" since it (unlike a regular SPST entry) does not allow the operator to define ruleset parameters (although it does allow the operator to specify Security Policy Object Identifiers, OIDs, as described below).*

1. If your intent is to map an SPST entry to a regular SPTT, click the **Select SPTT** button and supply the location of the regular SPTT file. Upon doing so, the Message Format and Object Identifier (OID) for the SPTT are displayed in the SPST Entry Detail pane:



Message Format: JANAP128

SPTT: <2.16.840.1.101.2.1.3.11>

□ Default SPTT

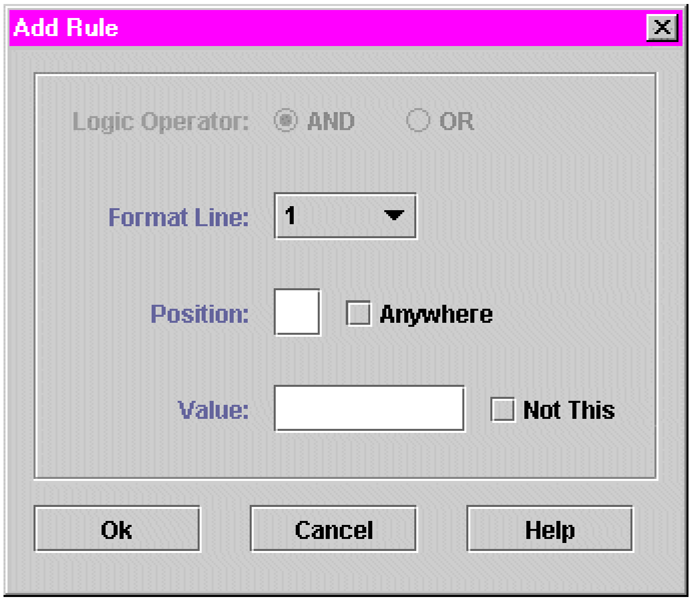
Content: ○ Rules ● Match Any

Content Rules

Create Rules or select Match Any.

jac

- Specify the desired Content type for the SPST entry. Accept the default ***Match Any*** if you want to permit any or all ruleset parameters for the message format and then click the **Ok** button (at the bottom of the SPST Entry Detail pane). The entry is added to the SPST Entries pane (see the third figure below). Otherwise, select ***Rules*** and then select the **Add** button if you want to define ruleset parameters for the entry. The Add Rule dialog is displayed:



Logic Operator: ● AND ○ OR

Format Line: 1

Position: □ Anywhere

Value: □ Not This

Define or construct ruleset parameters for the SPST entry by specifying/configuring the following fields:

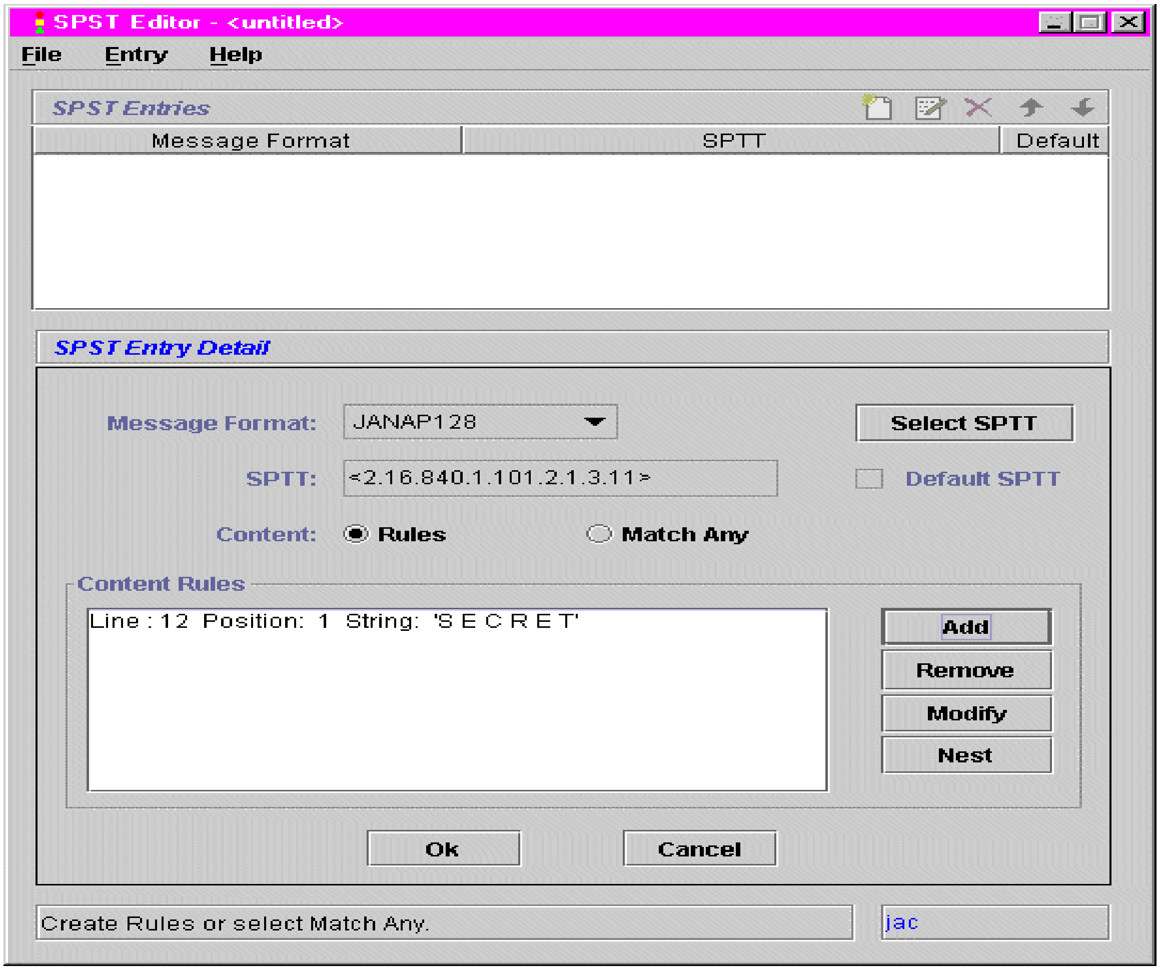
Logic Operator: This field allows you to specify the appropriate Boolean expression, i.e., AND or OR, for your ruleset. It is disabled when defining the first rule and then enabled when defining subsequent rules.

Format Line: This field specifies the format line to check when the message is parsed.

Position: This field specifies the character position to check when the message is parsed. If you want to check for any position, then select the toggle associated with the Anywhere field.

Value: This field specifies the text string (e.g., S E C R E T) to check when the message is parsed. If you want to check for all possible strings except one, then specify the string in the Value field and select the toggle associated with the Not This field.

When finished defining the rule, select the **Ok** button in the Add Rule dialog. The dialog is closed and the rule is displayed in the SPST Entry Detail pane:



Message Format: JANAP128

SPTT: <2.16.840.1.101.2.1.3.11>

□ Default SPTT

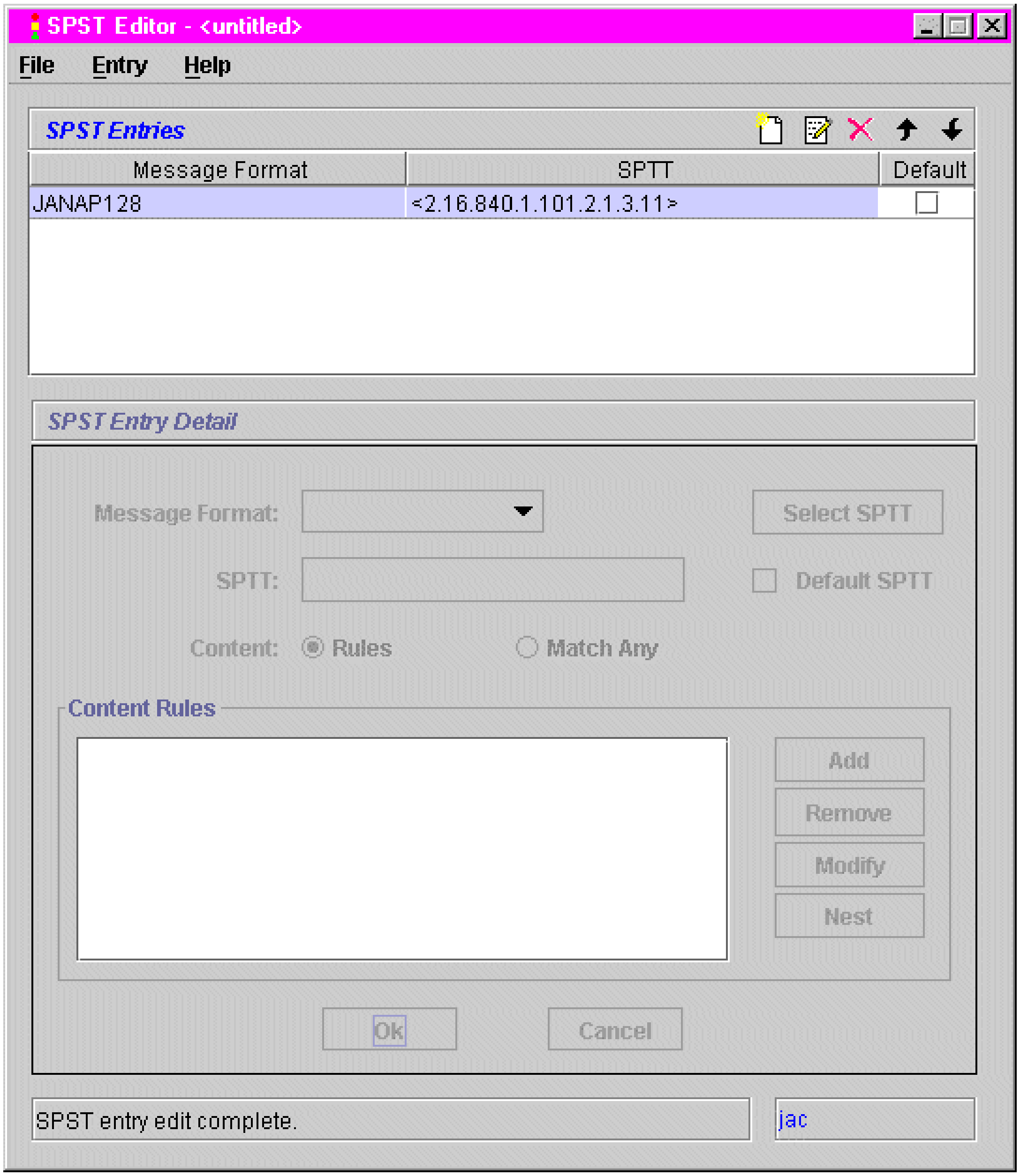
Content: ● Rules ○ Match Any

Content Rules

Line : 12 Position: 1 String: 'S E C R E T'

Create Rules or select Match Any.

Select the **Add** button again if you want to add additional rules to your SPST entry ruleset and when finished, select the **Ok** button (at the bottom of the SPST Entry Detail pane). Otherwise, select the **Ok** button directly. The entry is added to the SPST and the associated Message Format and SPTT OID values are displayed in the SPST Entries pane:



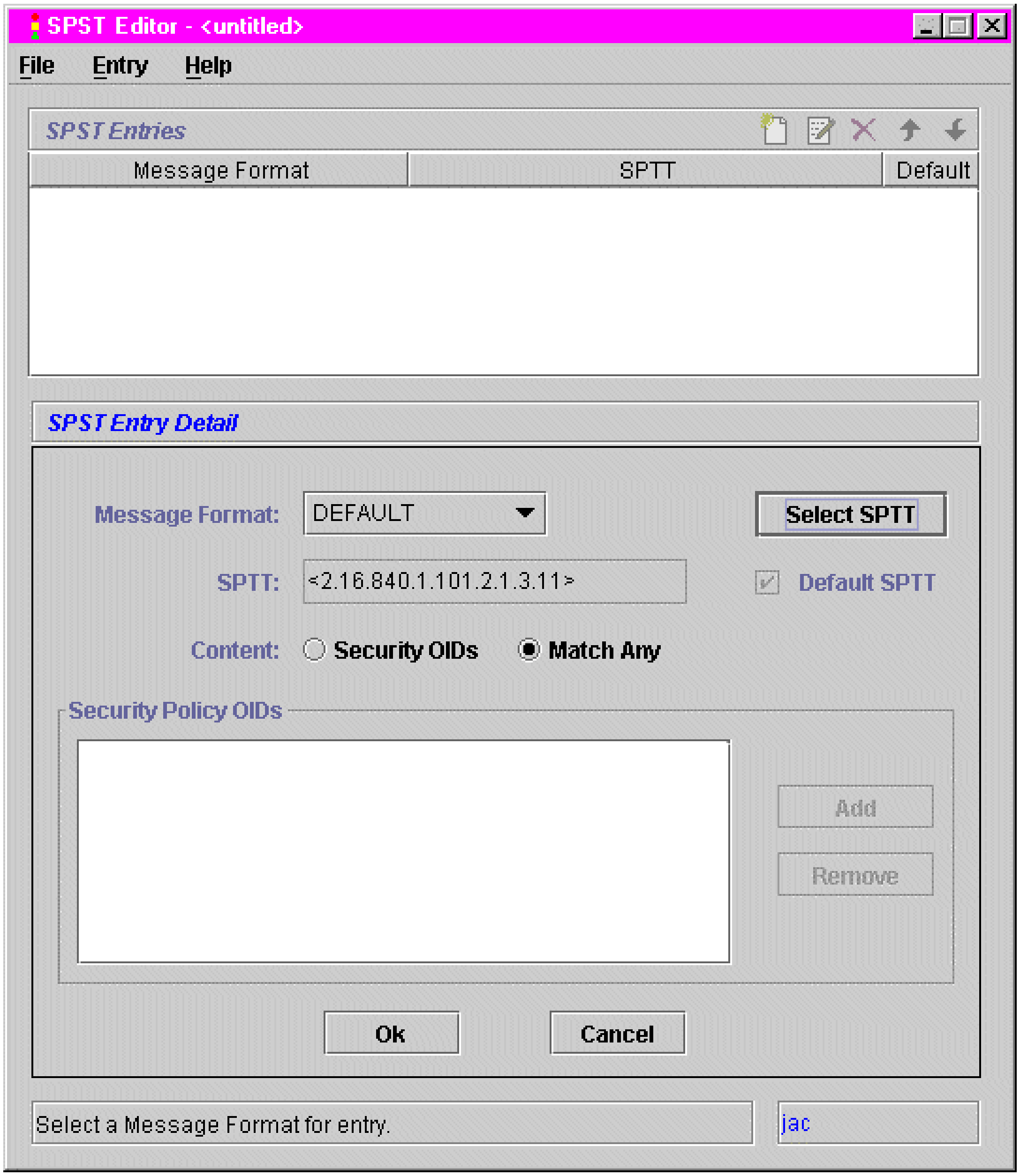
Message Format	SPTT	Default
JANAP128	<2.16.840.1.101.2.1.3.11>	□

SPST entry edit complete.

jac

- Repeat the appropriate steps above if you want to add additional entries to the SPST and then save the SPST by selecting ***Save SPST*** from the File menu. Otherwise, select ***Save SPST*** directly. If this is the first time you have saved the file, you will be prompted for a file location and name.

2. If your intent is to map an SPST entry to a default SPTT, click the **Select SPTT** button and supply the location of the default SPTT file. Upon doing so, the Message Format and Object Identifier for the SPTT are displayed in the SPST Entry Detail pane. You will also observe that the checkbox for the Default SPTT field is checked, the ***Match Any*** Content type is selected, and all remaining fields and buttons (except for **Ok** and **Cancel**) are disabled:



Message Format	SPTT	Default

Message Format: DEFAULT

SPTT: <2.16.840.1.101.2.1.3.11>

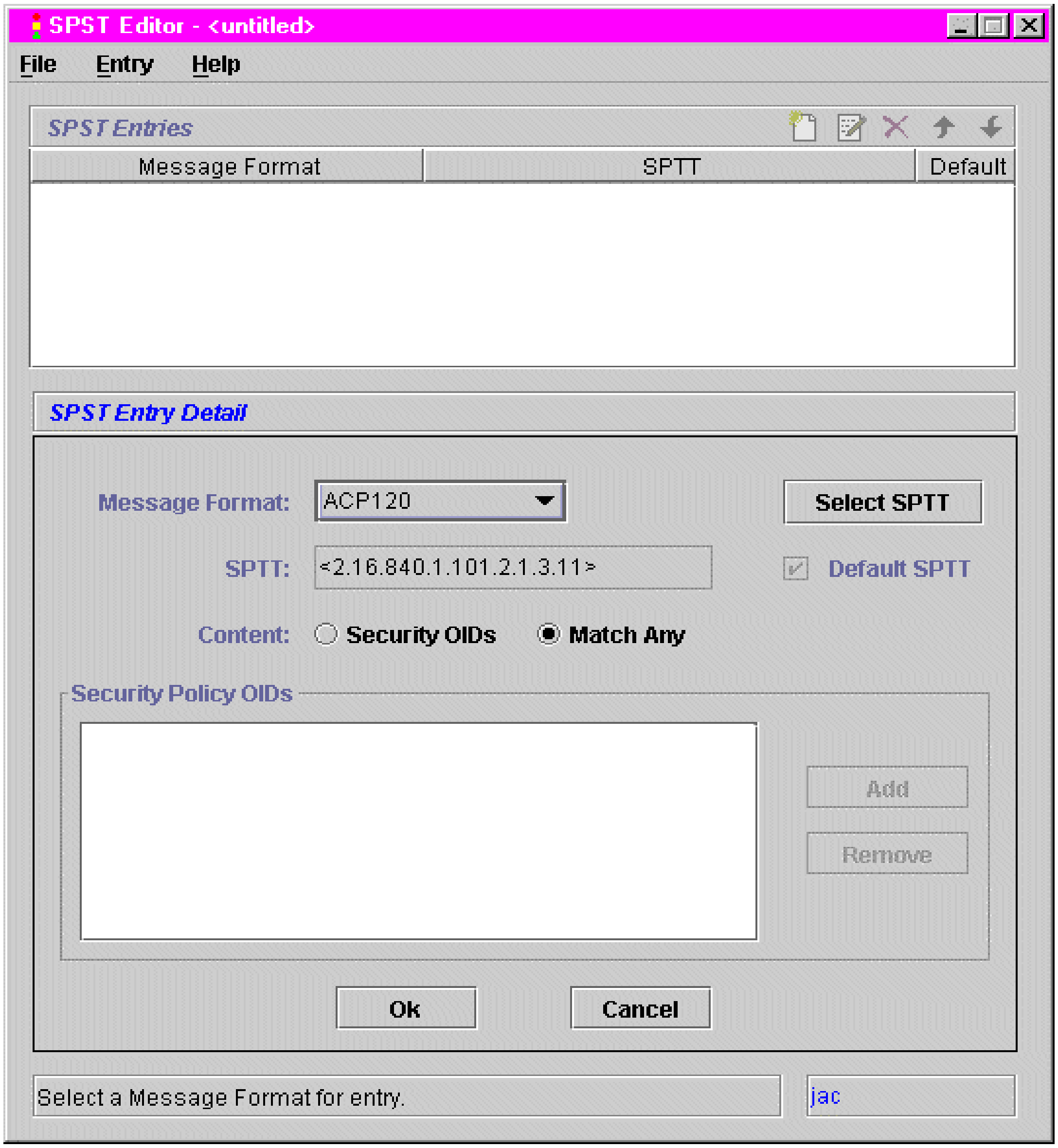
☑ Default SPTT

Content: ○ Security OIDs ● Match Any

Select a Message Format for entry.

jac

- Select the desired message format from the associated pop-up list. The selected format is then displayed in the Message Format field:



Message Format: ACP120

SPTT: <2.16.840.1.101.2.1.3.11>

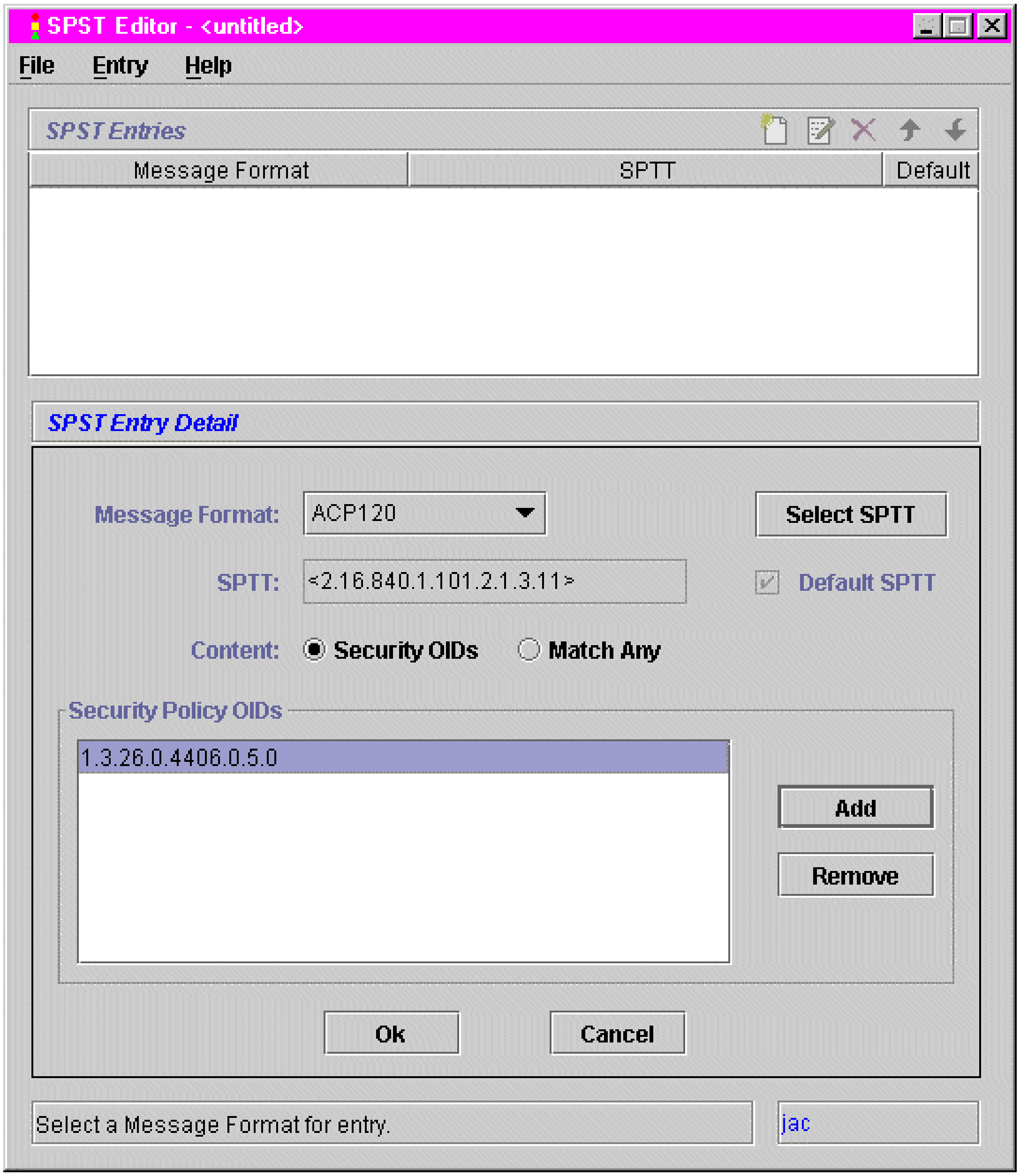
☑ Default SPTT

Content: ○ Security OIDs ● Match Any

Select a Message Format for entry.

jac

- If your intent is to match any or all ruleset parameters (or "criteria") for the selected message format, then accept the default ***Match Any*** and select the **Ok** button (at the bottom of the SPST Entry Detail pane). The entry is added to the SPST, the associated Message Format and SPTT OID values are displayed in the SPST Entries pane, and the Default field checkbox (also in the SPST Entries pane) is checked (see the second figure below). If, on the other hand, your intent is to specify Security Policy OIDs for the selected message format, then select ***Security OIDs*** in the Content field. (The **Add** and **Remove** buttons are then enabled.) Select the **Add** button, enter the desired OID in the Security Policy OIDs field (or sub-pane), and then hit the return key to accept the entry. The OID is then highlighted in the Security Policy OIDs field:



Message Format: ACP120

SPTT: <2.16.840.1.101.2.1.3.11>

☑ Default SPTT

Content: ● Security OIDs ○ Match Any

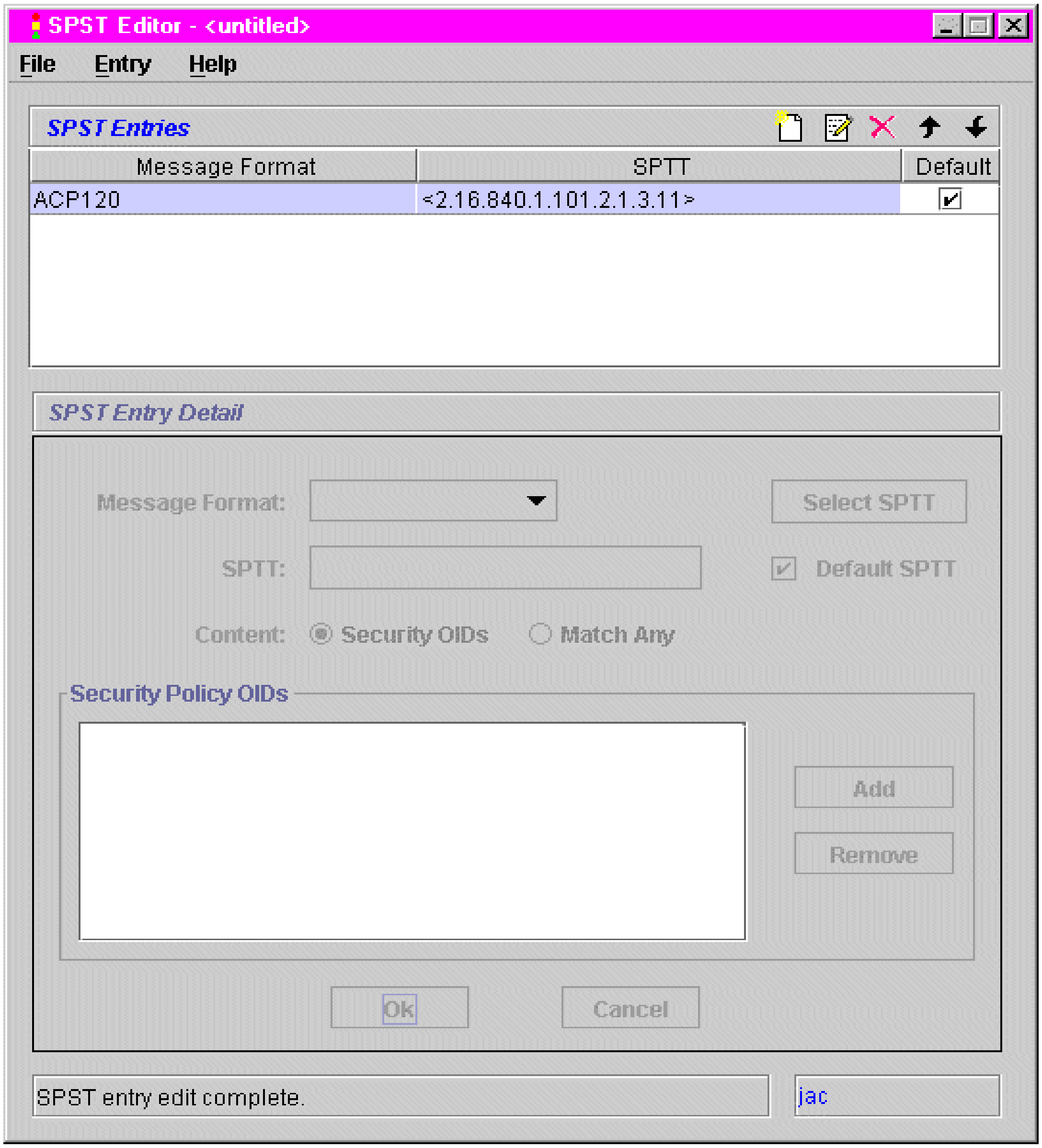
Security Policy OIDs

1.3.26.0.4406.0.5.0

Select a Message Format for entry.

jac

Add any additional Security Policy OIDs and/or select the **Ok** button (at the bottom of the SPST Entry Detail pane). The entry is added to the SPST and the associated Message Format and SPTT OID values are displayed in the SPST Entries pane. The Default field checkbox (also in the SPST Entries pane) is checked:



Message Format	SPTT	Default
ACP120	<2.16.840.1.101.2.1.3.11>	☑

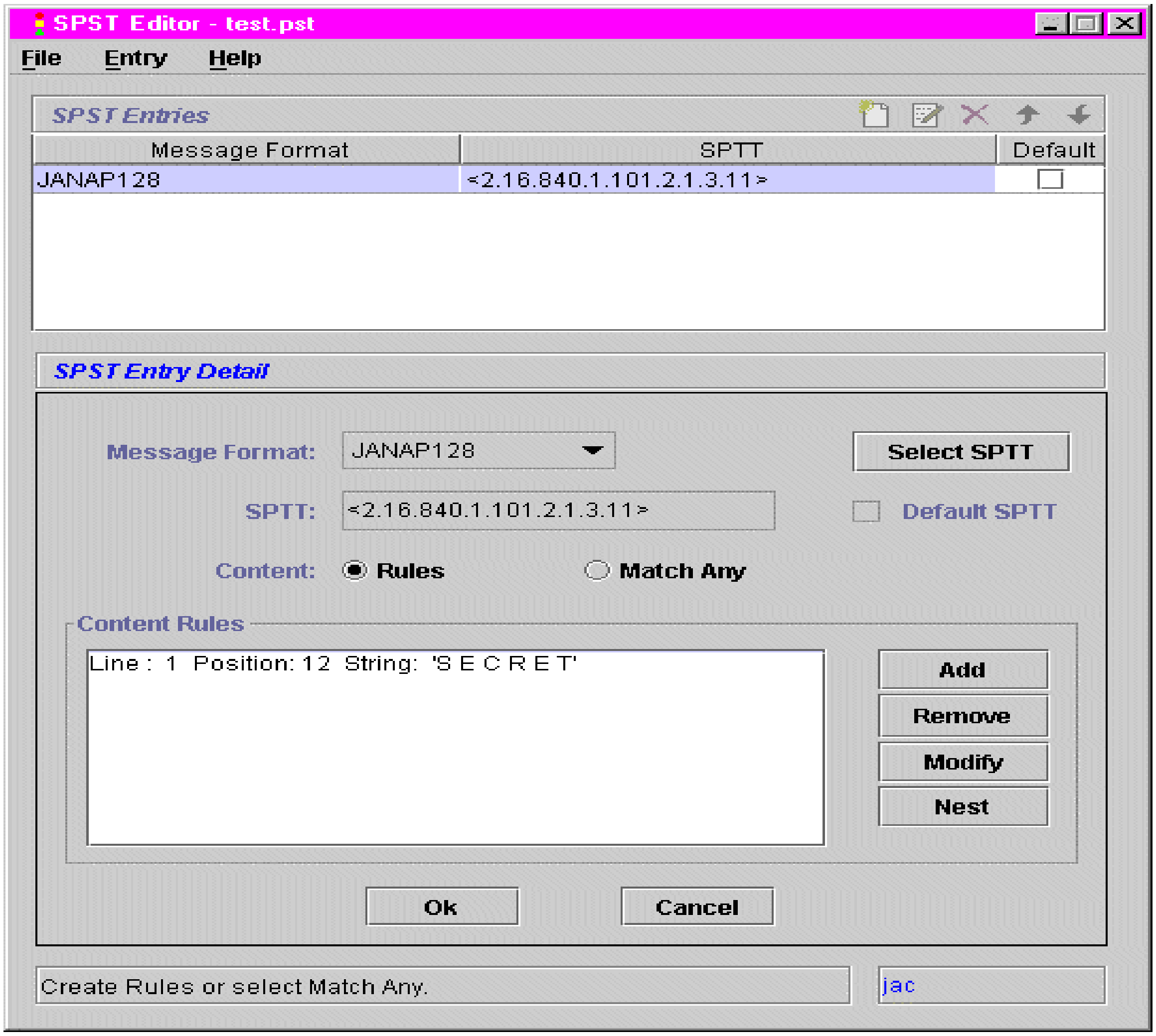
SPST entry edit complete.

jac

- Repeat the appropriate steps above if you want to add additional entries to the SPST and then save the SPST by selecting ***Save SPST*** from the File menu. Otherwise, select ***Save SPST*** directly. If this is the first time you have saved the file, you will be prompted for a file location and name.

Modify SPST Entry

To modify an SPST entry, you must highlight it in the SPST Entries pane and then select either ***Edit*** from the Entry menu or the **Edit** (or 2nd) button in the upper right-hand corner of the SPST Entries pane. Upon doing so, the associated Message Format, SPTT Object Identifier (OID), and possibly Content Rule or Security Policy OID values are displayed in the SPST Entry Detail pane depending upon the type of SPST entry selected. The buttons that govern operations in the pane may also vary depending upon the type of SPST entry selected:



Message Format	SPTT	Default
JANAP128	<2.16.840.1.101.2.1.3.11>	□

Message Format: JANAP128

SPTT: <2.16.840.1.101.2.1.3.11>

□ Default SPTT

Content: ● Rules ○ Match Any

Line : 1 Position: 12 String: 'S E C R E T'

Create Rules or select Match Any.

jac

- For regular SPST entries with associated ruleset values (as shown directly above), use the **Add**, **Remove**, **Modify**, and **Nest** buttons to modify these values. The **Add** button displays the Add Rule dialog, which allows you to add a rule or parameter to the selected SPST entry ruleset. (If necessary, see item "1" under "Add SPST Entry" above for a description of the fields contained in and the procedures for using the Add Rule dialog.) The **Remove** button allows you to remove a highlighted rule from the displayed ruleset. The **Modify** button displays the Modify Rule dialog, which is identical except for title to the Add Rule dialog and allows you to modify a rule (again, see item "1" under "Add SPST Entry" above, if necessary). The **Nest** button displays the Nest Rule dialog, which is identical except for title to the Add Rule and Modify Rule dialogs and allows you to nest (or subordinate) a rule under another rule in the ruleset.

- For default SPST entries with associated Security Policy OID values, highlight the OID and modify it if editing it; otherwise, use the **Add** and

Remove buttons to add and remove OID values. (If necessary, see item "2" under "Add SPST Entry" above for a description of the procedures for using the SPST Editor to create default SPST entries.)

- When finished modifying the selected SPST entry, click the **Ok** button at the bottom of the SPST Entry Detail pane. Then, select ***Save SPST*** from the File menu to save the modified SPST.

Remove SPST Entry

To remove an SPST entry, you must highlight it in the SPST Entries pane and then select either ***Delete*** from the Entry menu or the **Delete** (or 3rd) button in the upper right-hand corner of the SPST Entries pane. Upon doing so, the SPST entry is removed from the SPST Entries pane.

Reposition SPST Entry

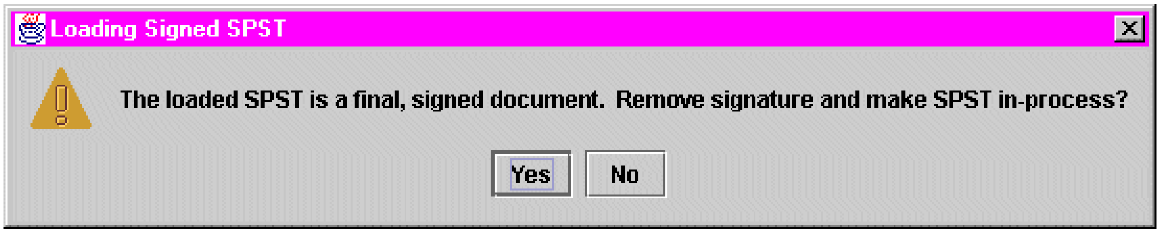
To reposition an SPST entry, you must highlight it in the SPST Entries pane and then select either the **Up Arrow** or **Down Arrow** button, depending on whether you want to move the entry up or down in the list of entries.

DIGITALLY SIGNING THE SPST

After you've finished creating or editing your SPST, you can then digitally sign it. To do this, perform the following steps:

- Open the SPST using the SPST Editor.

  ☒ **NOTE:** You cannot edit a previously signed (or "finalized") SPST. Consequently, if you select a signed SPST, the Loading Signed SPST notification is displayed (rather than the SPST Signature Wizard dialog) to inform you of this fact:

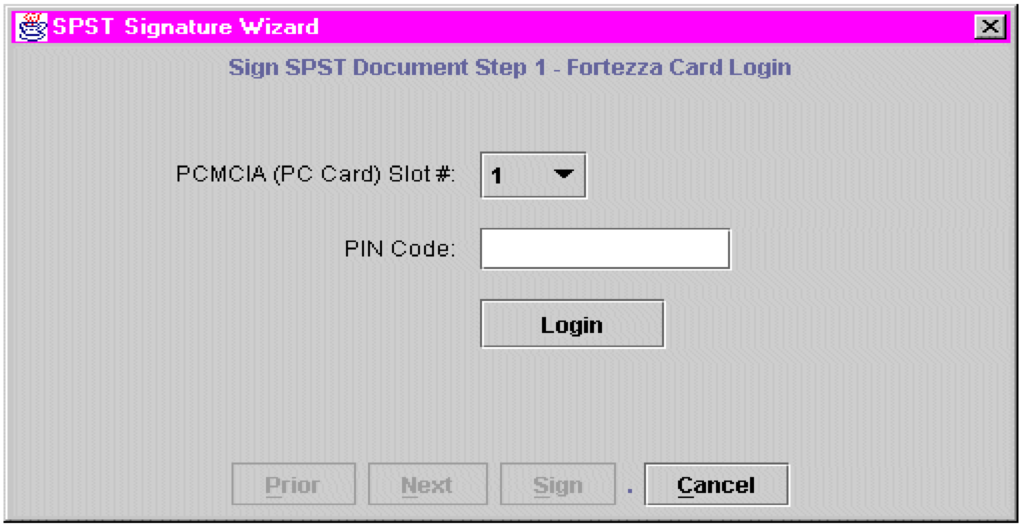


Loading Signed SPST

The loaded SPST is a final, signed document. Remove signature and make SPST in-process?

  If your intent is to remove the previous signature and make the SPST "in-process" again, then select the **Yes** button and proceed as follows. Otherwise, select the **No** button, upon which a confirmation notification is displayed, and then select the **OK** button to acknowledge the notification.

