THE BOEING COMPANY

CAGE CODE 81205

THIS DOCUMENT IS:

CONTROLLED BY: BOEING COMMERCIAL   AIRPLANE GROUP ALL REVISIONS TO THIS DOCUMENT SHALL BE APPROVED BY THE ABOVE ORGANIZATION PRIOR TO RELEASE

PREPARED UNDER ¨   CONTRACT NO.
¨   R&D
x   OTHER

PREPARED ON   PC/WORD FOR WINDOWS 2000
FONT: TIMES NEW ROMAN
FILE: VSS:
TDI/DOCUMENTS/CM_SNET_TDI_UserGuide.doc

DOCUMENT NO.   D6-81764   MODEL   N/A

TITLE   **SUPPLIER NETWORK - TECHNICAL DATA INTERCHANGE USERS MANUAL**

x   THE INFORMATION CONTAINED HEREIN IS NOT PROPRIETARY.

¨   THE INFORMATION CONTAINED HEREIN IS PROPRIETARY TO THE BOEING COMPANY AND SHALL NOT BE REPRODUCED OR DISCLOSED IN WHOLE OR IN PART OR USED FOR ANY DESIGN OR MANUFACTURE EXCEPT WHEN SUCH USER POSSESSES DIRECT.

ANY ADDITIONAL LIMITATIONS IMPOSED ON THIS DOCUMENT
WILL BE FOUND ON A SEPARATE PAGE.

PREPARED BY: _____ 6-7J14   _____
                         SIGNATURE   ORGN   DATE
Bev Glasser
BCAG IS e-Business Supplier Network Systems Analyst

APPROVED BY: _____ 6-7J14   _____
                         SIGNATURE   ORGN   DATE
Jeff R Wilson
BCAG e-Business Supplier Network Systems Manager

REVIEW / CONCURRENCE BY:

_____ 6-7J14 _____
SIGNATURE ORGN DATE

Anna Brannan
BCAG IS e-Business Supplier Network Systems Analyst

_____ 6-7J14 _____
SIGNATURE ORGN DATE

Patti F. Harrop
BCAG IS e-Business Supplier Network Systems Analyst

_____ 6-7J14 _____
SIGNATURE ORGN DATE

Jon Schunke
BCAG IS e-Business Supplier Network Systems Analyst

_____ 6-7J14 _____
SIGNATURE ORGN DATE

Bill Walsh
BCAG IS e-Business Supplier Network Systems Analyst

_____ 6-7J14 _____
SIGNATURE ORGN DATE

Steve Perry
BCAG IS e-Business Supplier Network Business Systems Analyst

SIGNATURE ORGN DATE

REVISIONS			
Rev Number	DESCRIPTION	DATE	APPROVAL
Original	Original version	1996	96
VSS: V13	Major document changes	06/2000	VSS: version 13
VSS: V27	Versions not officially released Added data type C30 to Section 5.3 Data Type Examples. • updated Appendix A SNETPC and Direct Delivery (formerly Special handling) processes due to the TDI Rel 15 blkpt (Sept 6, 2002) • updated phone numbers, mailstops, etc as a result of building move • general document clean up and maintenance • Added Direct Delivery internal interfaces	12/18/2002	VSS version 27
VSS: V18	Updated appendix sections dealing with DDI/DDO interface	1/12/04	S. Perry
VSS: V30	Replaced Steve Nolan with Jeff Wilson Took out Dennis Garrett Reformatted verbage on DDO and DDI in Appendix A	2/4/04	Bev
VSS: V45	Updated Appendix A by adding more interfaces	Feb 2005	Bev

This manual defines the Boeing Commercial Airplane Group (BCAG) Supplier Network, Technical Data Interchange:

- Computing architecture for external communications
- Setup and functionality for end-to-end data exchange
- BCAG standards for the architectural elements, transport services and application services.

This manual is intended for use by trading and design partners as a guide in establishing an electronic communication path to participate in electronic exchange of technical and administrative data with BOEING.

