IPv6/VSE

FTP
Security Supplement

Current Build

Table of Contents

Preface

About this Publication

This is the **IPv6/VSE SSH Secure Copy Supplement Guide**. The manual will introduce you to the SSH Secure Copy facility and provide information on using the SSH Secure Copy facility.

Trademarks

The following are lists of the trademark and products referenced in this manual. Symbols for trademarks and registered trademarks do not appear in subsequent references.

Barnard Software, Inc.

IPv6/VSE is a registered trademark of Barnard Software, Inc.

International Business Machines Corporation

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.

Copyrights

Contacting Barnard Software, Inc.

Technical Support is available from Barnard Software, Inc. by phone, mail or email:

Barnard Software, Inc.

Phone: 1-407-323-4773

Support: bsiopti@bsiopti.com

Sales: bsisales@bsiopti.com

Support is available from 9:00 a.m. through 5:00 p.m. EST, Monday through Friday.

If a TSR (Technical Support Representative) is not available at the time of your call, please leave a message and a TSR will return your call as soon as possible. Please provide the following information: name, company, phone number, product name, product release level, and a short description of the problem.

BSIUsers Announcement List Server

When new releases of IPv6/VSE are available BSI will post an announcement on its BSIUsers announcement list.

To subscribe to the BSIUsers announcement list send an email to this email address

BSIUsers-subscribe@yahoogroups.com

To unsubscribe to the BSIUsers announcement list send an email to this email address

BSIUsers-unsubscribe@yahoogroups.com

Problem Determination

If you have a problem using a IPv6/VSE application always check the SYSLST output for additional information and messages. Most messages are written to SYSLST and not to the VSE/ESA system console.

When contacting BSI for technical support always have the applications JCL/commands, console and SYSLST output available for problem determination. The SYSLST output is very important.

While a IPv6/VSE application is running, you can issue the **AR CANCEL XX,PARTDUMP** command to terminate IPv6/VSE application and dump the partition to SYSLST. Using the VSE/POWER Flush (F) command cancels the IPv6/VSE application partition without a dump.

If the IPv6/VSE application partition stops responding to its console interface, use the **AR DUMP XX** command to obtain a dump of the partition.

BSTTFTPS FTP Server Security

The BSTTFTPS FTP Server provides 3 types of security.

1. Security based on the BSTTSCTY.T security library member.
2. Security based on the BSTTSCTY.T security library member with userid, password and access checking done by the IBM BSTTISX security exit.
3. Security based on RACROUTE security calls to an external security product. The external security product can be IBM's z/VSE security facility provided in z/VSE 4.1 (and higher) or a 3rd party security facility like CA's TopSecret.

BSTTSCTY.T Security

FTP Server Security is defined in a library member. The BSTTSCTY.T library member should be placed in the same library you have the BSTTPARM.A verification code library member.

The lib.slib used for these members should not be the same as the installation library. This is because each time you upgrade IPv6/VSE sample BSTTSCTY.T and BSTTPARM.A members are cataloged into the installation lib.slib. We recommend that these members be kept in PRD2.CONFIG or your own configuration lib.slib.

The BSTTSCTY.T table can be reloaded while the FTP server is active by using the MSG xx,D=RELOAD command. Comments are within the BSTTSCTY.T member are only supported on a line with an asterisk (*) in column one (1).

FTP security commands are processed from the first rule to the last rule for each type of rule. If access is allowed by an early rule, later rules are not processed. And, if no rule is found to allow access, access will be denied by default.

BSTTSCTY.T Member Encryption

The BSTTSCTY.T member is used by serveral IPv6/VSE applications for various reasons. The Userid's and Password's stored in this member are used by the BSTTFTPS FTP Server for FTP Server access. These Userid's and Password's are also used by BSTTFTPC and BSTTMTPC to optionally validate LUSER/LPASS commands.

IPv6/VSE provides a utility called BSTTSCTC that can be used to optionally encrypt and decrypt the BSTTSCTY.T member. BSTTSCTC reads the BSTTSCTY.T member, detects its current condition and reverses that condition. This means that if the BSTTSCTY.T member is currently clear text, BSTTSCTC will encrypt the member. If the BSTTSCTY.T member is currently encrypted, BSTTSCTC will decrypt the member.

Applications using the BSTTSCTY.T member can detect its current state and process it in either mode (clear text or encrypted).