- Insert your Fortezza Crypto Card in the card reader.
- Select ***Sign SPST*** from the File menu. The SPST Signature Wizard dialog is displayed, reflecting Step 1 of the signing process (i.e., Fortezza Card Login):



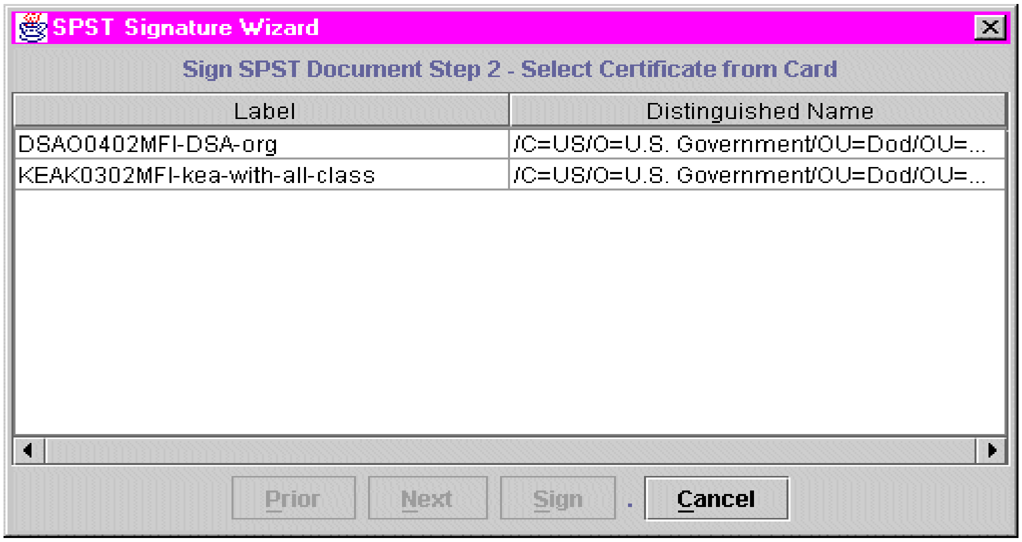
SPST Signature Wizard

Sign SPST Document Step 1 - Fortezza Card Login

PCMCIA (PC Card) Slot #: 1

PIN Code:

- Select the appropriate slot number in the PCMCIA (PC Card) Slot# field, enter the Fortezza Card PIN Code in the PIN Code field, and then select the **Login** button. You are then logged into the Fortezza Card, and the SPST Signature Wizard dialog is updated to reflect Step 2 of the signing process (i.e, certificate selection):

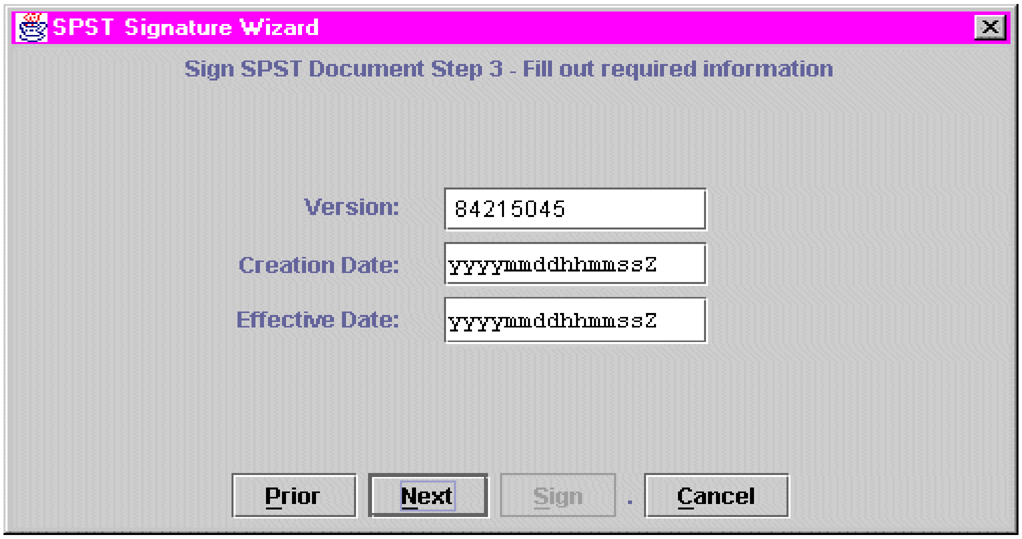


SPST Signature Wizard

Sign SPST Document Step 2 - Select Certificate from Card

Label	Distinguished Name
DSAO0402MFI-DSA-org	/C=US/O=U.S. Government/OU=Dod/OU=...
KEAK0302MFI-kea-with-all-class	/C=US/O=U.S. Government/OU=Dod/OU=...

- Highlight the appropriate certificate and then select the **Next** button. The SPST Signature Wizard dialog is updated to reflect Step 3 of the signing process (i.e., SPST header value input):



SPST Signature Wizard

Sign SPST Document Step 3 - Fill out required information

Version: 84215045

Creation Date: yyyymmddhhmmssZ

Effective Date: yyyymmddhhmmssZ

- Enter values in the following fields:

  Version: This is the version number of the SPST.

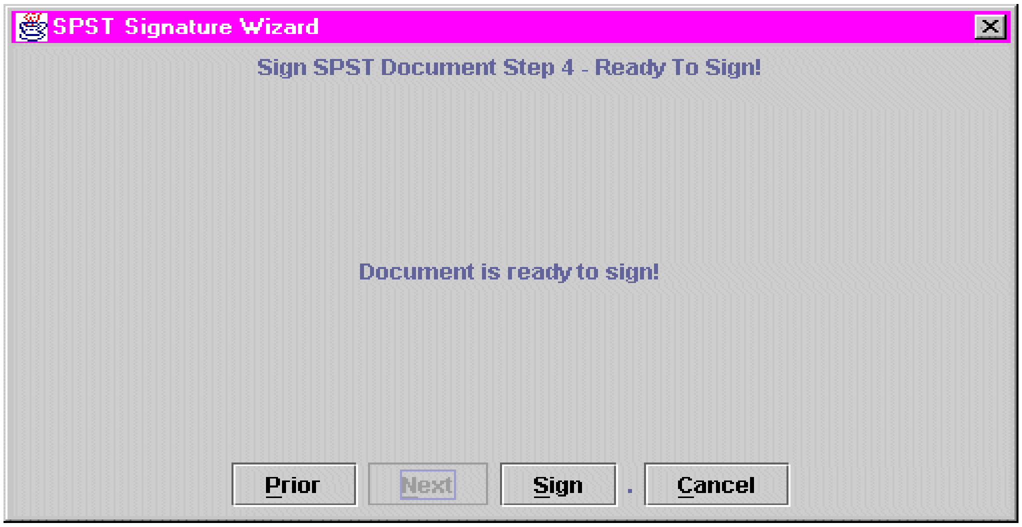
  Creation Date: This is the creation date (in Universal Coordinated Time, UTC) of the SPST.

  Effective Date: This is the date that you want the SPST to become effective. Enter the desired date in the following format:

  yyyymmddhhmmssZ

  where "yyyy" indicates the year, "mm" indicates the month, "dd" indicates the day, "hh" indicates the hour, "mm" indicates the minute, and "ss" indicates the second. The "Z" is automatically appended to the value and stands for Zulu time.

- Select the **Next** button. The SPST Signature Wizard dialog is updated to reflect Step 4 of the signing process (i.e., final signature assignation):



SPST Signature Wizard

Sign SPST Document Step 4 - Ready To Sign!

Document is ready to sign!

- Select the **Sign** button. The SPST is digitally signed and you are returned to the default SPST Editor Main Window.

SPST EDITOR LOGGING

The SPST Editor features a logging function that monitors and logs all user activities associated with creating, editing, and displaying SPSTs. Thus, whenever you invoke the SPST Editor to perform any of these operations, a log file is automatically created and saved to the *C:\cpe\csci\SecurityTranslationToolset\logs\SPSTEditor* folder.

☒ **NOTE:** To maintain and ensure the integrity of SPST Editor logging, only the system administrator (or other users with administrative privileges) can access (for the purpose of displaying, editing, or deleting) the associated log files. If necessary, refer to "SPST/SPTT Toolset Security Setup" in Chapter 2.

Log files are named as follows:

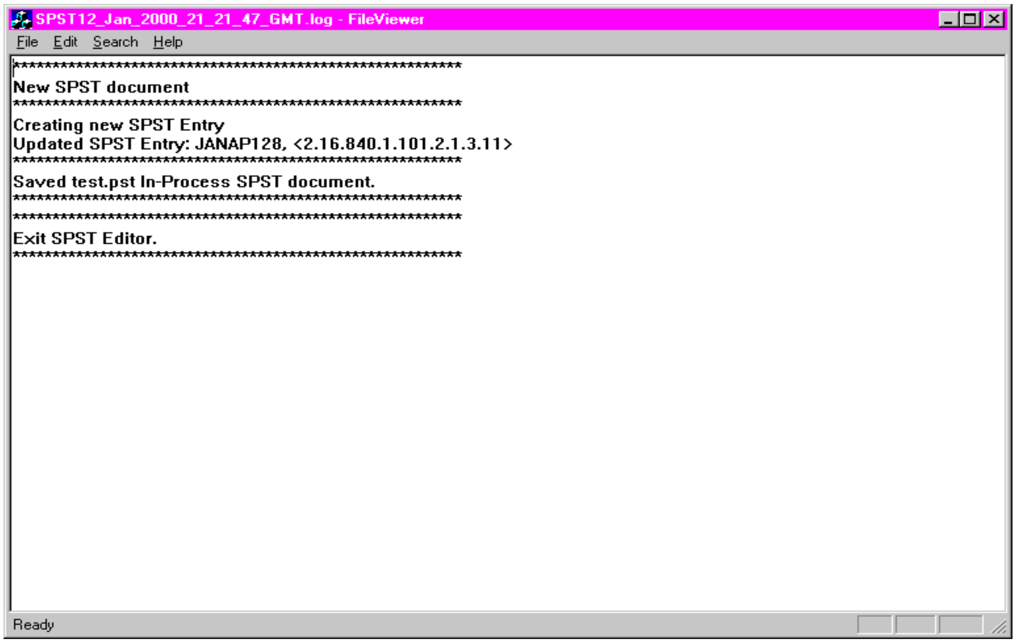
SPST[day]_[month]_[year]_[hour]_[minutes]_[seconds]_[time zone].log

Thus, the log file:

SPST12_Jan_2000_21_21_47_GMT.log

would have been created on January 12th, 2000, at 21:21:47, Greenwich Mean Time.

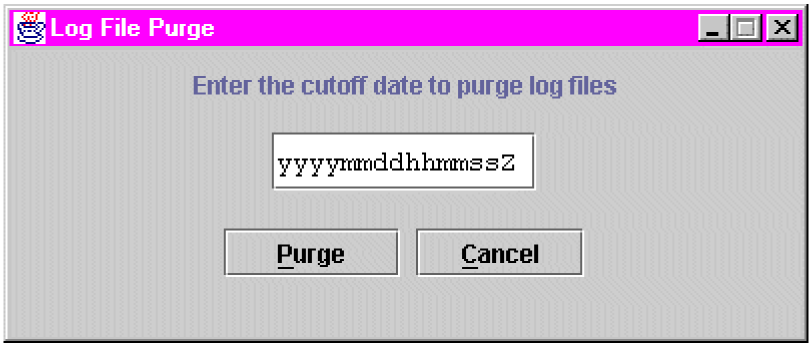
Log files can be accessed by selecting ***View Logs*** from the File menu and then specifying the file name when prompted. The following is an example of a log file (created on the above date and time):



```
************************************************************
New SPST document
************************************************************
Creating new SPST Entry
Updated SPST Entry: JANAP128, <2.16.840.1.101.2.1.3.11>
************************************************************
Saved test.pst In-Process SPST document.
************************************************************
************************************************************
Exit SPST Editor.
************************************************************
```

In this example, a user invoked the SPST Editor, defined an SPST entry, and then saved the SPST as: *test.pst.*

Log files can be deleted (again, only by the administrator or other users with administrative privileges) by selecting ***Purge Logs*** from the File menu. Upon doing this, the Log File Purge dialog is displayed:



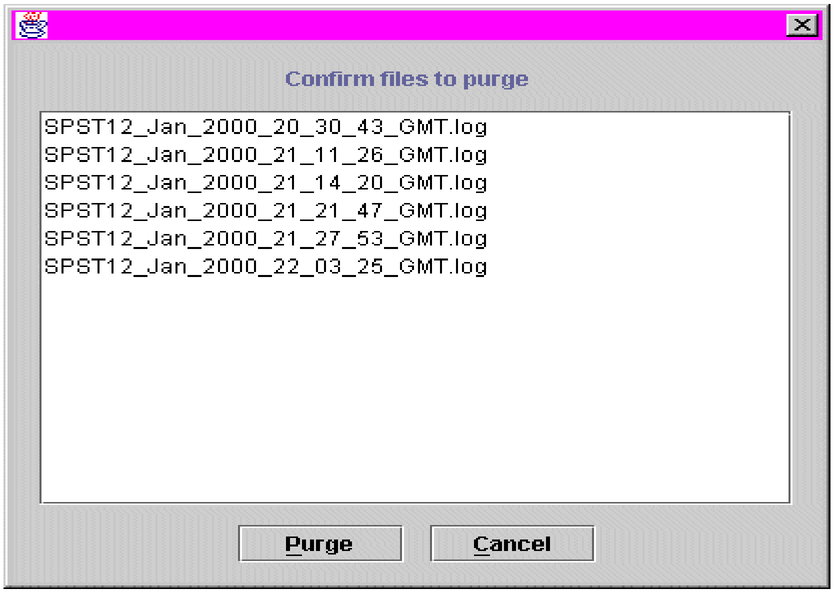
Enter the cutoff date to purge log files

- Enter the cutoff date (to purge log files) in the following format:

  yyyymmddhhmmssZ

  where “yyyy” indicates the year, “mm” indicates the month, “dd” indicates the day, “hh” indicates the hour, “mm” indicates the minute, and “ss” indicates the second. The “Z” is automatically appended to the value and stands for Zulu time.

- Select the **Purge** button. The Confirm Files to Purge dialog is then displayed:



Confirm files to purge

```
SPST12_Jan_2000_20_30_43_GMT.log
SPST12_Jan_2000_21_11_26_GMT.log
SPST12_Jan_2000_21_14_20_GMT.log
SPST12_Jan_2000_21_21_47_GMT.log
SPST12_Jan_2000_21_27_53_GMT.log
SPST12_Jan_2000_22_03_25_GMT.log
```

- Select the **Purge** button to confirm log file deletion. The log files are then deleted, and the dialog is closed.

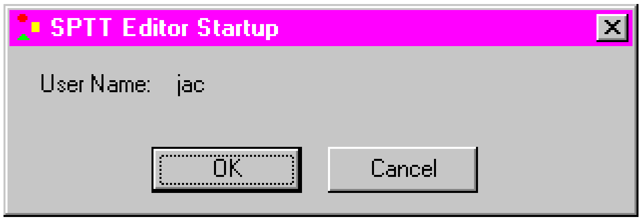
COMM
POWER

Chapter 4.
SPTT Editor Operations

This chapter describes how to start up the SPTT Editor, how to use the editor to create, modify, display, verify, or print (either to paper or ASCII file) Security Policy Translation Tables (SPTTs), and how to use the editor to digitally sign the SPTT. It also provides an overview of the SPTT Editor Main Window (in the startup section), as well as a discussion on SPTT Editor logging (specifically, how to view and purge the associated log files).

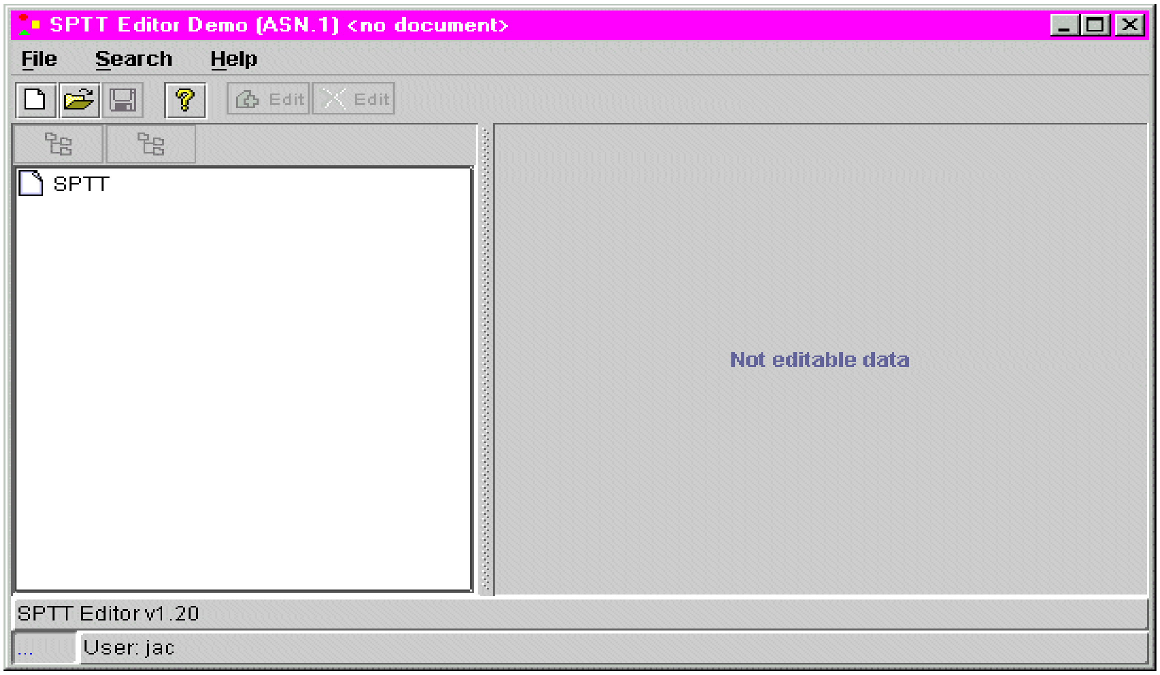
SPTT EDITOR STARTUP

To start up the SPTT Editor, select ***Start>>SPST-SPTT Toolset>>SPTT Editor*** from the desktop. The SPTT Editor Startup dialog is displayed:



User Name: jac

Select the **OK** button. The SPTT Editor Main Window is displayed:



SPTT Editor v1.20

User: jac

SPTT Editor Main Window Overview

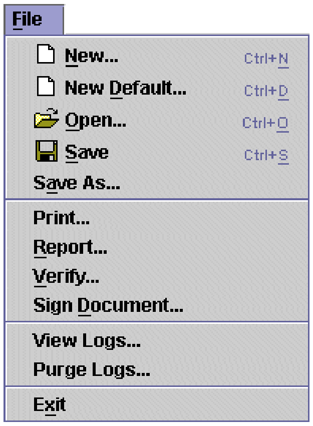
As shown above, the SPTT Editor Main Window comprises the following features:

- Menu Bar (across the top)
- Tool Bar (directly underneath the Menu Bar)
- Main Display Windows/Work Areas (on the left and right)
- Display Bars (across the bottom)

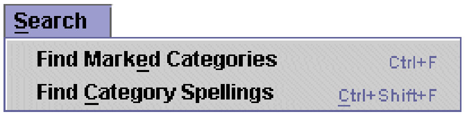
Menu Bar

The menu bar consists of three menus:

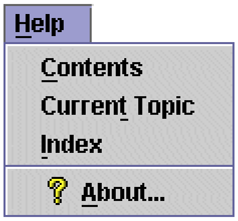
- **File Menu:** The File menu allows you to select standard file-related options including ***New, Open, Save, Save As,*** and ***Exit***. It also allows you to select some application-specific ones including ***New Default***, ***Print***, ***Report***, ***Verify***, ***Sign Document***, ***View Logs***, and ***Purge Logs***. These enable you to create a default SPTT, print information contained in a SPTT, output information contained in a SPTT to ASCII files, verify a SPTT, digitally sign a SPTT, view SPTT log files, and purge SPTT log files.



- **Search Menu:** The Search menu allows you to select application-specific search options including ***Find Marked Categories*** and ***Find Category Spellings***. These enable you to find previously marked categories and specific category spellings.


Search
Find Marked Categories Ctrl+F
Find Category Spellings Ctrl+Shift+F

- **Help Menu:** The Help menu allows you to select standard help-related options including ***Contents***, ***Current Topic***, ***Index***, and ***About***. These enable you to display a table of contents (from which a topic can be selected); display an index (from which an index item can be selected); display context-sensitive help information; and display information about the current software release.



Tool Bar

The tool bar, depending on the given operation, may feature any of the following application-specific buttons/icons:

- ✚ Edit The **+Edit** button allows you to select (or "mark") a security category for editing.
- ✕ Edit The **XEdit** button allows you to disable editing for a selected security category.
- ✚ Spelling The **+Spelling** button allows you to add a privacy mark/legacy mapping entry for a selected Security Policy Information File (SPIF) security classification.
- ✕ Spelling The **XSpelling** button allows you to remove a selected privacy mark/legacy list entry.
- The **Expand Tree** button allows you to expand the SPIF tree associated with a selected node.
- The **Contract Tree** button allows you to contract the SPIF tree associated with a selected node.
- ✚ Variable The **+Variable** button allows you to add a variable spelling entry for a selected SPIF required/allowed category item.
- ✕ Variable The **XVariable** button allows you to remove a selected variable spelling list entry.
- ✎ Variable The **\Variable** button allows you to edit a selected variable spelling list entry.
- ✚ Delim The **+Delim** button allows you to add a delimiter entry.
- ✕ Delim The **XDelim** button allows you to remove a selected delimiter entry.
- ✎ Delim The **\Delim** button allows you to edit a selected delimiter entry.

In addition to the above buttons, there are two tabs that are made available (directly over the right-hand pane) when defining categories. These are **Spellings** and **Settings** and control the type of information displayed and the user operations allowed in the right-hand pane.

Main Display Windows/Work Areas

The main display windows/work areas consist of two primary panes:

- **Left-hand Pane:** This pane is used for selecting (for the purpose of displaying or editing) SPTT headers, security classifications, and security categories.
- **Right-hand Pane**: This pane is used for defining SPTT headers, security classifications, and security categories selected in the left-hand pane.