KEY WORDS

Cost Effective

Electronic Communications

Encryption

FTP

Outside Entities

Private Key

Production Support

Public Internet

Public Key

Reliability

Secret Key

Security

ACRONYMS

TERM	DEFINITION
ASCII	American Standard Code For Information Interchange
BCAG	Boeing Commercial Airplane Group
CAD	Computer-aided design
CAM	Computer-aided manufacture
CATIA	Computer-graphics Aided three-dimensional Interactive Application
DCAC	Define Control And Configure
DDE	Digital Data Exchange; presently called TDI
DDD	Digital Data Distribution
DDR	Digital Data Request
DPD	Digital Product Data

DTU   Data Transfer Utility

EDI   Electronic Data Interchange

EBCDIC   Extended Binary Coded Decimal Interchange Code

E-Mail   Electronic Mail

IGES   International Graphics Exchange Standard

INTERNET   A group of networks based on TCP/IP and CSMA/CD

ISDN   Integrated Services Digital Network

LAN   Local Area Network

MOM   Message Oriented MiddleWare

PDM   Produce Data Management, part of DCAC

PGP   Pretty Good Privacy encryption package

SNET   Supplier Network

SNETPC   Boeing SNET TDI interface software for PCs

TDI   Technical Data Interchange

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to present a technical look at the Boeing Commercial Airplane Group (BCAG), Materiel Division's, Supplier Network (SNET) Project - Technical Data Interchange (TDI).

It is intended for use by suppliers and design partners as a guide in establishing an electronic communication path to participate in electronic exchange of technical and administrative data with Boeing.

1.2 Scope

This document is limited in scope to the use, benefits and implementation of the current production functionality offered by SNET TDI, although many other potentially beneficial scenarios may exist that are beyond the scope of this publication.

1.3 Supplier Network and Technical Data Interchange

Boeing Commercial Airplane Group, Materiel Division, Supplier Network project was created to develop a cost effective communications network for improving the flow of internal and external information. An "open systems" architecture was implemented to provide a single logical point of access for all electronic communications with Boeing from all outside entities. The SNET TDI system is now used by most Boeing Commercial divisions besides the Materiel Division.

The SNET project consists of two separate and distinct parts:
1) Electronic Data Interchange (EDI) - the exchange of electronic business forms (purchase orders, shipping schedules, etc.)
2) Technical Data Interchange (TDI) - the exchange of any other type of data in electronic format (primarily used to exchange CATIA, Digital Product Definition (DPD)data, DCAC/PDM data, text data, etc.)

1.4 Project Overview - Technical Data Interchange

The project goal was to design and implement an automated electronic method by which BOEING, its customer base, and trading partners could efficiently and effectively exchange digital data in a rapid and secure manner. The process that was developed is known as Technical Data Interchange or TDI.

What is Technical Data Interchange?

Technical Data Interchange is a process for electronic exchange of technical and administrative data with our trading partners, vendors and design/build partners.

Examples of "technical" data are:
- Digital product definition
- Master dimension data
- Specification control drawings
- Automated parts list
- Drawing change notices
- Performance specifications
- Executable and source code

Examples of "administrative" data include:
- Schedule charts
- Spreadsheets
- Database files
- PC generated graphics

What are the benefits?

- Reduction in data distribution flow time.
- More cost effective than the current alternatives (paper and tape)
- Improvement in data integrity
- Increased accuracy with fewer errors occurring during transfer.

An additional benefit, though less tangible, is that TDI provides extension of the concurrent engineering environment into the trading partner base and neutralizes time zone differences.

Electronic exchange of digital data is rapidly evolving from exclusive proprietary systems to an open systems architecture. This greatly enhances the cost and feasibility of exchange between unlike systems on both domestic and international levels. Competitive manufacturers of tomorrow cannot afford to ignore the substantial savings in time, cost, systems integration, and process improvements that this new technology offers our industry.

2.   SYSTEM OVERVIEW

2.1   Network Architecture Overview

The TDI system was designed in a modular fashion for easy modification of the current environment and functionality. It is used for electronic file transfers between Boeing and its customers. The networks into the TDI system are divided into two groups - internal networks used by Boeing Groups and external networks accessible by our trading partners.   The network requirements are determined on a case-by-case basis for each SNET TDI user based on the user's business needs.

2.2   Supplier and Trading Partner Access to Boeing

Suppliers and Trading Partners may connect to Boeing to access the SNET TDI service utilizing either the public internet or private network connections to Boeing. The Boeing Company selected several network providers to offer electronic access to Boeing. These network providers may route the traffic to Boeing via a private connection which is not connected to the public internet, or via the public internet. This method allows Suppliers and Trading Partners to determine the network provider and the type of connection based upon their needs.

The following page is a graphical representation of the SNET-TDI system.