128-bit AES encryption is used to encrypt/decrypt the BSTTSCTY.T member.

The BSTTSCTY.T member is distributed as a clear text member. If you want this member encrypted we recommend that you keep the member clear text until all your userid/passwords and security rules are in the member and correct. At this point, you can use the BSTTSCTC utility to encrypt the member. Later if you need to add, delete or modify the security rules or userid/passwords, use BSTTSCTC to decrytp the member. Make your changes, verify the changes and use BSTTSCTC to re-encrypt the member.

BSTTSCTC Sample JCL

```
// LIBDEF PHASE,SEARCH=(ipv6lib.slib)
// LIBDEF SOURCE,SEARCH=(lib.slib) (*1)
// EXEC BSTTSCTC,SIZE=BSTTSCTC
/*
```

The BSTTSCTY.T member is accessed using the `// LIBDEF SOURCE,SEARCH` chain. Therefore, this search chain ***must*** specify the *lib.slib* containing the member you wish to process.

BSTTSCTC Sample Output

```
// LIBDEF PHASE,SEARCH=(BSILIB.TTDEV)
// LIBDEF SOURCE,SEARCH=(PRD2.CONFIG)
// EXEC BSTTSCTC,SIZE=BSTTSCTC
1S54I  PHASE BSTTSCTC IS TO BE FETCHED FROM BSILIB.TTDEV
07-Nov-2016 11:07:43 0034 BSTT000I INITIATED  BSTTSCTC Build257 11/07/16 10.42
07-Nov-2016 11:07:43 0034 BSTT003I COPYRIGHT (C) 1998-2016 BARNARD SOFTWARE
07-Nov-2016 11:07:43 0034 BSTT014I BSTTAESI LOADED A=0052AE00 L=000058E8
07-Nov-2016 11:07:43 0034 BSTT004I CB=BUFF A=00531000 L=00028000
07-Nov-2016 11:07:43 0034 BSTT714I BSTTSCTY.T        OPENED
07-Nov-2016 11:07:43 0034 BSTT010I BSTTSCRTY.T IS CLEAR TEXT
07-Nov-2016 11:07:43 0034 BSTT010I ENCRYPTION INVOKED
07-Nov-2016 11:07:43 0034 BSTT001I TERMINATED BSTTSCTC
1S55I  LAST RETURN CODE WAS 0000

// LIBDEF PHASE,SEARCH=(BSILIB.TTDEV)
// LIBDEF SOURCE,SEARCH=(PRD2.CONFIG)
// EXEC BSTTSCTC,SIZE=BSTTSCTC
1S54I  PHASE BSTTSCTC IS TO BE FETCHED FROM BSILIB.TTDEV
07-Nov-2016 11:12:50 0034 BSTT000I INITIATED  BSTTSCTC Build257 11/07/16 11.11
07-Nov-2016 11:12:50 0034 BSTT003I COPYRIGHT (C) 1998-2016 BARNARD SOFTWARE,
07-Nov-2016 11:12:50 0034 BSTT014I BSTTAESI LOADED A=0052AE00 L=000058E8
07-Nov-2016 11:12:50 0034 BSTT004I CB=BUFF A=00531000 L=00028000
07-Nov-2016 11:12:50 0034 BSTT714I BSTTSCTY.T        OPENED
07-Nov-2016 11:12:50 0034 BSTT010I BSTTSCTY.T        ENCRYPTED
07-Nov-2016 11:12:50 0034 BSTT010I DECRYPTION INVOKED
07-Nov-2016 11:12:50 0034 BSTT001I TERMINATED BSTTSCTC
1S55I  LAST RETURN CODE WAS 0000
```

BSTTSCTY.T Rules

FTP server security is defined in the BSTTSCTY.T library member. This library member contains FTP server security commands.

(a) FTP-LUSER is used to require the LUSER and LPASS commands

```
FTP-LUSER REQUIRED
FTP-LUSER OPTIONAL
```

OPTIONAL is the default if this command is omitted.

FTP-LUSER REQUIRED indicates that the BSTTFTPC (batch FTP) and BSTTMTPC (batch Email) application must have LUSER/LPASS commands proceeding the OPEN command. This command has nothing to do with FTP server security. The FTP server always requires a valid userid and password to login. If you specify FTP-LUSER REQUIRED and do not have LUSER/LPASS commands in your BSTTFTPC/BSTTMTPC job stream you will get a 'BSTT013E ACCESS ERROR R15=00000040' message and the job will fail.