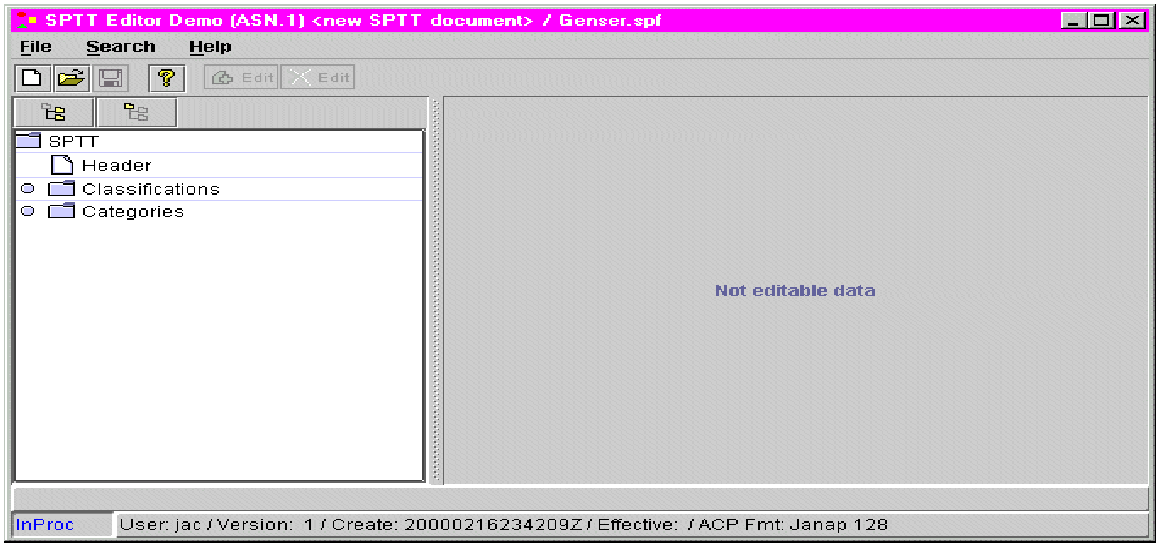
Display Bars

The display bars consist of two horizontal bars (at the bottom), the first of which displays feedback relating to operator selections and the second of which displays the SPTT status (i.e., "InProc" or "Signed" for In Process or Signed SPTT), the user name of the person currently logged onto the SPTT Editor, and SPTT header information.

CREATE/OPEN SPTT

Upon invoking the SPTT Editor via the Windows NT Start menu, you must choose to either create/open a "regular" SPTT or create/open a "default" SPTT, and then perform "1" or "2" below depending upon your choice. *Basically speaking, a default SPTT is one that maps Security Policy Information File (SPIF) classification values to MFI Local Classification values. As such, it contains no other classification/category translation data and thus can be thought of as an "abbreviated" SPTT.*

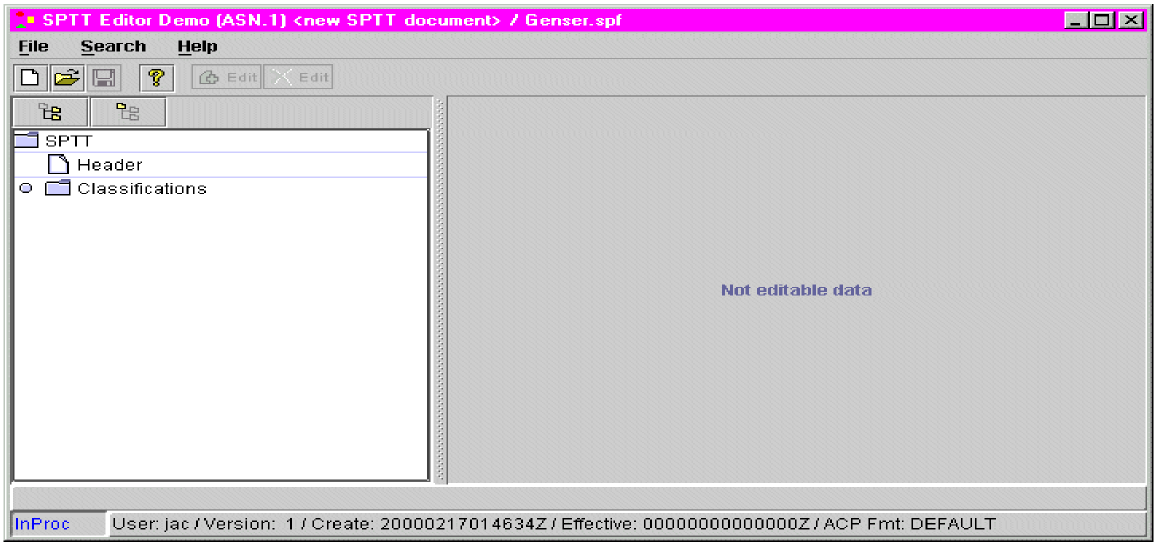
1. If your intent is to create or open a regular SPTT, then select ***New*** or ***Open*** from the File Menu. (You can also accomplish this by selecting the Paper or Folder icons, respectively.) If you select ***New***, you will be prompted to supply the location of the Security Policy Information File (SPIF) for which the SPTT will be built. If you select ***Open***, you will be prompted to supply the location of the regular SPTT file. Once done, a tree structure of the SPIF data is displayed in the left-hand pane:



Not editable data

InProc User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128

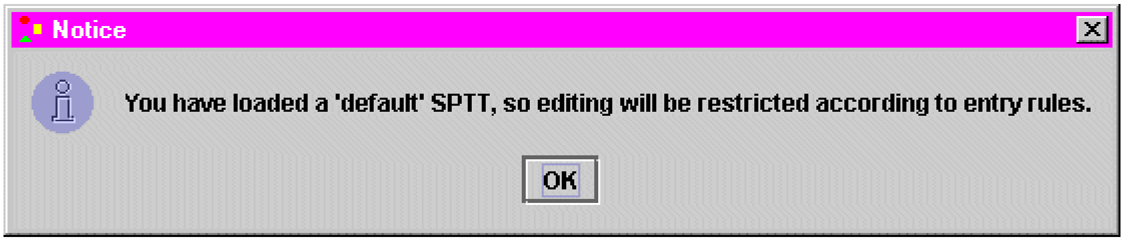
2. If your intent is to create or open a default SPTT, then select ***New Default*** or ***Open*** from the File Menu. If you select ***New Default***, you will be prompted to supply the location of the SPIF for which the default SPTT will be built. Once done, a tree structure of the SPIF data is displayed in the left-hand pane:



Not editable data

InProc User: jac / Version: 1 / Create: 20000217014634Z / Effective: 00000000000000Z / ACP Fmt: DEFAULT

If you select ***Open***, you will be prompted to supply the location of the default SPTT file. However, once done, the following Notice dialog is displayed to inform you that editing will be restricted according to entry rules. (This also serves as a reminder that you have selected a default SPTT.) Select the **OK** button to acknowledge the notification and then the tree structure (of SPIF data) is displayed (as shown in the previous figure).



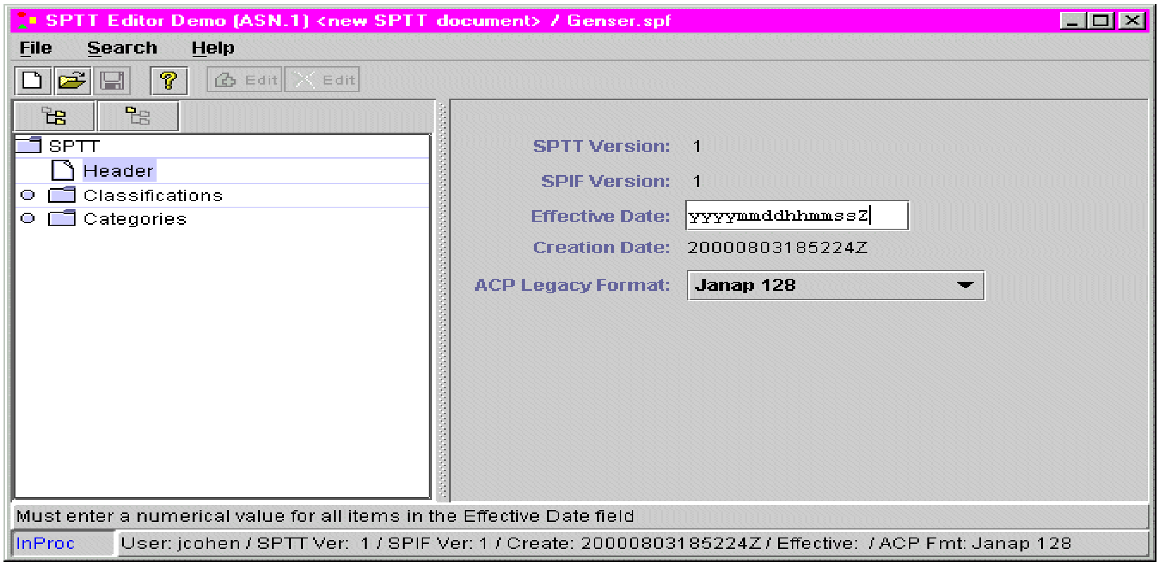
You have loaded a 'default' SPTT, so editing will be restricted according to entry rules.

As alluded to above, the data and operations provided when creating or editing default SPTTs are constrained somewhat over those provided when creating or editing regular SPTTs. That is, you can define header information as well as classifications for a default SPTT, but you cannot define categories (thus the Categories folder isn't even displayed). Further, when defining headers or classifications, you can do some but not all of the operations normally afforded when creating or editing a regular SPTT. For example, when defining the header for a default SPTT, you can only specify/change the Effective Date, whereas when defining the header for a regular SPTT, you can specify/change the ACP Legacy Format as well. These types of operator constraints are also effective when defining classifications for a default SPTT. That is, you can define MFI Local Classifications but you cannot define classification spellings nor can you select Required/Allowed Categories.

Regardless of whether you performed “1” or “2” above, you are now free to create or modify the regular or default SPTT in accordance with the procedures described below. However, keep in mind that certain operator constraints are imposed when using the editor to create or modify default SPTTs (as stated above) and that the procedures are written from the perspective of creating or modifying a regular SPTT (and thus all functionalities are described).

Define SPTT Header

To define the SPTT header, select the **Header** folder in the left-hand pane. The header fields are displayed in the right-hand pane:



SPTT Version: 1

SPIF Version: 1

Effective Date: yyyymmddhhmmssZ

Creation Date: 20000803185224Z

ACP Legacy Format: Janap 128

Must enter a numerical value for all items in the Effective Date field

InProc User: jcohen / SPTT Ver: 1 / SPIF Ver: 1 / Create: 20000803185224Z / Effective: / ACP Fmt: Janap 128

The header fields (specifically, Effective Date and ACP Legacy Format) are provided to enable you to specify the effective date and ACP legacy format for your SPTT. Header fields include:

SPTT Version: This is the version number of the SPTT. This field is display only.

SPIF Version: This is the version number of the SPIF upon which the SPTT is based. This field is display only.

Effective Date: This is the date that you want the SPTT to become effective. Enter the desired date in the following format:

yyyymmddhhmmssZ

where "yyyy" indicates the year, "mm" indicates the month, "dd" indicates the day, "hh" indicates the hour, "mm" indicates the minute, and "ss" indicates the second. The "Z" is automatically appended to the value and stands for Zulu time.

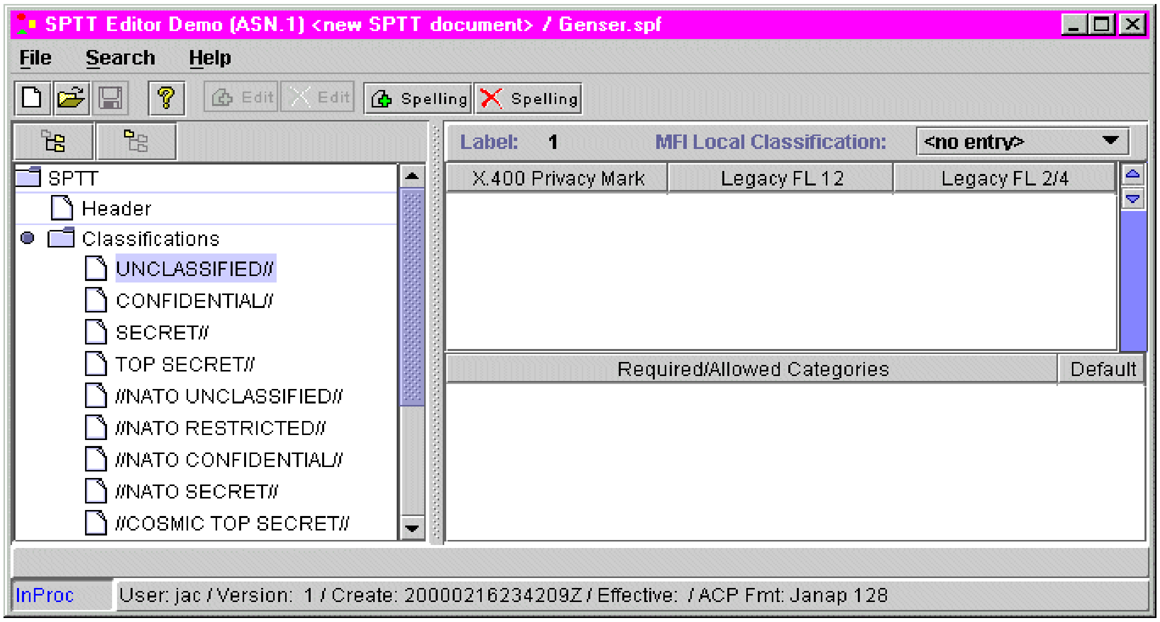
Creation Date: This is the creation date (in Universal Coordinated Time, UTC) of the SPTT. This field is display only.

ACP Legacy Format: This is the ACP legacy format for the SPTT. Select the desired ACP legacy format from the associated menu box.

☒ **NOTE:** You can, if desired, postpone defining the SPTT header until you're actually ready to make your SPTT operational (or "effective").

Define Classifications

Select the open icon to the left of the **Classifications** folder (in the left-hand pane) to define the legacy translations of the basic classification levels. (*This step must be done before categories can be defined since categories are dependent upon classifications.*) The SPIF classification levels are displayed directly below the **Classifications** folder, the right-hand pane is redisplayed to include the appropriate classification parameters, and the appropriate buttons are added to the button bar to support parameter definition:

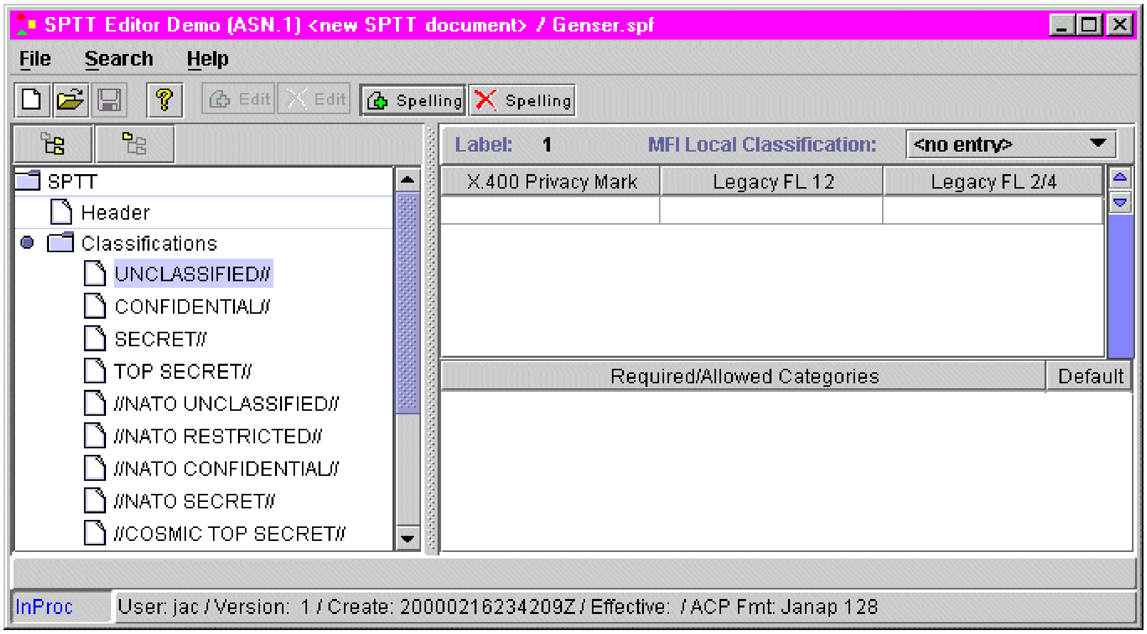


Label: 1 MFI Local Classification: <no entry>

User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128

Each of these classifications should be defined as follows:

- Define the classification spellings by clicking on a classification level (e.g., UNCLASSIFIED) and selecting the **+Spelling** button. A row of blank cells is added to the right-hand middle pane, directly under the X.400 Privacy Mark/Legacy FL12/Legacy FL2/4 headings:



Label: 1 MFI Local Classification: <no entry>

User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128

- Fill in these cells as necessary by clicking on the desired cell and typing. The cells are defined as follows:

  X.400 Privacy Mark: This is a text value to be carried around within the ACP-120 label for conversions from Legacy to ACP-120. This is used to convey values such as CLEAR.

Legacy FL12: This is the classification string that appears in the FL12a format line of the legacy message.

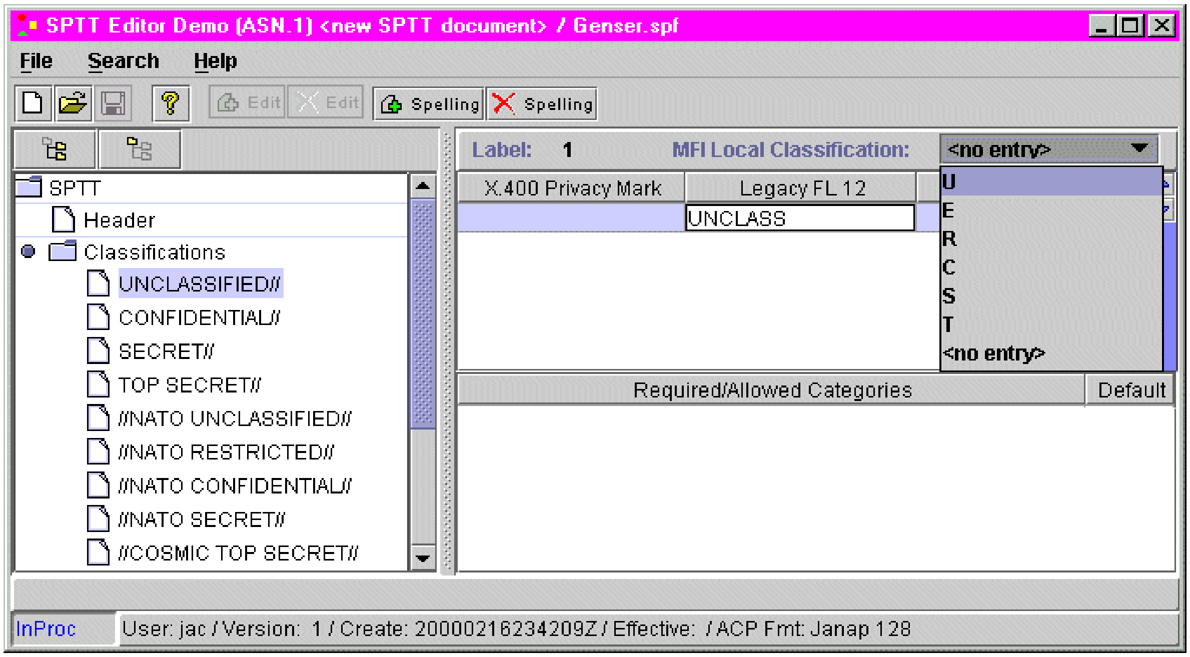
Legacy FL2/4: This is the classification character that appears in the FL2 and FL4 format lines of the legacy message.

☒ **NOTE:** Multiple rows of values can be added for each classification value. That is, upon specifying the desired cell values for a given row, you can select the **+Spelling** button again and another row of blank cells is displayed. Also note that the **XSpelling** button is provided to enable you to remove or delete a selected row.

- Specify an MFI local classification equivalency for each classification value.

  ☒ **NOTE:** This value is needed so that the MFG knows at what internal level to process the associated SPIF classification value. Hence, this must be done for each SPIF classification value!