The internal Boeing networks support the following operating systems:
- WIN95 and upward
- MVS
- UNIX or AIX

The external networks utilize one of the following environments:
- Public networks
- Private networks

The external networks utilize the following network connectivity protocols:
- Public Internet
- ISDN
- Frame Relay
- Dedicated line

Boeing Supplier Network Access Options

Boeing Internal Network

Network Environment

Boeing Supplier

Windows Server

PC

SNET-TDI

IBM mainframe

x or AIX workstation

Public Internet

Private Internet Services

WAN Device (Modem / Router)

05/25/2000

THE BOEING COMPANY
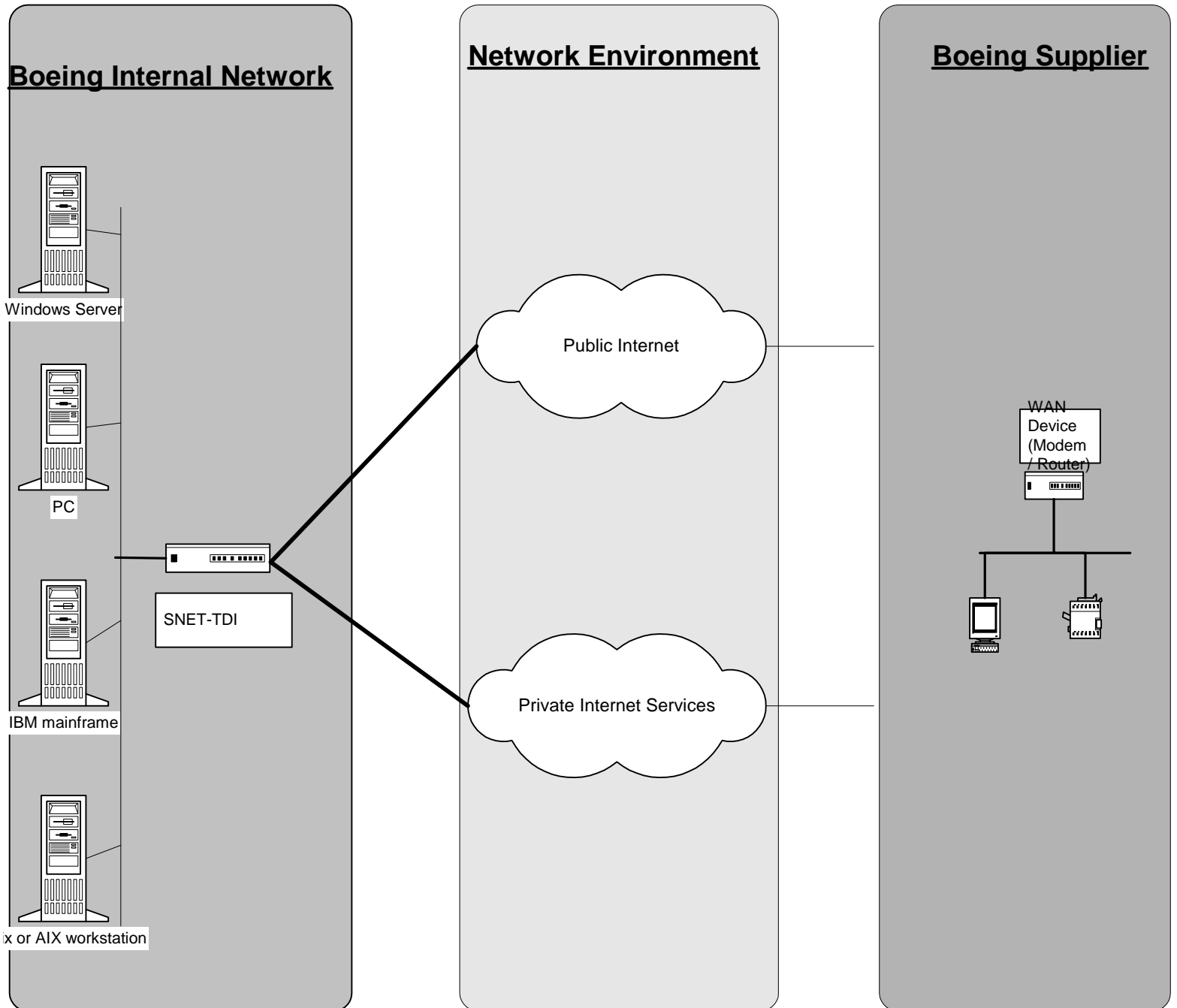
2.3   SNET TDI interface processes

The Supplier Network Technical Interchange Interface document in Appendix A of this user guide describes the interfaces available to SNET TDI users along with sample file names. The interfaces are divided into two groups - **internal interfaces** used by Boeing groups and **external interfaces** used by Boeing's trading partners.