(b) FTP-IP/FTP-IP6 are used to allow or deny access by IP addresses

```
FTP-IP  ALLOW SUBNET-ADDRESS SUBNET-MASK
FTP-IP  DENY  SUBNET-ADDRESS SUBNET-MASK
FTP-IP6 ALLOW SUBNET-ADDRESS SUBNET-MASK
FTP-IP6 DENY  SUBNET-ADDRESS SUBNET-MASK
```

FTP-IP commands are ignored by a BSTTFTPS partition using the IPv6/VSE IPv6 TCP/IP stack (BSTT6NET). FTP-IP6 command are ignored by a BSTTFTPS partition using the IPv6/VSE IPv4 TCP/IP stack.

(c) FTP-USER is used to define a userid and password

```
FTP-USER USERID PASSWORD <initial-directory-string>

Note: USERIDs and PASSWORDs are limited to 8 characters.
The initial-directory-string is used to specify an initial
directory for the userid. The format of the string is the same
as used in a CWD command to mount a file system and set the
directory.

FTP-USER userid password SMNT-POWER
FTP-USER userid password SMNT-LIBRARY-PRD2/CONFIG
FTP-USER userid password SMNT-VSAM-VSESP.USER.CATALOG
```

(d) FTP-ACCESS is used to define access rights

```
FTP-ACCESS ALLOW USERID POWER QUEUE CLASSES PREFIX READ|WRITE
FTP-ACCESS DENY  USERID POWER QUEUE CLASSES PREFIX READ|WRITE
FTP-ACCESS ALLOW USERID LIBRARY LIB SLIB MEMBER TYPE READ|WRITE
FTP-ACCESS DENY  USERID LIBRARY LIB SLIB MEMBER TYPE READ|WRITE
FTP-ACCESS ALLOW USERID VSAM CATALOG DATASET READ|WRITE
FTP-ACCESS DENY  USERID VSAM CATALOG DATASET READ|WRITE
FTP-ACCESS ALLOW USERID SAM FILE.NAME READ|WRITE
FTP-ACCESS DENY  USERID SAM FILE.NAME READ|WRITE
FTP-ACCESS ALLOW USERID DLBL dlbl READ|WRITE
FTP-ACCESS DENY  USERID DLBL dlbl READ|WRITE
```

```
Note: Unless READ is specified, WRITE is assumed. WRITE is the
default. This is required for compatibility with earlier
releases of the FTP server.
```

Security definition lines in the BSTTSCTY.T library member can be continued. An X in column 72 indicates continuation. Only one continuation line is supported. When continuation is used the 2 80 character lines are placed together in storage and the continuation character X is replaced by a blank before processing the security command.

Default BSTTSCTY.T Member

```
*
* FTP-IP ALLOW SUBNET-ADDRESS SUBNET-MASK

* FTP-IP DENY SUBNET-ADDRESS SUBNET-MASK

*
FTP-IP ALLOW 0.0.0.0 0.0.0.0
*
* FTP-USER USERID PASSWORD
*
FTP-USER *   *
*
*  FTP-ACCESS ALLOW USERID POWER QUEUE CLASSES PREFIX
*  FTP-ACCESS DENY  USERID POWER QUEUE CLASSES PREFIX
*  FTP-ACCESS ALLOW USERID LIBRARY LIB SLIB MEMBER TYPE
*  FTP-ACCESS DENY  USERID LIBRARY LIB SLIB MEMBER TYPE
*  FTP-ACCESS ALLOW USERID VSAM CATALOG DATASET
*  FTP-ACCESS DENY  USERID VSAM CATALOG DATASET
*  FTP-ACCESS ALLOW USERID SAM FILE.NAME
*  FTP-ACCESS DENY  USERID SAM FILE.NAME
*  FTP-ACCESS ALLOW USERID DLBL DLBL
*  FTP-ACCESS DENY  USERID DLBL DLBL
*
FTP-ACCESS ALLOW * * * * * *
```

The FTP-IP command defines IP/SUBNET address allowed to access the FTP server. IP addresses are specified in standard dotted decimal notation. The default FTP-IP command accepts connections from any IP address.