  To do this, select the pull-down menu to the right of the MFI Local Classification field. A menu box is then presented from which a local classification can be selected:



Label: 1 MFI Local Classification: <no entry>

X.400 Privacy Mark	Legacy FL 12
	UNCLASS

User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128

- For each SPIF classification value, default categories can be selected IF the SPIF contains required/allowed categories for the particular classification levels. If the Required/Allowed Categories pane contains allowed/required categories, then default values can be selected.

  During label translation from Legacy to X.400, these selected default categories will be added to the ACP-120 label automatically IF the SPIF stipulated required/allowed rules are NOT met (i.e., only one, all, one or more).

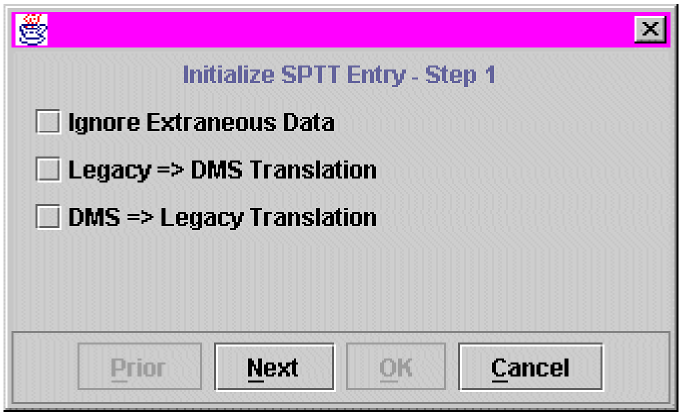
Define and Verify Categories

Define Categories

Once you have defined classifications for your SPTT, you can then define the desired categories. There are two types of categories that can be defined:

- **Level 3 Categories:** These are categories that are listed at the 3rd level in a displayed SPIF tree. In the subsequent main window example, these would include "USA", "CAN", "DEU", "FRA", "NLD", "NOR", "PRT", and "GBR". Level 3 Categories DO NOT contain country codes.
- **Level 2 Categories:** These are categories that are listed at the 2nd level in a displayed SPIF tree. In the subsequent main window example, these would include "GENSER DOD EYES ONLY" and "GENSER INTEL EYES ONLY (Tag set 7 – Tag type 2)". Level 2 Categories do contain country codes, all of which are listed at the corresponding level 3.

To define categories, select the open icon to the left of the **Categories** folder, highlight (by clicking) the desired category, and then click the **+Edit** button. Upon doing so, the plus sign to the left of the category is enabled (or selected), the right-hand pane is redisplayed to include the appropriate configuration parameters, the appropriate buttons are added to the button bar to support parameter definition, and the Initialize SPTT Entry – Step 1 dialog is displayed:


Initialize SPTT Entry - Step 1

□ Ignore Extraneous Data

□ Legacy => DMS Translation

□ DMS => Legacy Translation

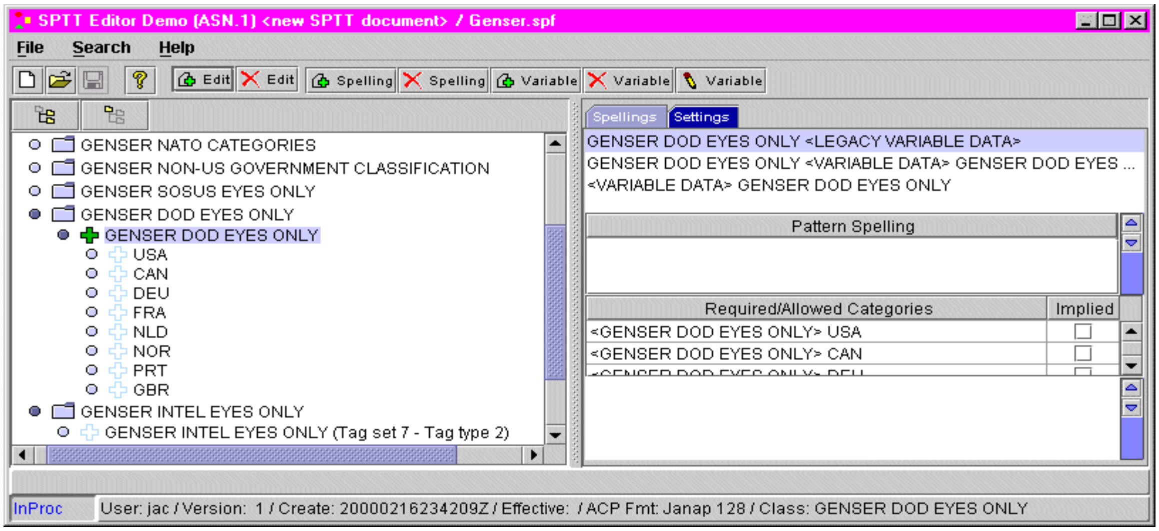
Select any or all of the following options:

Ignore Extraneous Data. This can be selected depending upon whether unrecognized legacy country codes are to be accepted or not.

Legacy=>DMS Translation. This can be selected for Legacy to DMS Translations.

DMS=>Legacy Translation. This can be selected for DMS to Legacy Translations.

Select the **Next** button and enter a Special Handling Designator (SHD) in the SHD field, if applicable, and click the **Next** button again and then the **OK** button. The Initialize SPTT Entry – Step 1 dialog is closed, providing you full access to the fields and buttons necessary to configure your SPTT security categories. The buttons provided and thus the operations afforded will vary depending upon whether you selected a Level 2 or a Level 3 Category:



- ○ GENSER NATO CATEGORIES
- ○ GENSER NON-US GOVERNMENT CLASSIFICATION
- ○ GENSER SOSUS EYES ONLY
- ● GENSER DOD EYES ONLY
  - ● GENSER DOD EYES ONLY
    - ○ USA
    - ○ CAN
    - ○ DEU
    - ○ FRA
    - ○ NLD
    - ○ NOR
    - ○ PRT
    - ○ GBR
- ● GENSER INTEL EYES ONLY
  - ○ GENSER INTEL EYES ONLY (Tag set 7 - Tag type 2)

GENSER DOD EYES ONLY <LEGACY VARIABLE DATA>
GENSER DOD EYES ONLY <VARIABLE DATA> GENSER DOD EYES ...
<VARIABLE DATA> GENSER DOD EYES ONLY

Pattern Spelling

Required/Allowed Categories	Implied
<GENSER DOD EYES ONLY> USA	☐
<GENSER DOD EYES ONLY> CAN	☐
<GENSER DOD EYES ONLY> DEU	☐

InProc User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128 / Class: GENSER DOD EYES ONLY

To continue, go to either “Level 2 Category Definitions” or “Level 3 Category Definitions” below, depending on the type of category you have selected.

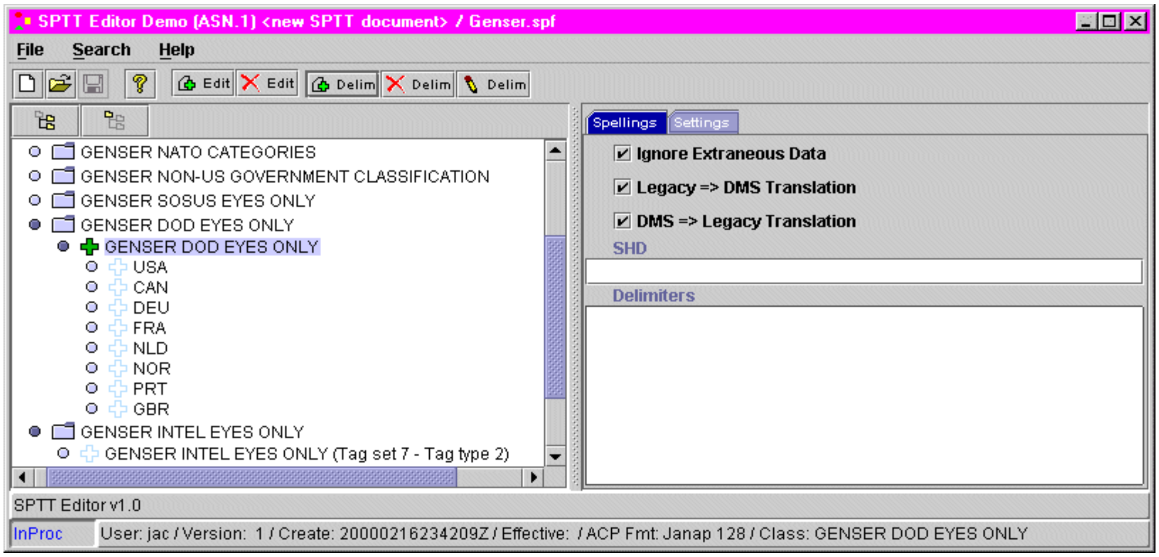
☒ **NOTE:** If editing (or viewing) a SPTT, you can, if desired, select ***Find Marked Categories*** from the Search menu to list all previously marked categories in the right-hand pane. You can then select any category in the list, after which the right-hand pane is redisplayed to reflect the associated category parameters. You can also select ***Find Category Spellings*** from the Search menu to search for specific category spellings.

Level 2 Category Definitions

- Select a pattern from the top right-hand pane by clicking it. For Level 2 Categories, there are three patterns available (as shown in the above example).
- Once a pattern is chosen, select the **+Spelling** button and define the fixed text part of the pattern, e.g., “GENSER DOD EYES ONLY”, in the associated field. Multiple patterns can be added by repeating this step for each additional pattern desired. Any previously added spelling can be edited by selecting and retyping it. Also, entries can be deleted by highlighting the row and then selecting the **XSpelling** button.
- Define the desired country codes in the Required/Allowed Categories pane. This pane contains a complete list of country codes that are required/allowed per the SPIF definition. Any country code can be set to an “implied” state simply by clicking the box associated with the country code. An implied state means that this country code will be added to the translated label unconditionally, whether or not it was contained in the original label.
- For each country code, a set of legacy spellings must also be defined.

First click on the country code, and then select the **+Variable** button. This allows you to enter the legacy representation of the country code. More than one spelling can be defined by repeating this step. As spellings are added, they are displayed in the bottom right-hand pane.

- Once country codes have been defined, they can be edited or deleted by selecting the entry and then clicking the **\Variable** button or the **XVariable** button, respectively.
- Select the **Settings** tab to complete the definition. The right-hand pane is redisplayed to include the remaining configuration parameters, and the appropriate buttons are added to the button bar to support configuration of these parameters:



SPTT Editor Demo (ASN.1) <new SPTT document> / Genser.spf

○ GENSER NATO CATEGORIES
○ GENSER NON-US GOVERNMENT CLASSIFICATION
○ GENSER SOSUS EYES ONLY
● GENSER DOD EYES ONLY
● GENSER DOD EYES ONLY
○ USA
○ CAN
○ DEU
○ FRA
○ NLD
○ NOR
○ PRT
○ GBR
● GENSER INTEL EYES ONLY
○ GENSER INTEL EYES ONLY (Tag set 7 - Tag type 2)

☑ Ignore Extraneous Data
☑ Legacy => DMS Translation
☑ DMS => Legacy Translation
SHD
Delimiters

SPTT Editor v1.0
InProc User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128 / Class: GENSER DOD EYES ONLY

The upper right-hand pane displays the initialization parameters specified upon first selecting the Level 2 category (if necessary, see above). (*You can change these, if desired.*) The bottom right-hand pane is the Delimiters pane.

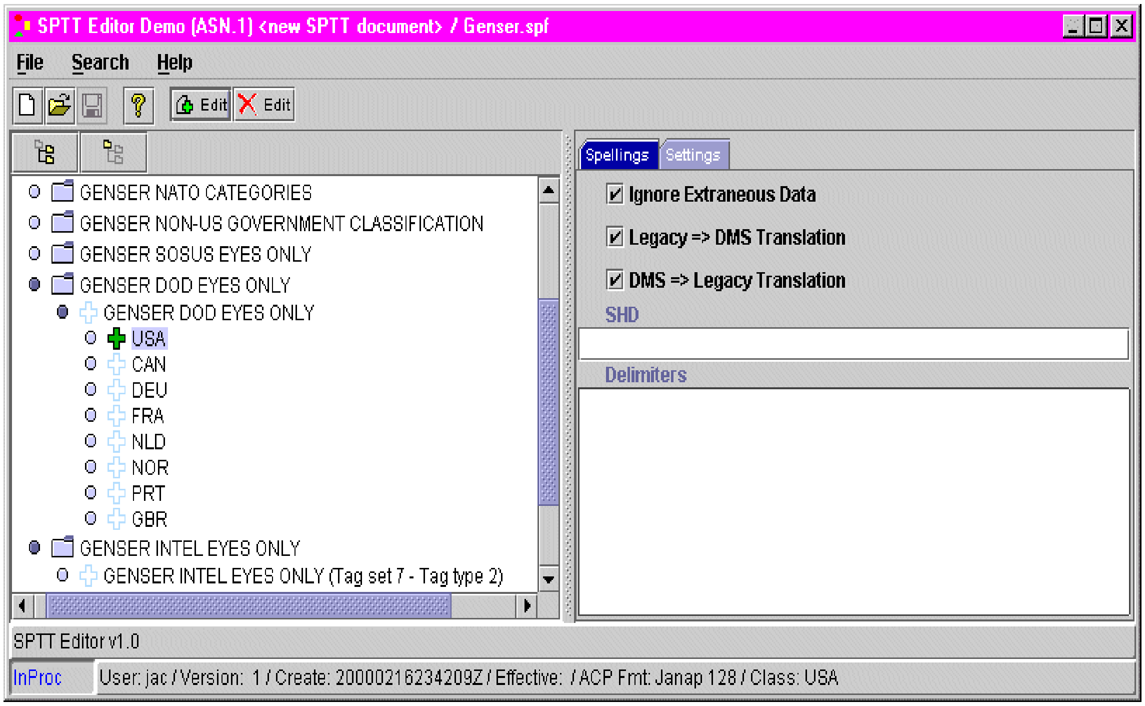
- Define the country code delimiters in the Delimiters pane. These are characters that are used in the legacy format to separate the individual country code values, i.e., /. Delimiters are added, deleted, or edited by selecting the **+Delim**, **XDelim**, or **\Delim** button, respectively.
- Verify the SPTT in accordance with the procedures described below in “Verify the SPTT for Duplicate Category Spellings”.

Level 3 Category Definitions

For Level 3 Category Definitions, there is only one applicable pattern since Level 3 Categories do not contain country codes.

- Select the **+Spelling** button to enable you to define the spelling pattern for the category. Multiple patterns can be added by repeating this step for each additional spelling pattern desired. Any previously added spelling can be edited by selecting and retyping it. Also, entries can be deleted by highlighting the row to be deleted and then selecting the **XSpelling** button.

- In the Required/Allowed Categories pane, may be a list of SPIF defined categories associated with the category. Any of these may be selected as "implied" meaning that they will be added unconditionally to the translated label, whether or not they appeared in the original label.
- Select the **Settings** tab to complete the definition. The right-hand pane is redisplayed to include the remaining configuration parameters:



SPTT Editor Demo (ASN.1) <new SPTT document> / Genser.spf

- ○ GENSER NATO CATEGORIES
- ○ GENSER NON-US GOVERNMENT CLASSIFICATION
- ○ GENSER SOSUS EYES ONLY
- ● GENSER DOD EYES ONLY
  - ● GENSER DOD EYES ONLY
    - ○ USA
    - ○ CAN
    - ○ DEU
    - ○ FRA
    - ○ NLD
    - ○ NOR
    - ○ PRT
    - ○ GBR
- ● GENSER INTEL EYES ONLY
  - ○ GENSER INTEL EYES ONLY (Tag set 7 - Tag type 2)

☑ Ignore Extraneous Data

☑ Legacy => DMS Translation

☑ DMS => Legacy Translation

SHD

Delimiters

SPTT Editor v1.0

InProc User: jac / Version: 1 / Create: 20000216234209Z / Effective: / ACP Fmt: Janap 128 / Class: USA

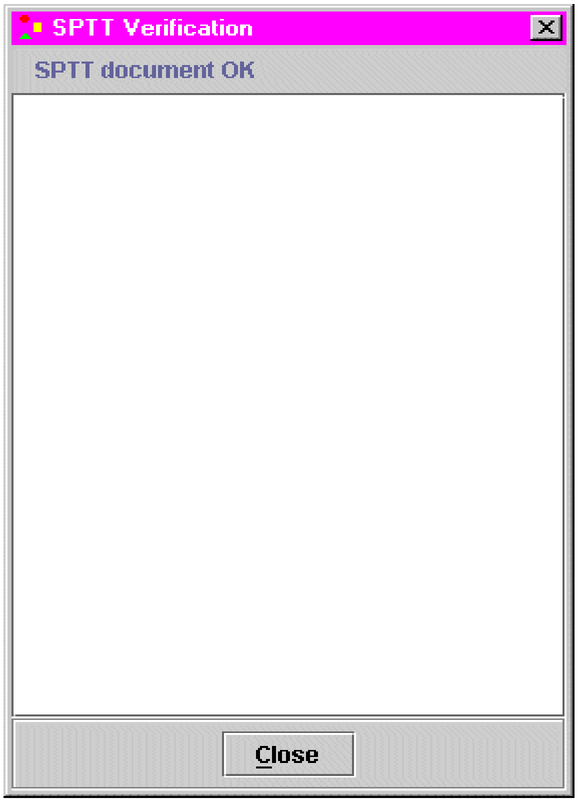
The upper right-hand pane displays the initialization parameters specified upon first selecting the Level 3 category (if necessary, see above). (*You can change these, if desired.*) The bottom right-hand pane, the Delimiters pane, is not applicable to Level 3 Categories and thus is grayed out (or disabled).

- Verify the SPTT in accordance with the procedures described below in "Verify the SPTT for Duplicate Category Spellings".