Trading partners have the option to either come to the SNET-TDI server and FTP the files at their leisure or they may opt to have Boeing FTP the files to a secure account on the supplier server. Both these scenarios are described in the Interface document. For the trading partner, the description of the internal interfaces are informational.   The description of each process contains samples of file naming formats valid for that specific interface. For more details, see Appendix A - Supplier Network Technical Data Interchange Interfaces.

2.4   Outbound to Trading Partner

Requests from within Boeing for delivery of files to the trading partner are read and placed in TDI's queuing process.

TDI reads each request off the queue, obtains the file, encrypts/signs the file (unless the electronic connection between Boeing and the trading partner is HARDWARE ENCRYPTED), and sends the data to the trading partner.

The SNET TDI system delivers outbound files to trading partners via an external interface FTP process. SNET TDI is configured to FTP files directly to the trading partner's site. The trading partner must meet specific requirements if they wish to have SNET TDI data pushed to their system.

These requirements include:

> 1) IP address and an FTP account secured by password,
>
> 2) trading partner's system must be operational on a 7X24 schedule (exceptions can be made if the trading partner coordinates system unavailability schedules with the SNET TDI Organization).

Trading partners may also opt to have SNET TDI deliver outbound files to their FTP account and the trading partner will initiate an FTP session to the SNET TDI machine, log onto their assigned FTP account and download files to their own system.

2.5   Inbound from Trading Partner

The trading partner must be certified for inbound to the TDI system prior to sending files inbound to Boeing. If the trading partner has a new requirement to send files inbound, they should contact their Boeing buyer to initiate this requirement. Once the certification process is complete, the trading partner must follow specific SNET TDI rules on naming files to ensure proper processing and delivery of the file within Boeing. For additional information on SNET TDI's File Name Format requirements for sending data inbound to Boeing, see Appendix A – Supplier Network Technical Data Interchange Interfaces' section on the External Interface for Inbound Push.
When a file is received from the trading partner, TDI decrypts the file (unless the electronic connection between Boeing and the trading partner is HARDWARE ENCRYPTED), and hands the file off to the designated end user process..

If the data is CATIA, the SNET-TDI system forwards the data to the Boeing mainframe isolation region where it is virus scanned and integrity checked. Then, the mainframe

application called DTU is notified that the file has been received and is ready for delivery to the designated application system.

3.   SNET-TDI GROUP INFORMATION

3.1   Supplier Network Support Responsibilities

The SNET-TDI connection responsibilities are divided between two groups. The responsibilities range from gathering the network requirements to testing and implementing the connection into production. The specifics are defined below:

3.1.1   SNET-TDI Business Systems Analyst Responsibilities

The SNET-TDI Coordinator provides the following support:
* TDI system sustaining support - responsible for providing, approving, and prioritizing the sustaining and update requirements of the SNET-TDI production and test system,
* new trading partner connection requirements - responsible for the coordination of requirements, including facilitation of the Trading Partner Agreement, support in facilitating data on/off Boeing mainframe(s), Boeing business procedure consultation to buyers and supplier technical contacts, as needed,
* production support - responsible for timely delivery of production data by responding to file delivery failures on/off Boeing mainframe(s).

3.1.2   SNET-TDI Technical and New-Connection Analyst Responsibilities

The SNET-TDI Technical and New-Connection focals provide the following support:
* software maintenance - responsible for maintenance of the SNET TDI application
* production support - responsible for timely delivery of production data by responding to file delivery failures and providing a technical support line for all support questions
* new trading partner connection setup - responsible for coordination and setup of network for exchange of technical data requiring encryption.

The SNET TDI new-connection focal will perform the following tasks to facilitate the setup of the network connection:
a) Contact the designated trading partner focal to confirm spelling and correctness of company's name, focal's and backup's name, phone number, email address
b) If there is a requirement to push data to the trading partner, request a push account on the trading partner's firewall.
c) Create TDI FTP account(s) for the trading partner
d) Inform the designated trading partner focal of the TDI FTP account name(s) and login password.
e) If the connection is not hardware encrypted, perform PGP key exchange process as stated in Section 4 Encryption Information.
f) Finalize the TDI table updates to recognize the trading partner's TDI FTP account
g) Notify the Boeing focal(s) and the SNET-TDI Coordinators responsible for the certification test

3.2 Trading Partner Responsibilities

The trading partner should provide a designated primary and backup focal to the SNET TDI new-connection focal who will act as the "single point of contact" for the following:

- TDI FTP account owner
- PGP encryption
- Production support
- Distribute any correspondence to the appropriate people

3.2.1 Trading Partner focal change

Since the SNET TDI group maintains a list that identifies one primary and one backup focal at each trading partner site who is authorized to receive FTP account/password information, it is imperative that trading partners notify us whenever there is a "focal" change, mailing address, and/or phone number change. To make focal changes for the SNET TDI electronic connection for your company, please contact the SNET TDI Technical Support phone number or SNET TDI group email box listed in Section 7.1 - Supplier Network (SNET-TDI Availability and Support Schedule) and provide updated information concerning any focal changes.