The FTP-USER command defines a userid and password. Either or both of these values may be specified as an asterisk (*). The asterisk indicates any value is valid. Specify an asterisk for the userid and any value with be accepted. Specify an asterisk for the password and any value will be accepted. The default FTP-USER command accepts any userid with any password.

The FTP-ACCESS command defines access rules. Access may be allowed or denied to any file system (VSE/POWER, LIBRARY or VSAM). Within each file system other access restrictions are permitted.

The FTP-ACCESS command allows you to restrict access to the VSE/POWER file system based on queue, member prefix and class. Valid queues are RDR, LST, PUN, XMT and CMD. The CMD queue is used to validate VSE/POWER commands sent from an FTP client via the SITE PWRCMD facility. When using the CMD queue you can specify the VSE/POWER command to ALLOW or DENY in the member prefix field.

The FTP-ACCESS command allows you to restrict access to the LIBRARY file system based on library, sublibrary, member name and member type.

The FTP-ACCESS command allows you to restrict access to the VSAM file system based on catalog name and dataset (cluster) name.

Using the IBM BSSTISX Security Phase

IBM provides a security exit routine called BSSTISX. The IPv6/VSE BSTTFTPS FTP Server security exit routine BSTTFTS1.PHASE calls the IBM security exit to verify security. The BSTTSCTY.T member is still used but only for FTP-IP/FTP-IP6 IP address checking. All FTP-USER and FTP-ACCESS commands in the member are ignored.

The IBM provided TCP/IP Security Exit BSSTISX allows you to control TCP/IP based access (e.g. via FTP) using RACROUTE calls to the currently active Security Manager. This can be the IBM provided Basic Security Manager (BSM) or an External Security Manager (ESM).

To enable the BSTTFTS1.PHASE security exit

1) Copy the BSTTFTS1.PHASE to a configuration lib.slib as BSTTFTSX.PHASE
2) LIBDEF the configuration lib.slib first in the BSTTFTPS PHASE,SEARCH chain
3) Add the following BSSTISX command to your BSTTFTPS startup commands

```
BSSTISX [anonym_uid][,[anonym_pwd][,[preproc][,[postproc][,[mode]]]]]
```

The BSSTISX command tells BSTTFTPS to use the IBM BSSTISX routine and to initialize for its usage.

anonym_uid

Here you can specify a user ID, which is defined to BSM. Each time a client logs on with user ID ANONYMOUS your specified user ID and its access rights will be used.

anonym_pwd

With this parameter you can specify the password of the BSM defined user ID for user

ANONYMOUS.

preproc

If you like to use a self-written preprocessing exit, specify here the name of your preprocessing exit phase.

postproc

For a self-written post-processing exit you have to specify here the name of your post-processing exit phase.

mode

The mode parameter can be used to change the processing options of the BSSTISX exit.Therefore, you have to specify the sum of the selected option codes. By default, all supported checks are active. The mode values are bits and can be added together to specify multiple modes.

1 No administrator check for files & libs
2 No administrator check for POWER spool file.
4 No RACROUTE calls for files and libraries
8 No POWER user-id validations
16 ICCF READ requests are not rejected

Sample Library Copy JCL

In this example, PRD2.CONFIG is being used as the configuration lib.slib. After the LIBR COPY is complete change the BSTTFTPS JCL to LIBDEF the PRD2.CONFIG lib.slib before the BSI IPv6/VSE lib.slib in the PHASE,SEARCH chain.

```
// EXEC LIBR,SIZE=256K
CON S=lib.slib:PRD2.CONFIG
COPY BSTTFTS1.PHASE:BSTTFTSX.PHASE REP=YES
/*
```

RACROUTE Security

The IPv6/VSE BSTTFTPS FTP Server security exit routine BSTTFTS2.PHASE issues RACROUTE macro calls to access an external security server product.

To use the BSTTFTS2.PHASE security routine ...