Verify the SPTT for Duplicate Category Spellings

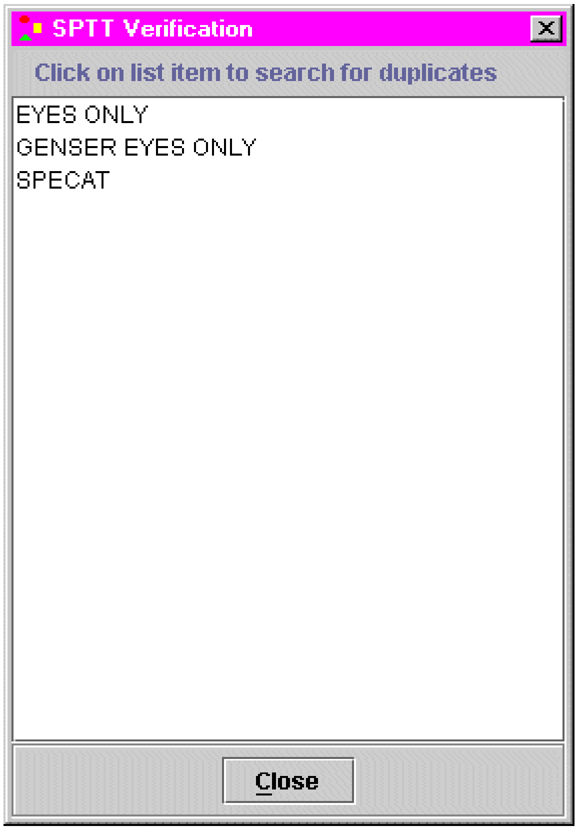
After you've finished defining categories for your SPTT, you should verify the SPTT for any duplicate spellings that may exist across SPTT categories. To do this, perform the following steps:

1. Select ***Verify*** from the File menu. If no duplicate spellings are found, the SPTT Verification dialog is displayed confirming this fact (i.e., "SPTT document OK") and you can proceed to Step 6 below:



SPTT document OK

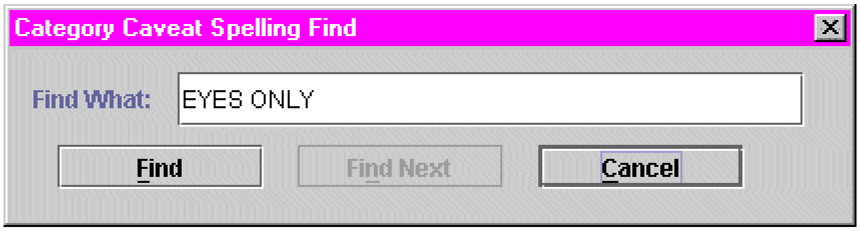
If, on the other hand, duplicate spellings are found, the SPTT Verification dialog is displayed, reflecting these duplicate spellings:



Click on list item to search for duplicates

EYES ONLY
GENSER EYES ONLY
SPECAT

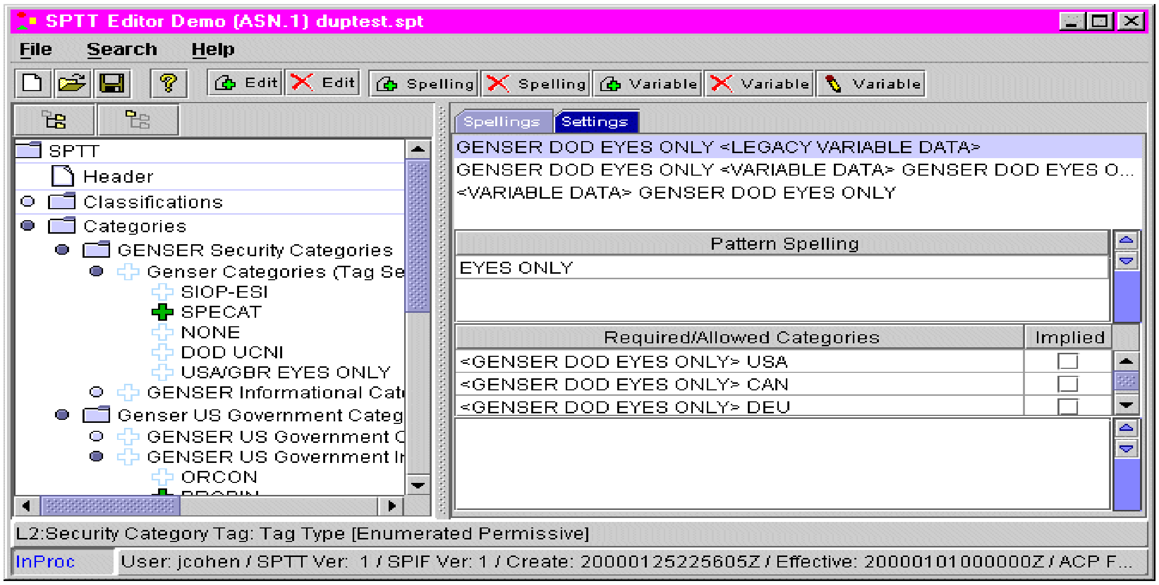
2. Select (or highlight) the first duplicate entry (in this case, "Eyes Only"). The Category Caveat Spelling Find dialog is displayed:



Category Caveat Spelling Find

Find What: EYES ONLY

3. Select the **Find** button. The search operation is commenced and the first occurrence of the highlighted entry (again, "Eyes Only") is displayed in the Pattern Spelling pane:



SPTT Editor Demo (ASN.1) duptest.spt

GENSER DOD EYES ONLY <LEGACY VARIABLE DATA>
GENSER DOD EYES ONLY <VARIABLE DATA> GENSER DOD EYES O...
<VARIABLE DATA> GENSER DOD EYES ONLY

Pattern Spelling
EYES ONLY

Required/Allowed Categories	Implied
<GENSER DOD EYES ONLY> USA	□
<GENSER DOD EYES ONLY> CAN	□
<GENSER DOD EYES ONLY> DEU	□

L2:Security Category Tag: Tag Type [Enumerated Permissive]

InProc User: jcohen / SPTT Ver: 1 / SPIF Ver: 1 / Create: 20000125225605Z / Effective: 20000101000000Z / ACP F...

4. Select the **Find Next** button to display all subsequent duplicate spellings of the first entry. Reconcile (or, if desired, "ignore") duplicate spelling occurrences of the first entry and then repeat the above steps for any additional duplicate spelling entries in the list.

5. Select the **Close** button in the SPTT Verification dialog and then repeat the SPTT verification by once again selecting ***Verify*** from the File menu. The SPTT Verification dialog should be redisplayed with the "SPTT document OK" confirmation (i.e., without any duplicate spelling entries). If not, you will need to repeat the appropriate steps above to reconcile any duplicate spelling entries cited in the new list.

6. Save the SPTT file, once completed and verified. If saving for the first time, select ***Save As*** from the File pull-down menu and supply the file location and name when prompted. Otherwise, if editing an existing SPTT, select ***Save*** from the File pull-down menu or click the Diskette icon.

7. Exit the SPTT Editor by selecting ***Exit*** from the File menu or by selecting the **Close** ("X") button in the upper right-hand corner of the SPTT Editor Main Window. Select the **Yes** button in response to the

confirmation dialog.

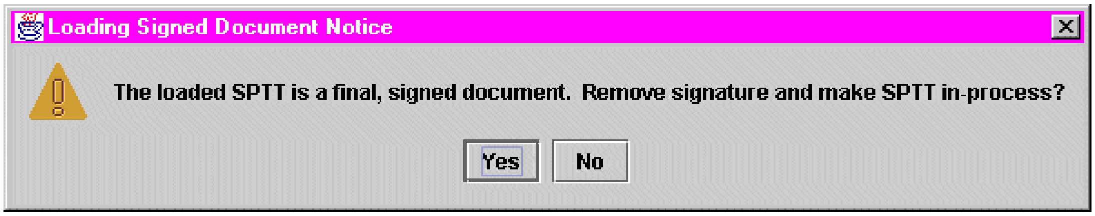
8. Validate the SPTT via the SPTT Simulator (see Chapter 5). Once validated, the SPTT can be digitally signed by performing the procedures described below in "Digitally Signing the SPTT".

DIGITALLY SIGNING THE SPTT

After you've finished creating, editing and/or verifying your SPTT and have successfully validated it using the SPTT Simulator (if necessary, see Chapter 5), you can then digitally sign it. To do this, perform the following steps:

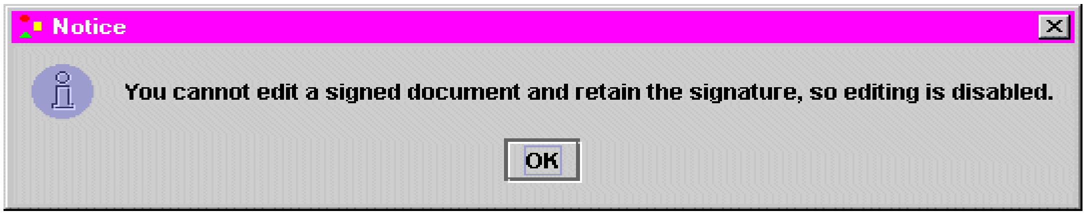
- Open the SPTT using the SPTT Editor.

☒ **NOTE:** You cannot edit a previously signed (or "finalized") SPTT. Consequently, if you select a signed SPTT, the Loading Signed Document Notice dialog is displayed (rather than the SPTT Signature Wizard dialog) to inform you of this fact:



The loaded SPTT is a final, signed document. Remove signature and make SPTT in-process?

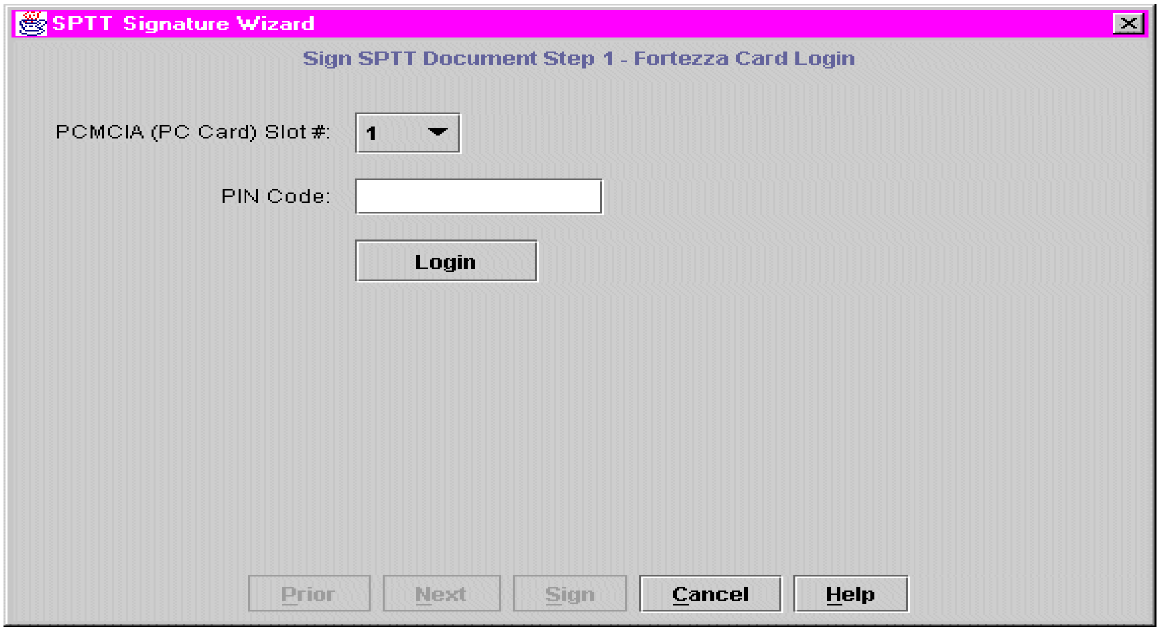
If your intent is merely to view (but not remove the signature from) the signed document, then select the **No** button. The following Notice dialog is then displayed to inform you that you cannot edit a signed document. Select the **OK** button to acknowledge the notification.



You cannot edit a signed document and retain the signature, so editing is disabled.

If, on the other hand, your intent is to remove the previous signature and make the SPTT "in-process" again, then select the **Yes** button and proceed as follows:

- Insert your Fortezza Crypto Card in the card reader.
- Select ***Sign Document*** from the File menu. The SPTT Signature Wizard dialog is displayed, reflecting Step 1 of the signing process (i.e., Fortezza Card Login):



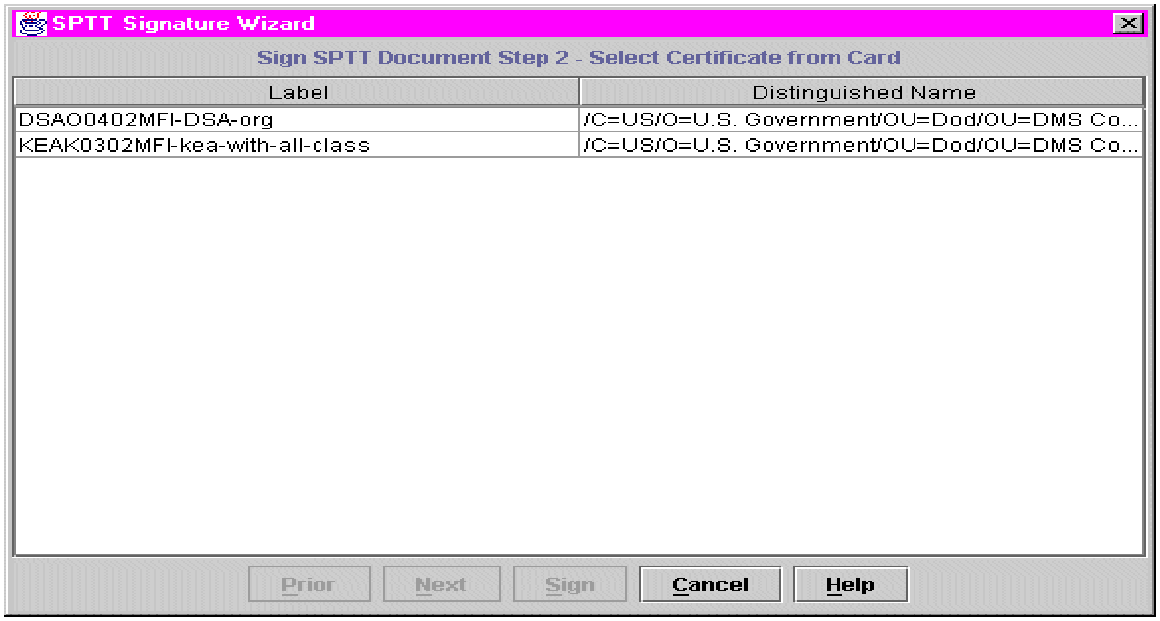
SPTT Signature Wizard

Sign SPTT Document Step 1 - Fortezza Card Login

PCMCIA (PC Card) Slot #: 1

PIN Code:

- Select the appropriate slot number in the PCMCIA (PC Card) Slot# field, enter the Fortezza Card PIN Code in the PIN Code field, and then select the **Login** button. You are then logged into the Fortezza Card, and the SPTT Signature Wizard dialog is updated to reflect Step 2 of the signing process (i.e, certificate selection):

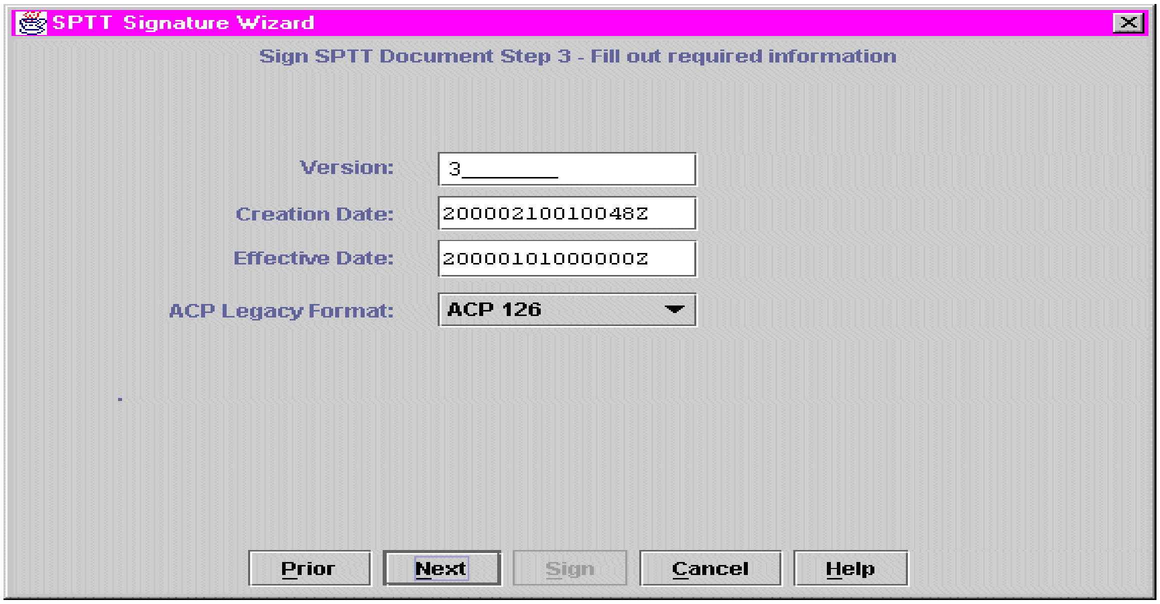


SPTT Signature Wizard

Sign SPTT Document Step 2 - Select Certificate from Card

Label	Distinguished Name
DSAO0402MFI-DSA-org	/C=US/O=U.S. Government/OU=Dod/OU=DMS Co...
KEAK0302MFI-kea-with-all-class	/C=US/O=U.S. Government/OU=Dod/OU=DMS Co...

- Highlight the appropriate certificate and then select the **Next** button. The SPTT Signature Wizard dialog is updated to reflect Step 3 of the signing process (i.e., SPTT header value input, modification, or acceptance):



SPTT Signature Wizard

Sign SPTT Document Step 3 - Fill out required information

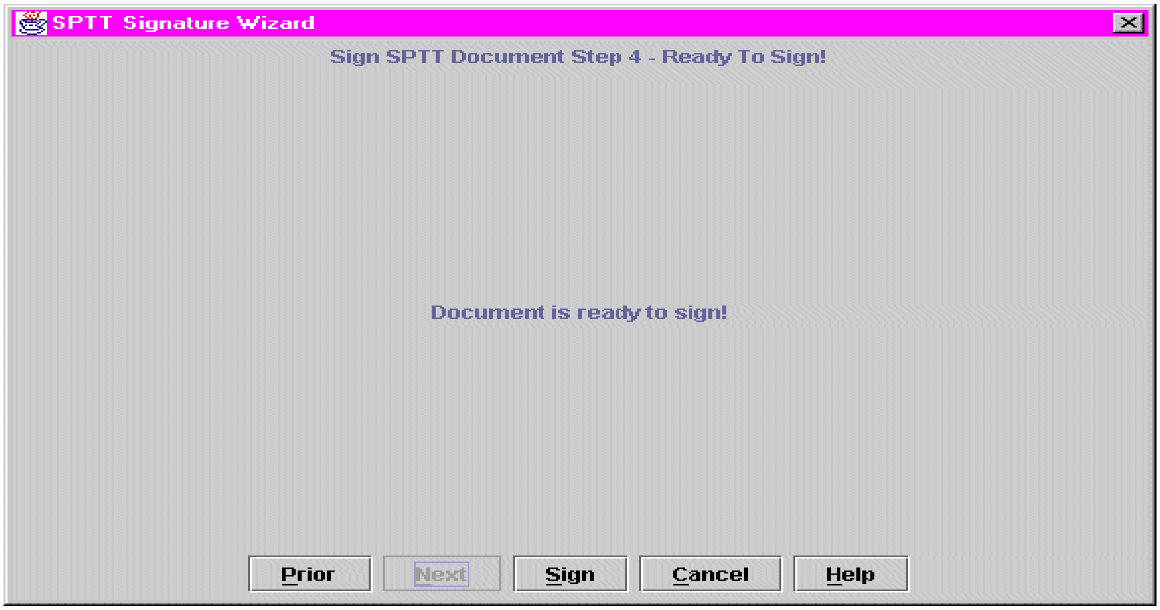
Version: 3________

Creation Date: 20000210010048Z

Effective Date: 20000101000000Z

ACP Legacy Format: ACP 126

- Enter/modify values in the Version, Creation Date, Effective Date, and ACP Legacy Format fields and select the **Next** button. (For a description of these fields, please refer to "Define SPTT Header" above.) Otherwise, if accepting the displayed values, select the **Next** button directly. In either case, the SPTT Signature Wizard dialog is updated to reflect Step 4 of the signing process (i.e., final signature assignation):



SPTT Signature Wizard

Sign SPTT Document Step 4 - Ready To Sign!

Document is ready to sign!

- Select the **Sign** button. The SPTT is digitally signed and you are returned to the default SPTT Editor Main Window.

SPTT EDITOR LOGGING

The SPTT Editor features a logging function that monitors and logs all user activities associated with creating, editing, and displaying SPTTs. Thus, whenever you invoke the SPTT Editor to perform any of these operations, a log file is automatically created and saved to the

C:\cpe\csci\SecurityTranslationToolset\logs\SPTTEditor folder.

☒ **NOTE:** To maintain and ensure the integrity of SPTT Editor logging, only the system administrator (or other users with administrative privileges) can access (for the purpose of displaying, editing, or deleting) the associated log files. If necessary, refer to "SPST/SPTT Toolset Security Setup" in Chapter 2.

Log files are named as follows:

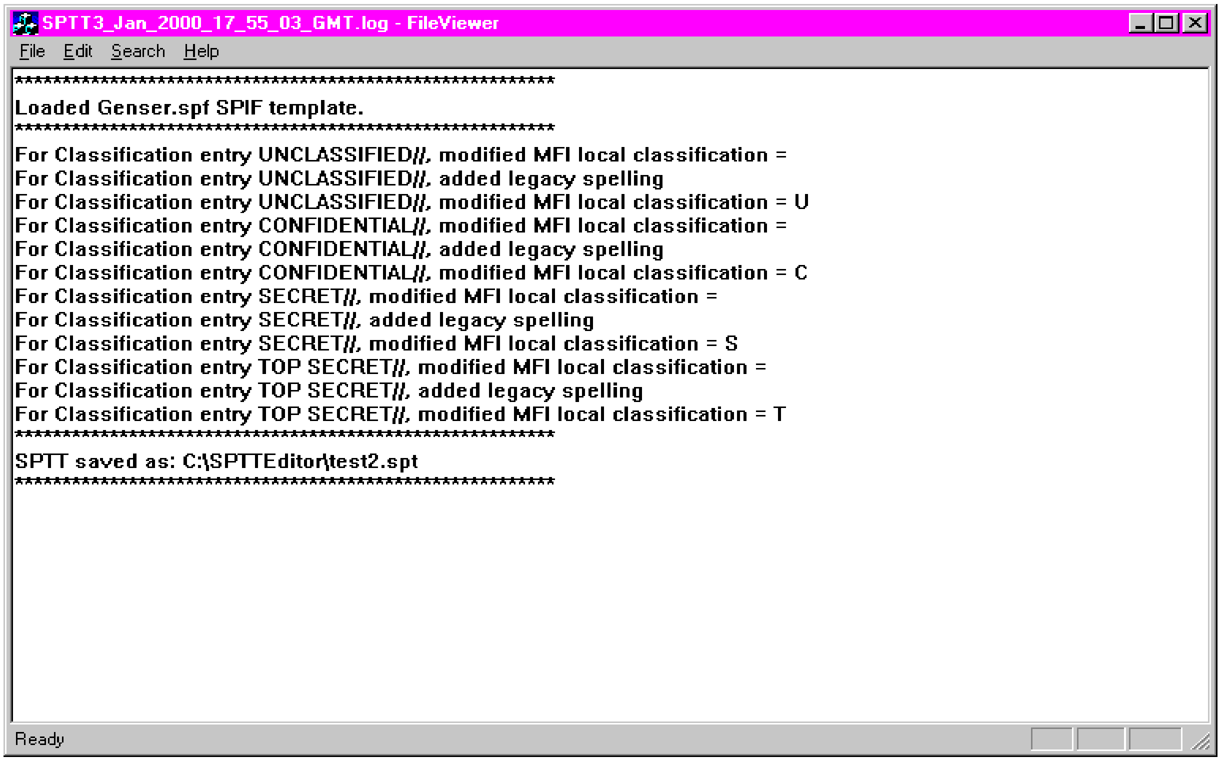
SPTT[day]_[month]_[year]_[hour]_[minutes]_[seconds]_[time zone].log

Thus, the log file:

SPTT3_Jan_2000_17_55_03_GMT.log

would have been created on January 3, 2000, at 17:55:03, Greenwich Mean Time.