3.2.2 Accessing the SNET-TDI Firewall Server and FTP Account/password

The SNET TDI new-connection focal will provide the designated trading partner focal with a SNET TDI FTP account name and login password.

To access the FTP account:
a) Connect to the Boeing FTP server using the domain name "tdi.boeing.com"
b) At the "Name" prompt, enter your SNET TDI FTP account name
c) At the "Password" prompt, enter your password
d) If you are able to log in successfully, enter "dir" to see a listing of files in your SNET TDI FTP account.
e) If you have any problems, contact our SNET TDI Technical Support group

3.2.3 Frequency of TDI FTP Account/password change

Since the password for your FTP userid will expire every 180 days, the SNET TDI group will be updating the password and sending Password Notification letter along with the effective date to the SNET TDI FTP account owner who is designated as your group's primary focal.

3.2.4 Setting up your FTP software

The following will explain what features of your FTP software that you will use to interface with our SNET TDI application.

You will need some type of FTP software that will allow you to connect to remote sites, get (download) and put (upload) files from a remote site and delete files at the remote site. Your FTP can be either a DOS command-line type FTP or a GUI

(Graphic User Interface type FTP which allows you to "drag and drop" files). If you wish to use a GUI type FTP software, but do not currently have one, call the SNET TDI Technical Support Line and we can provide you with additional information regarding GUI FTP software packages available on a 30-day free trial basis.

Please note: The "how to" instructions for your FTP software (described below) assumes that you have a graphical user interface (GUI) type FTP. Information on DOS FTP can be made available to you if you are not planning to use a GUI FTP software.

3.2.5   Setting up Your GUI-type FTP software

After installation of the GUI FTP software, you will want to set up a "profile" or "site label" specifically for your Boeing TDI FTP connection (if you have more than one connection with Boeing (i.e., a connection for Boeing Seattle and a connection for Boeing Wichita), then you will want to set up a separate "profile" {or "site label"} for each connection).

It is also recommended that you set up a folder specific to each Boeing connection on your hard drive (such as: c:\Boeing SNET TDI - Seattle and/or c:\Boeing SNET TDI - Wichita). This will be the folder into which you will be downloading files from your FTP account on the SNET TDI system.

1. **How to create a Boeing SNET TDI connection profile using "Add site" or   "New site" (or something like that):**
    a)   Profile or site label (description) can be "Boeing SNET TDI - Seattle
         or Wichita"
    b)   Host address or IP must be the domain name of the SNET TDI system which is:
         tdi.boeing.com
    c)   Userid or account name will be your Boeing SNET TDI FTP account name
         (i.e., dde_xxxxxx)
    d)   To secure this connection to the SNET TDI system, you must leave the
         password field BLANK so that your FTP software prompts you for the
         password each and every time you start-up a connection to the SNET TDI
         system.
    e)   Login type must be normal and not anonymous.
    f)   Transfer mode or type should be ASCII or image (Binary) and not "Auto
         detect".
    g)   Host type should be VMS or VMS UCX.
    h)   Initial local directory should be your hard drive folder where you will be
         downloading files to.
    i)   Make certain that any Connection Retries-type field is set to zero or 1.
    j)   Save your Boeing SNET TDI connection profile.

2.   **Connecting to your Boeing TDI FTP account (dde_xxxxxx):**
    a)   You need to be connected to your internet first, then use your FTP method to
         connect to the SNET TDI system.
         The domain name of our machine is tdi.boeing.com.
    b)   At the account or user name prompt: enter your Boeing TDI FTP account

name. (Note: If using a GUI FTP, you will not see this prompt if you filled in the account name field in your profile).

   c) At the password prompt: enter your password

3. **Transferring (FTP'ing) files:**

   a) If receiving files from Boeing, select the file(s) to transfer.
If sending files to Boeing, encrypt & sign the files first using the PGP software then select the file(s) to transfer

   b) Make certain that the transfer type or mode is either ASCII or BINARY depending on the type of data that is being transferred.
Do not use Auto Detect.

   c) Drag (FTP) the selected file(s) to the destination directory or double clicking on the selected file(s) will put the file(s) in your most current destination directory.