1. Copy the BSTTFTS2.PHASE to a configuration lib.slib as BSTTFTSX.PHASE
2. LIBDEF the configuration lib.slib first in the BSTTFTPS PHASE,SEARCH chain

Sample Library Copy JCL

In this example, PRD2.CONFIG is being used as the configuration lib.slib. After the LIBR COPY is complete change the BSTTFTPS JCL to LIBDEF the PRD2.CONFIG lib.slib before the BSI IPv6/VSE lib.slib in the PHASE,SEARCH chain.

```
// EXEC LIBR,SIZE=256K
CON S=lib.slib:PRD2.CONFIG
COPY BSTTFTS2.PHASE:BSTTFTSX.PHASE REP=YES
/*
```

BSM Resources

The BSTTFTPS RACROUTE security routine uses the IBM BSM FACILITY feature. The BSTTSCTY.T member is still used but only for FTP-IP/FTP-IP6 IP address checking. All FTP-USER and FTP-ACCESS commands in the member are ignored.

When using the BSTTFTS2.PHASE RACROUTE security phase without defined any resources no one will be able to logon to the FTP server. The logon process is a 2-step process. 1st, you create an environment with a specified userid and password. 2nd, you check to see if the valid userid has access to the BSTTFTPS FACILITY. Either of these steps can fail resulting in a logon failure.

Once the FACILITY BSTTFTPS is defined and users authorized but no other resources are defined then userid and passwords are checked but all other access is allowed. If the resource name is not defined to the BSM it is assumed that access is allowed.

Be aware that authorizing a user to use BSTTFTPS FTP server to access a resource does not guarantee the resource can be accessed if another level of security is present. For example, you may define rules allow a user to access the VSE/Power LST queue. However, VSE/Power itself may limit access due to its own security rules. If the user attempts to delete a LST queue entry they do not own, VSE/Power may deny the delete request.

For additional information about RACROUTE Security, see the RACROUTE Security chapter in the z/VSE Administration manual and chapter that has the description for the BSTADMIN utility.

Class	Name	Description
FACILITY	BSTTFTPS	BSTTFTPS FTP Server
FACILITY	BSTTFTPS.POWER.queue.class.name	BSTTFTPS Power Access
FACILITY	BSTTFTPS.VSAM.catalog.cluster	BSTTFTPS VSAM Access
FACILITY	BSTTFTPS.SAM.dataset	BSTTFTPS SAM Access
FACILITY	BSTTFTPS.LIBRARY.lib.slib.member.type	BSTTFTPS Library Access
FACILITY	BSTTFTPS.DLBL.name	BSTTFTPS DLBL access
FACILITY	BSTTFTPS.NULL	BSTTFTPS NULL FileSystem
FACILITY	BSTTFTPS.BSTTBEAM	BSTTFTPS BSTTBEAM

Note: The `BSTTFTPS.NULL` resource is used to control access to the NULL (empty) FileSystem. The `BSTTFTPS.DLBL.NULL` resource is used to control access to the NULL file. The NULL FileSystem can be used when you do not want any other FileSystems mounted when an FTP Client connects to the FTP Server.

Basic BSTTFTPS IBM BSM Setup

```
// EXEC BSTADMIN,SIZE=BSTADMIN
 ADD FACILITY BSTTFTPS               UACC(READ) DATA('FTP SERVER')
 ADD FACILITY BSTTFTPS.POWER    GEN UACC(NONE) DATA('FTP POWER')
 ADD FACILITY BSTTFTPS.VSAM     GEN UACC(NONE) DATA('FTP VSAM')
 ADD FACILITY BSTTFTPS.SAM      GEN UACC(NONE) DATA('FTP SAM')
 ADD FACILITY BSTTFTPS.LIBRARY  GEN UACC(NONE) DATA('FTP LIBRARY')
 ADD FACILITY BSTTFTPS.DLBL     GEN UACC(NONE) DATA('FTP DLBL')
 ADD FACILITY BSTTFTPS.NULL     GEN UACC(NONE) DATA('FTP NULL')
 ADD FACILITY BSTTFTPS.BSTTBEAM GEN UACC(NONE) DATA('FTP BSTTBEAM')
/*
```

After executing the above job the FACILITY resources used by the BSTTFTPS RACROUTE exit are defined. However, no users have been allowed access and all resource access is denied by default.

The UACC(NONE) shown here specifies Universal ACCess is NONE. So, by default, no access is permitted. This may or may not be desired. Specifying UACC(READ) or UACC(UPDATE) may provide a better default for these GENeric rules.