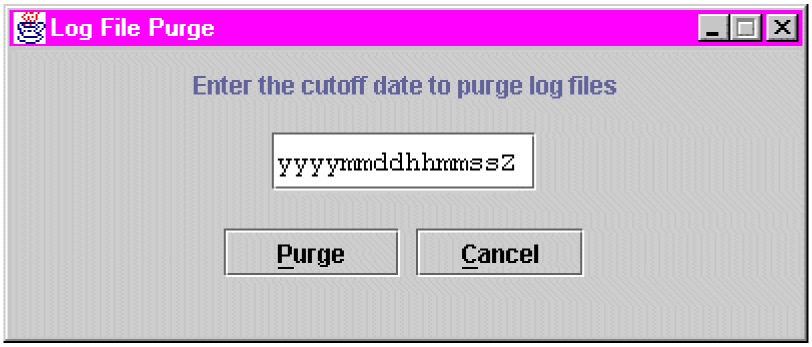
Log files can be accessed by selecting ***View Logs*** from the File menu and then specifying the file name when prompted. The following is an example of a log file (created on the above date and time):



```
**************************************************************
Loaded Genser.spf SPIF template.
**************************************************************
For Classification entry UNCLASSIFIED//, modified MFI local classification =
For Classification entry UNCLASSIFIED//, added legacy spelling
For Classification entry UNCLASSIFIED//, modified MFI local classification = U
For Classification entry CONFIDENTIAL//, modified MFI local classification =
For Classification entry CONFIDENTIAL//, added legacy spelling
For Classification entry CONFIDENTIAL//, modified MFI local classification = C
For Classification entry SECRET//, modified MFI local classification =
For Classification entry SECRET//, added legacy spelling
For Classification entry SECRET//, modified MFI local classification = S
For Classification entry TOP SECRET//, modified MFI local classification =
For Classification entry TOP SECRET//, added legacy spelling
For Classification entry TOP SECRET//, modified MFI local classification = T
**************************************************************
SPTT saved as: C:\SPTTEditor\test2.spt
**************************************************************
```

In this example, a user opened the *Genser.spf* SPIF template, defined classifications, and then saved the SPTT as: *C:\SPTTEditor\test2.spt.*

Log files can be deleted (again, only by the administrator or other users with administrative privileges) by selecting ***Purge Logs*** from the File menu. Upon doing this, the Log File Purge dialog is displayed:

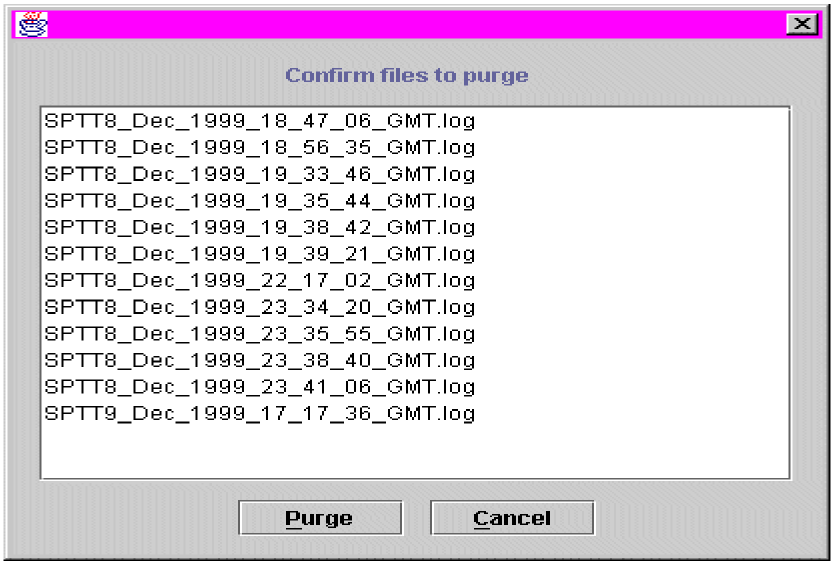


- Enter the cutoff date (to purge log files) in the following format:

  yyyymmddhhmmssZ

  where "yyyy" indicates the year, "mm" indicates the month, "dd" indicates the day, "hh" indicates the hour, "mm" indicates the minute, and "ss" indicates the second. The "Z" is automatically appended to the value and stands for Zulu time.

- Select the **Purge** button. The Confirm Files to Purge dialog is then displayed:



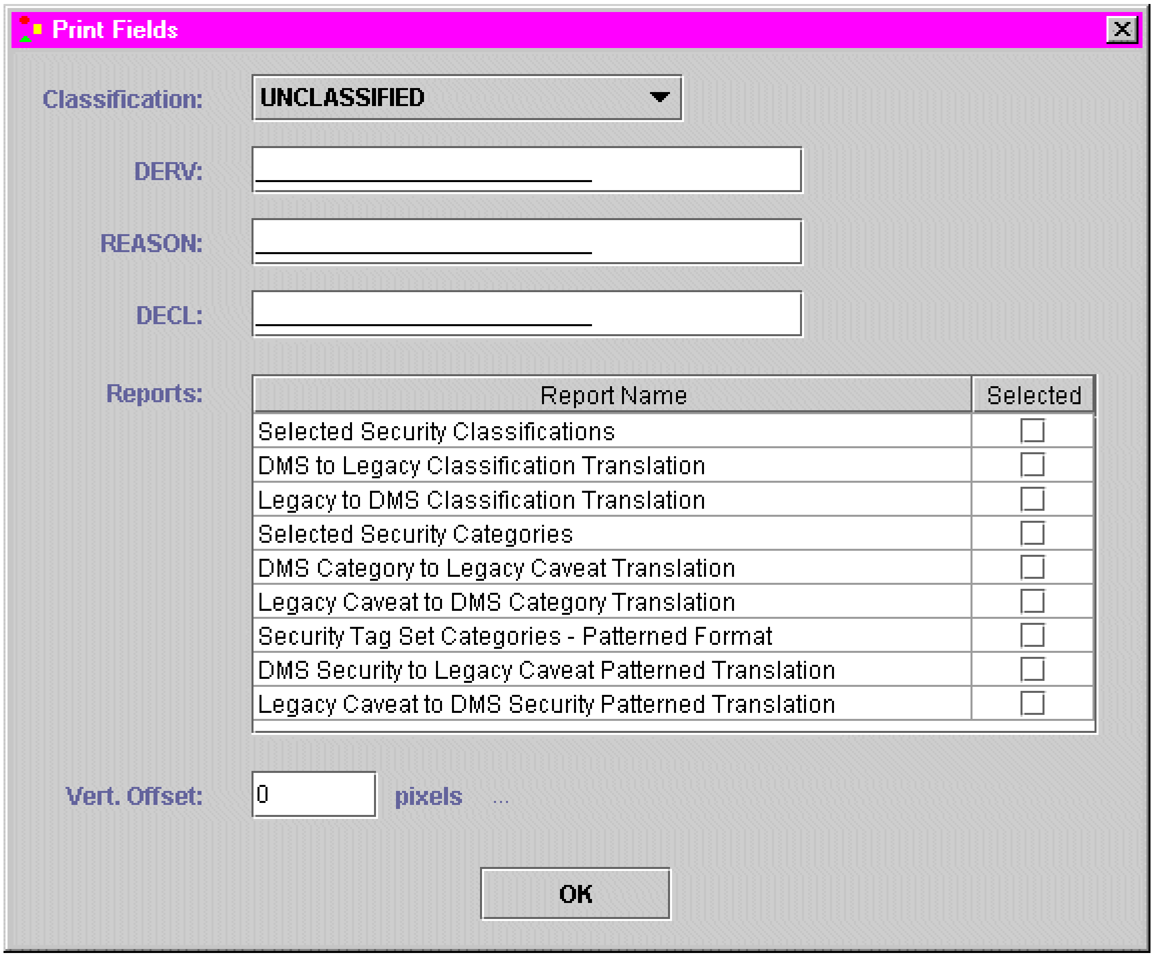
```
SPTT8_Dec_1999_18_47_06_GMT.log
SPTT8_Dec_1999_18_56_35_GMT.log
SPTT8_Dec_1999_19_33_46_GMT.log
SPTT8_Dec_1999_19_35_44_GMT.log
SPTT8_Dec_1999_19_38_42_GMT.log
SPTT8_Dec_1999_19_39_21_GMT.log
SPTT8_Dec_1999_22_17_02_GMT.log
SPTT8_Dec_1999_23_34_20_GMT.log
SPTT8_Dec_1999_23_35_55_GMT.log
SPTT8_Dec_1999_23_38_40_GMT.log
SPTT8_Dec_1999_23_41_06_GMT.log
SPTT9_Dec_1999_17_17_36_GMT.log
```

- Select the **Purge** button to confirm log file deletion. The log files are then deleted, and the dialog is closed.

PRINT SPTT INFORMATION

To print (either to paper or ASCII file) specific information contained in a particular SPTT, open the SPTT (if you haven't already) and perform the following steps:

- Select ***Print*** or ***Report*** from the File menu depending upon the desired operation. The Print Fields dialog is displayed:



Classification: UNCLASSIFIED

DERV: ______________________

REASON: ______________________

DECL: ______________________

Reports:

Report Name	Selected
Selected Security Classifications	□
DMS to Legacy Classification Translation	□
Legacy to DMS Classification Translation	□
Selected Security Categories	□
DMS Category to Legacy Caveat Translation	□
Legacy Caveat to DMS Category Translation	□
Security Tag Set Categories - Patterned Format	□
DMS Security to Legacy Caveat Patterned Translation	□
Legacy Caveat to DMS Security Patterned Translation	□

Vert. Offset: 0 pixels

- Assign attributes to any/all of the following document declassification fields, depending upon the selected report type:

  Classification: This indicates the classification marking for the selected report.

  DERV: This indicates the derivation of the classification for the selected report.

  REASON: This indicates the reason for the classification for the selected report.

  DECL: This indicates declassification instructions for the information contained in the selected report.

- Select the desired report type. Report types include:

  Selected Security Classifications – is used to verify the security classifications authorized in the SPTT and the associated internal MFI classification.

  DMS to Legacy Classification Translation – is used to verify that an appropriate FL12 marking is associated with each possible classification in the security label and that the classification markings on messages sent to the Message Conversion System (MCS) will be properly formatted for that system.

Legacy to DMS Classification Translation – is used to verify that all valid combinations of the FL2/FL4 security character and FL12 classification/marking are properly associated with the applicable classification/privacy mark/default category in the DMS Security Label and that the assigned default "required category" for each DMS security classification in the DMS Security Label is correct.

Selected Security Categories – is used to validate the security categories that have been selected/not selected for translation and, if selected, the allowable direction(s) of the translation.

DMS Category to Legacy Caveat Translation – is used to verify that each selected security category has an associated FL4/FL12 combination and that the legacy messages generated by the MFI and sent to the MCS will have the proper security markings for processing by that system.

Legacy Caveat to DMS Category Translation – is used to verify that all valid combinations of FL4 SHD/FL12 caveats are properly associated with each SPIF security category and that the appropriate default category has been assigned for each security category.

Security Tag Set Categories – Patterned Format – is used to validate the security tag sets/categories that have been selected/not selected for translation and, if selected, the FL12 caveat formats of the enumerated categories and the allowable directions of the translation.

DMS Security to Legacy Caveat Patterned Translation – is used to verify that the legacy messages generated by the MFI and sent to the MCS will have the proper security markings for processing by that system and that the "implied category" for the tag set has been correctly specified.

Legacy Caveat to DMS Security Patterned Translation – is used to verify that all valid combinations of FL SHD/FL12 caveats are properly associated with each security tag set, that the appropriate default category has been assigned for each security tag set, and that the "implied category" of the tag set has been correctly specified.

- Click the **OK** button. The Print Fields dialog is closed and either the Print dialog or the Save dialog is then displayed. If printing, select the desired printer, click the **OK** button, and the report is then printed. Otherwise, if saving to ASCII file, then supply the desired location and name of the ASCII file.

☒ **NOTE:** The Vert. Offset field is provided to enable you to shift the text relative to lines in the report by *X* pixels up (-value) or down (+value).

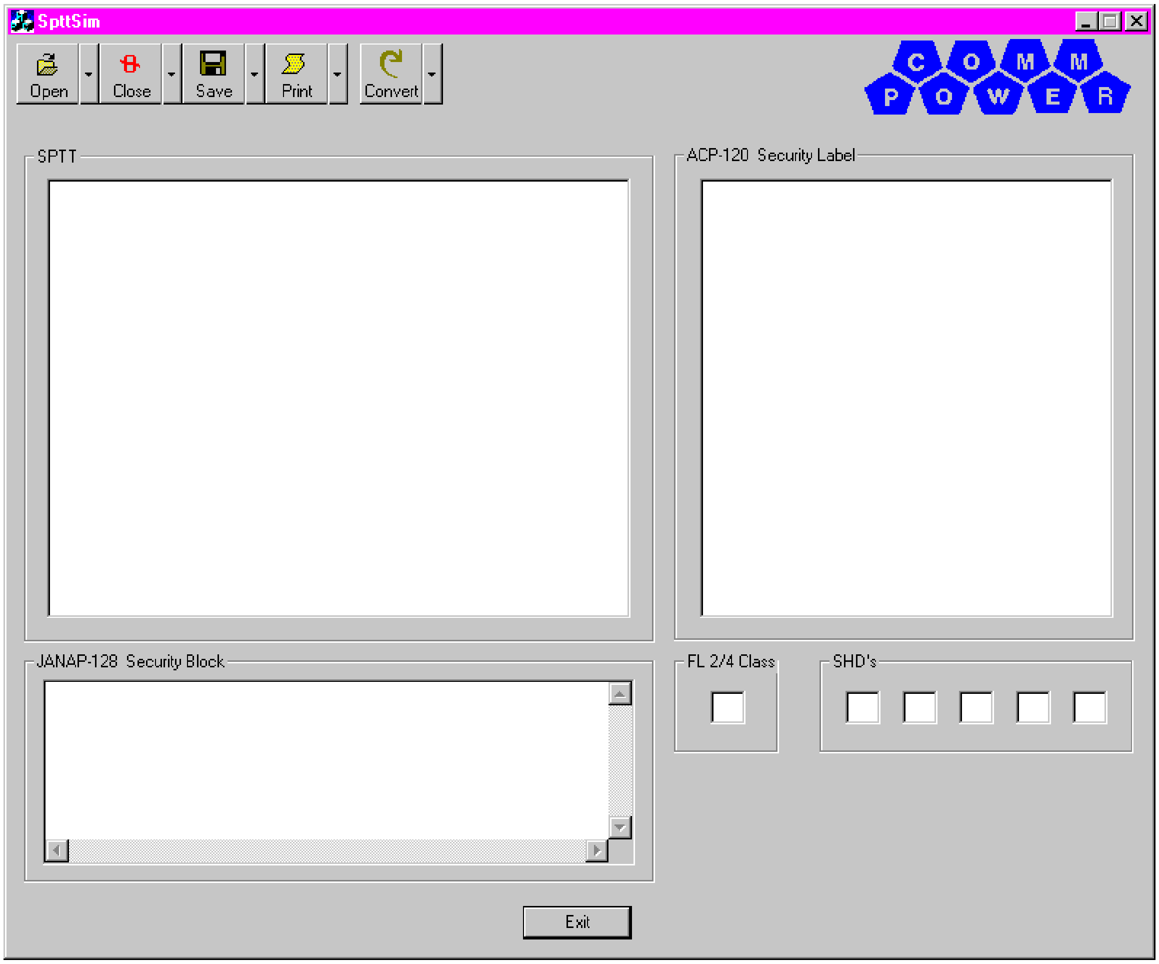
Chapter 5.

SPTT Simulator Operations

This chapter describes how to start up the SPTT Simulator and how to use the SPTT Simulator to validate a new or modified SPTT. It also provides an overview of the SPTT Simulator Main Window (in the startup section).

SPTT SIMULATOR STARTUP

To start up the SPTT Simulator, select ***Start>>SPST-SPTT Toolset>>SPTT Simulator*** from the desktop. Once startup is complete, the SPTT Simulator Main Window is displayed:



SPTT Simulator Main Window Overview

As shown above, the SPTT Simulator Main Window comprises the following features:

- Menu Buttons (across the top)
- Main Display Windows/Work Areas (at the top and bottom)

Menu Buttons

The menu buttons consist of the following:

- Open The **Open** menu button allows you to open a SPTT, an ACP-120 Security Label, or a JANAP-128 Security Block.
- Close The **Close** menu button allows you to close a SPTT, an ACP-120 Security Label, or a JANAP-128 Security Block.
- Save The **Save** menu button allows you to save a SPTT, an ACP-120 Security Label, or a JANAP-128 Security Block.
- Print The **Print** menu button allows you to print a SPTT, an ACP-120 Security Label, or a JANAP-128 Security Block.
- Convert The **Convert** menu button allows you to convert an ACP-120 Security Label (to a JANAP-128 Security Block) or a JANAP-128 Security Block (to an ACP-120 Security Label).

In addition to the above buttons, the **Exit** button is provided to enable you to exit from the SPTT Simulator Main Window.