Allowing Users to Logon to BSTTFTPS

To allow a *userid* to logon to the BSTTFTPS FTP server, use the following example.

```
// EXEC BSTADMIN,SIZE=BSTADMIN
 AG FTPSUSER DATA('USERS OF BSTTFTPS')
 CO FTPSUSER userid
 PE FACILITY BSTTFTPS ID(FTPSUSER) ACC(READ))
/*
```

At this point, the *userid* specified in the above example will be allowed to logon to the BSTTFTPS FTP server. However, the *userid* will not be able to access any resources.

Allowing Users Access to BSTTFTPS Resources

For example, to allow a userid to access the VSE/POWER LST queue you would define a new generic resource called BSTTFTPS.POWER.LST, add a new group, connect a user with the new group and finally allow the group access to the facility defined.

```
// EXEC BSTADMIN,SIZE=BSTADMIN
 ADD FACILITY BSTTFTPS.POWER.LST GEN UACC(UPDATE) DATA('POWER LST')
 AG PLSTUSER DATA('USERS OF POWER LST')
 CO PLSTUSER userid
 PE FACILITY BSTTFTPS.POWER.LST ID(PLSTUSER) ACC(UPDATE))
/*
```

To allow a userid to access to a VSAM catalog you would define a new generic resource called BSTTFTPS.VSAM.catalog, add a new group, connect a user with the new group and finally allow the group access to the facility defined.

```
// EXEC BSTADMIN,SIZE=BSTADMIN
 ADD FACILITY BSTTFTPS.VSAM.VSESP.USER.CATALOG GEN UACC(UPDATE)
DATA('VSAM VSESPUC')
 AG SPUCUSER DATA('USERS OF VSESPUC')
 CO SPUCUSER userid
 PE FACILITY BSTTFTPS.VSAM.VSESP.USER.CATALOG ID(SPUCUSER) ACC(UPDATE))
/*
```

Secure Password Facility

The BSTTFTPC batch FTP client requires a USER and PASS command to be specified in the command sequence. These commands contain the userid and password to be used to login to the specified FTP Server.

If password security is important to your organization, you may want to consider using the BSTTPASS utility to create a secure encrypted password member for use by BSTTFTPC and BSTTMTPC (the Batch Email Client).

Passwords stored by the Encrypted Password Facility are associated with userid's. If you have the same userid on multiple systems with different passwords then the current encrypted password support will not work for this userid. We recommend using unique userids for each system for better security.

The BSTTPASS utility uses a library member called BSTTPASS.STORE that is accessed via the 1st lib.slib in the LIBDEF SOURCE,SEARCH chain. The first time the BSTTPASS utility is used the BSTTPASS.STORE member is created with 256 empty password entries. Thereafter, the existing member is accessed and updated.

The BSTTPASS.STORE is stored in an encrypted format using 128-bit AES encryption.

BSTTFTPC AUTO Command

When the BSTTPASS.STORE encrypted password store is in use the PASS command is replaced with an AUTO command in the BSTTFTPC command stream. When BSTTFTPC processes the AUTO command the BSTTPASS.STORE member is accessed to provide the required password.

```
BSTTFTPC JCL using USER/PASS commands ...

// EXEC BSTTFTPC,SIZE=BSTTFTPC
ID ..
OPEN ..
*
USER userid
PASS password
...

BSTTFTPC JCL using USER/AUTO commands ...

// EXEC BSTTFTPC,SIZE=BSTTFTPC
ID ..
OPEN ..
*
USER userid
AUTO
...
```

BSTTMTPC AUTH LOGIN Command

When the BSTTPASS.STORE encrypted password store is in use the password specified in the BSTTMTPC AUTH LOGIN command can be omitted. When the password is omitted BSTTMTPC will access the BSTTPASS.STORE to supply the required password.

```
BSTTMTPC JCL using a password in the AUTH LOGIN command ...

// EXEC BSTTMTPC,SIZE=BSTTMTPC
ID ..
OPEN ...
EHLO domain.name
AUTH LOGIN userid password
...

BSTTMTPC JCL using no password in the AUTH LOGIN command ...

// EXEC BSTTMTPC,SIZE=BSTTMTPC
ID ..
OPEN ...
EHLO domain.name
AUTH LOGIN bsi1957
...
```

BSTTREXC AUTO Command

When the BSTTPASS.STORE encrypted password store is in use the PASS command is replaced with an AUTO command in the BSTTREXC command stream. When BSTTREXC processes the AUTO command the BSTTPASS.STORE member is accessed to provide the required password.