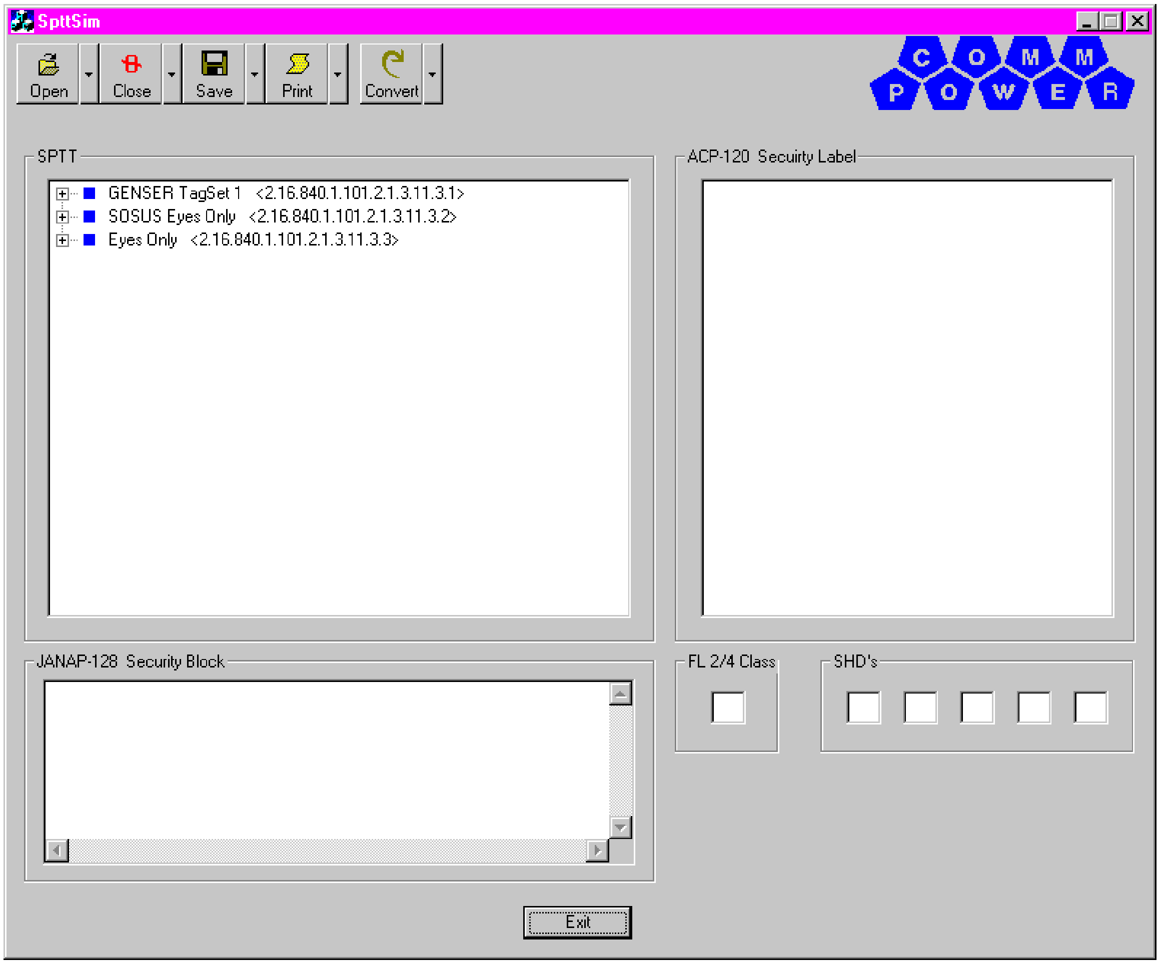
Main Display Windows/Work Areas

The main display windows/work areas consist of three primary panes:

- **SPTT**: This pane (located in the upper left-hand corner) is used for displaying and selecting security categories.
- **ACP-120 Security Label:** This pane (located in the upper right-hand corner) is used for displaying ACP-120 Security Labels.
- **JANAP-128 Security Block:** This pane (located in the lower left-hand corner) is used for displaying Format Line 12a of a legacy message. The fields to its immediate right are used for displaying Format Lines 2/4 and any Special Handling Designators (SHDs) associated with the legacy message.

OPEN SPTT

Upon invoking the SPTT Simulator via the Windows NT Start menu (as described above), select the menu associated with the **Save** button and choose to either open a SPTT, an ACP-120 Label, or a Security Block. If you selected an ACP-120 Label or a Security Block, the information is displayed in the ACP-120 Security Label or the JANAP-128 Security Block panes, respectively. If you selected a SPTT, the information (consisting of a directory tree structure) is displayed in the SPTT pane:

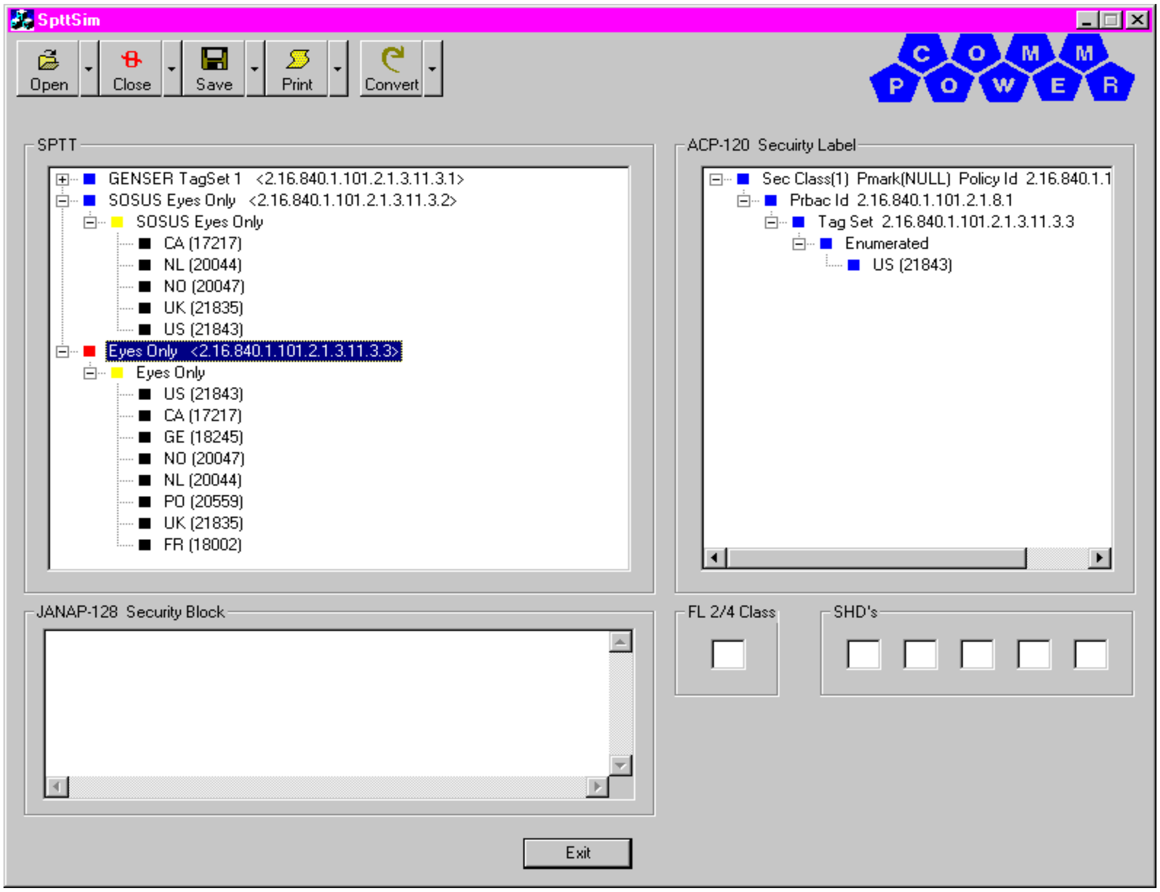


GENSER TagSet 1 <2.16.840.1.101.2.1.3.11.3.1>
SOSUS Eyes Only <2.16.840.1.101.2.1.3.11.3.2>
Eyes Only <2.16.840.1.101.2.1.3.11.3.3>

You are now free to perform the desired security label translations as described below.

ACP-120 to Legacy Translations

- Create your ACP-120 label by dragging SPTT category entries from the SPTT pane into the ACP-120 Security Label pane. Upon doing so, the security label associated with the selected security category is displayed in the ACP-120 Security Label pane:



SPTT

```
⊞ ■ GENSER TagSet 1  <2.16.840.1.101.2.1.3.11.3.1>
⊟ ■ SOSUS Eyes Only  <2.16.840.1.101.2.1.3.11.3.2>
   ⊟ ■ SOSUS Eyes Only
       ■ CA (17217)
       ■ NL (20044)
       ■ NO (20047)
       ■ UK (21835)
       ■ US (21843)
⊟ ■ Eyes Only  <2.16.840.1.101.2.1.3.11.3.3>
   ⊟ ■ Eyes Only
       ■ US (21843)
       ■ CA (17217)
       ■ GE (18245)
       ■ NO (20047)
       ■ NL (20044)
       ■ PO (20559)
       ■ UK (21835)
       ■ FR (18002)
```

ACP-120 Security Label

```
⊟ ■ Sec Class(1) Pmark(NULL) Policy Id 2.16.840.1.1
   ⊟ ■ Prbac Id 2.16.840.1.101.2.1.8.1
      ⊟ ■ Tag Set 2.16.840.1.101.2.1.3.11.3.3
         ⊟ ■ Enumerated
             ■ US (21843)
```

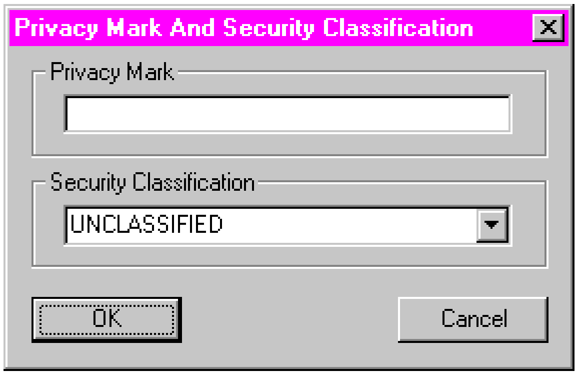
JANAP-128 Security Block

FL 2/4 Class □

SHD's □ □ □ □ □

☒ **NOTE:** During the “drag and drop” process, warnings may appear to inform you of invalid choices. It is up to you whether or not to take action. Also, you may also be prompted to choose additional categories depending upon SPTT required/allowed rules.

- Set the classification/privacy mark of the label. Do this by selecting the first line in the ACP-120 Security Label pane and then right clicking and choosing the Configure Privacy Mark and Classification option. The Privacy Mark and Security Classification dialog is displayed:



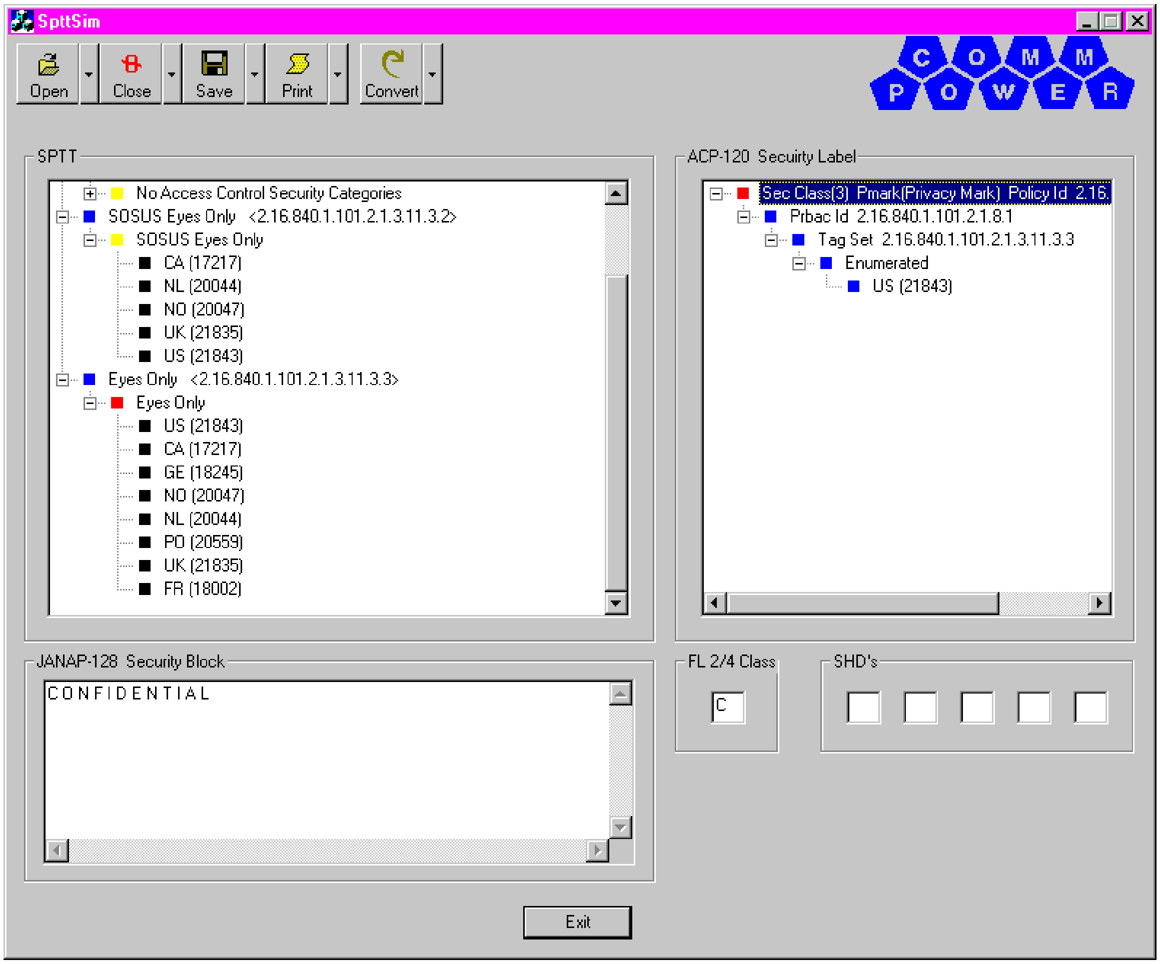
Privacy Mark:

Security Classification: UNCLASSIFIED

Enter the privacy mark (“free form”) in the Privacy Mark field, select the desired classification, and then click the **OK** button.

☒ **NOTE:** Failure to do this step will result in an UNCLASSIFIED label.

- Select ***ACP-120 Label*** from the **Convert** menu button. If the translation is successful, the resulting legacy label is displayed in the JANAP-128 Security Block pane and the associated fields (i.e., FL 2/4 Class and SHD's):



SPTT

```
⊞ 🟨 No Access Control Security Categories
⊟ 🟦 SOSUS Eyes Only  <2.16.840.1.101.2.1.3.11.3.2>
   ⊟ 🟨 SOSUS Eyes Only
        ■ CA (17217)
        ■ NL (20044)
        ■ NO (20047)
        ■ UK (21835)
        ■ US (21843)
⊟ 🟦 Eyes Only  <2.16.840.1.101.2.1.3.11.3.3>
   ⊟ 🟥 Eyes Only
        ■ US (21843)
        ■ CA (17217)
        ■ GE (18245)
        ■ NO (20047)
        ■ NL (20044)
        ■ PO (20559)
        ■ UK (21835)
        ■ FR (18002)
```

ACP-120 Security Label

```
⊟ 🟥 Sec Class(3) Pmark(Privacy Mark) Policy Id 2.16.
   ⊟ 🟦 Prbac Id 2.16.840.1.101.2.1.8.1
      ⊟ 🟦 Tag Set 2.16.840.1.101.2.1.3.11.3.3
         ⊟ 🟦 Enumerated
              🟦 US (21843)
```

JANAP-128 Security Block: CONFIDENTIAL

FL 2/4 Class: C

SHD's: □ □ □ □ □

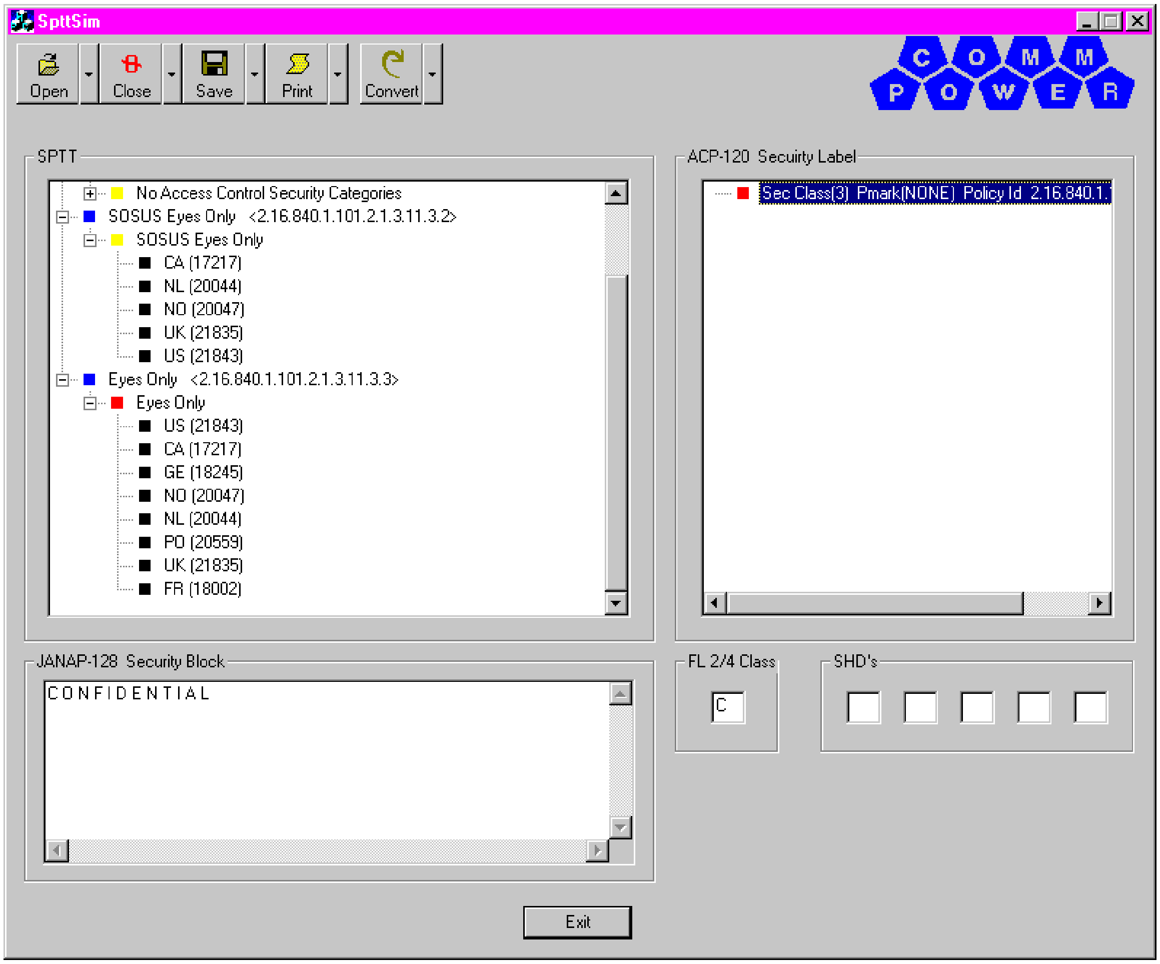
☒ **NOTE:** If you encounter an unexpected failure condition that indicates a problem with the configuration of a particular security category, you will need to access the SPTT via the SPTT Editor, correct the problem, save the SPTT, and then repeat the above steps.

- When finished performing all necessary security translations required to validate the SPTT, select the desired option from the **Save** menu button and then select the **Exit** button to close the SPTT Simulator Main Window.

Legacy to ACP-120 Translations

- Perform the ACP-120 to Legacy Translation defined above in order to get a JANAP security block example. Then, manipulate the JANAP values as desired.

- Select ***Security Block*** from the **Convert** menu button. If the translation is successful, the resulting ACP-120 label is displayed in the ACP-120 Security Label pane:



```
⊞ No Access Control Security Categories
⊟ SOSUS Eyes Only   <2.16.840.1.101.2.1.3.11.3.2>
   ⊟ SOSUS Eyes Only
      CA (17217)
      NL (20044)
      NO (20047)
      UK (21835)
      US (21843)
⊟ Eyes Only   <2.16.840.1.101.2.1.3.11.3.3>
   ⊟ Eyes Only
      US (21843)
      CA (17217)
      GE (18245)
      NO (20047)
      NL (20044)
      PO (20559)
      UK (21835)
      FR (18002)
```

ACP-120 Security Label: Sec Class(3) Pmark(NONE) Policy Id 2.16.840.1.

JANAP-128 Security Block: CONFIDENTIAL

FL 2/4 Class: C

☒ **NOTE:** If you encounter an unexpected failure condition that indicates a problem with the configuration of a particular security category, you will need to access the SPTT via the SPTT Editor, correct the problem, save the SPTT, and then repeat the above steps.

- When finished performing all necessary security translations required to validate the SPTT, select the desired option from the **Save** menu button and then select the **Exit** button to close the SPTT Simulator Main Window.

COMM
POWER

GLOSSARY

This appendix defines the acronyms and special terms that are used in this manual.

AUTODIN: Automatic Digital Network

DISN: Defense Information System Network

DMS: Defense Messaging System

DN: Distinguished Name

FL2: Format Line 2

FL4: Format Line 4

FL12: Format Line 12

Fortezza: Message encryption cards

GMT: Greenwich Mean Time

I/O: Input/Output

JANAP/ACP-128: Joint Army Navy Air Force Procedure. The U.S. Military message format for AUTODIN network communications.

MFG: Multi-Function Gateway

NATO: North Atlantic Treaty Organization

OID: Object Identifier

PCMCIA: Personal Computer Memory Card International Association

SHD: Special Handling Designator

SPIF: Security Policy Information File

SPST: Security Policy Selection Table

SPTT: Security Policy Translation Table

UTC: Universal Coordinated Time

X.400: A standard message handling protocol

COMM
POWER

INDEX

COMM
POWER