BSTTREXC JCL using USER/PASS commands ...

```
// EXEC BSTTREXC,SIZE=BSTTREXC
ID ..
OPEN ..
*
USER userid
PASS password
...
```

BSTTREXC JCL using USER/AUTO commands ...

```
// EXEC BSTTREXC,SIZE=BSTTREXC
ID ..
OPEN ..
*
USER userid
AUTO
...
```

BSTTPASS Utility

The Encrypted Password Repository (Member) is managed by the BSTTPASS application. The BSTTPASS application accesses the library member BSTTPASS.STORE via the 1st lib.slib in the LIBDEF SOURCE,SEARCH chain. BSTTPASS then reads commands (ADD, DEL, REP, PRT) from SYSIPT to add, delete, replace or print the password in the Encrypted Password Member. This member can contain up to 256 passwords.

Using BSTTPASS

The BSTTPASS application is used to mange the Encrypted Password Repository located in the library member BSTTPASS.STORE. Commands are read from SYSIPT for processing. The commands are ADD, DEL, REP and PRT. The name of the Userid of the Password (16 characters) follows the command. The ADD and REP commands also have 2 additional data cards. The first additional card contains the userid beginning in column 1 and the second card is the PASS command in the BSTTFTPC format.

Any card read with an asterisk in column 1 is a comment and is ignored by the BSTTPASS application. Comments are not permitted anywhere else in the member.

All commands are fixed format. The command must begin in column 1 and contain only a single space between parameters.

The REP command is effectively the same as a DEL command followed by and ADD command.

The ADD command adds a new Userid and Password but does not check to see if the userid currently exists. We recommend using the REP command instead of ADD.

The PRT command specifies the userid of the password entry you want to print or an asterisk (*) can be used to specify all userid and password entries.

Sample JCL

```
// LIBDEF PHASE,SEARCH=(ipv6lib.slib)
// LIBDEF SOURCE,SEARCH=(lib.slib)
// EXEC BSTTPASS,SIZE=BSTTPASS
*
*  ADD a new userid/password
ADD user1
user1
PASS pass1
*
* DEL a userid/password
DEL user2
*
* REP a userid/password
REP user3
user3
PASS pass3
*
* Print the password Repository
PRT *
/*
```

Sample Output

```
// LIBDEF PHASE,SEARCH=(BSILIB.TTDEV)
// LIBDEF SOURCE,SEARCH=(PRD2.CONFIG)
// EXEC BSTTPASS,SIZE=BSTTPASS
08-Nov-2016 11:02:54 0038 BSTT000I INITIATED  BSTTPASS Build257 11/04/16 13.57
08-Nov-2016 11:02:55 0038 BSTT003I COPYRIGHT (C) 1998-2016 BARNARD SOFTWARE
08-Nov-2016 11:02:55 0038 BSTT014I BSTTAESI LOADED A=0052B600 L=000058E8
08-Nov-2016 11:02:55 0038 BSTT004I CB=BUFF A=00531000 L=0000A000
08-Nov-2016 11:02:55 0038 BSTT714I BSTTPASS.STORE    CREATED
08-Nov-2016 11:02:55 0038 BSTT715I CMD=ADD  KEY=user1
08-Nov-2016 11:02:55 0038 BSTT715I CMD=DEL  KEY=user1
08-Nov-2016 11:02:55 0038 BSTT715I CMD=REP  KEY=user1
08-Nov-2016 11:02:55 0038 BSTT715I CMD=REP  KEY=user2
08-Nov-2016 11:02:55 0038 BSTT715I CMD=REP  KEY=user3
08-Nov-2016 11:02:55 0038 BSTT715I CMD=PRT  KEY=*

08-Nov-2016 11:02:55 0038 BSTT010I user1
08-Nov-2016 11:02:55 0038 BSTT010I PASS pass1
08-Nov-2016 11:02:55 0038 BSTT010I user2
08-Nov-2016 11:02:55 0038 BSTT010I PASS pass2
08-Nov-2016 11:02:55 0038 BSTT010I user3
08-Nov-2016 11:02:55 0038 BSTT010I PASS pass3

08-Nov-2016 11:02:55 0038 BSTT001I TERMINATED BSTTPASS
```