4. **Processing the downloaded files:**

   a) If receiving encrypted files from Boeing, decrypt file(s) using PGP decryption instructions.

   b) Once you have successfully processed files that you ftp'd from your SNET TDI FTP account (i.e., decrypted and verified the data is readable on your system), delete the file from your SNET TDI account.
Within 5 minutes of deleting the file, SNET TDI will remove the record of this file from the PICKUP.LOG file (in your directory) and add a record in the HISTORY.LOG file. Explanations of the PICKUP.LOG and HISTORY.LOG files are described in section 5.4.4 and 5.4.5.

4.   ENCRYPTION INFORMATION

Pretty Good Privacy (PGP) is the encryption software Boeing has chosen as the standard encryption package you must use to set up your communications platform.

4.1   Overview

The Boeing Company requires all sensitive data transmitted outside the company to be encrypted. This section outlines the BOEING encryption methodology and procedures used to deliver data electronically via Supplier Network (SNET), Technical Data Interchange (TDI).

The encryption process begins with a file of user data to which the encryption package applies a mathematical algorithm and a "key" to encode the data into an unreadable file. The resulting file is, theoretically, mathematically infeasible to decode without the key used to encode it. Encryption of data files is analogous to using a key to lock a door or filing cabinet. Securing the key ensures that what is behind the lock will remain secure. However, if the key is compromised, anyone having the key could unlock the data. Therefore, assuring the security of the key is of paramount importance to the security of the data! Additionally, Boeing will require that one person at the trading partner site be identified as being responsible for Security Maintenance.

4.2   Public Key Encryption

This section outlines the process that Supplier Network (SNET) - Technical Data Interchange (TDI) uses to install and use the PGP public key software encryption tool.

4.2.1   Definition Of Encryption Related Terms:

The following terms are used throughout this section:

PGP   Pretty Good Privacy (PGP) is the encryption software package that SNET TDI uses to exchange sensitive data with Boeing trading partners.

PGP Corp   The company which owns and commercially markets the PGP software encryption product.

Key Ring   The file which contains your keys. With PGP, there is a key ring (file) for both the private keys and the public keys. The pass phrase is the password into the private key ring.

Public Key   The public key is created in conjunction with the private key. It is the key which encrypts a message. Public keys are distributed to all parties that need to exchange encrypted data. The sender uses the recipient's public key to encrypt a message. The recipient uses his/her private key to decrypt the message.

Private Key The private key is the key which can decrypt a message. The private key is created in conjunction with the public key.   When a message is encrypted with a public key, the only key that can decrypt it is the private key associated with the public key.

Passphrase   PGP uses the Passphrase to secure the public and private key pair. The Passphrase is much like a password on an account.

RSA   Rivest-Shamir-Adleman public key cryptosystem. The RSA algorithm is proprietary and closed. Note: To be compatible with SNET TDI, you must be able to build an RSA type key.

DSS   Diffie-Hellman is the EIGamal variation of Diffie-Hellman. This cryptographic algorithm is open; however, SNET TDI does not currently support DSS generated keys.

IDEA   International Data Encryption Algorithm. PGP uses this algorithm to encrypt the data.

4.2.2   Encryption Setup with BOEING Trading Partners

In order to exchange encrypted files with a Boeing trading partner using PGP, several items must be completed. The following is a list of the items and the party responsible for completion.

- The Boeing public key file will be sent to the trading partner using the telecommunication link established by SNET TDI or via email to the trading partner technical contact.
  Responsibility: Boeing SNET TDI analyst

- The trading partner public key must be sent to Boeing using the telecommunication link established by SNET TDI or by email to the SNET TDI analyst.
  Responsibility: Trading partner technical contact

4.2.3   Public Key Exchange Procedure

Ordering the PGP Encryption software

PGP Corp owns and markets the PGP encryption software. It can be purchased directly via their web site at www.pgp.com. From time to time PGP Corp negotiates special pricing for Boeing suppliers and customers. Before you purchase a copy of PGP, be sure to contact one of the SNET TDI business analysts.

Features of the PGP Encryption software

Your PGP software should be used for PGP key management, encrypt/sign, & decrypt capabilities.

For Win95 or upwards and Win NT, the following will explain what features of your PGP software that you will use to interface with our SNET TDI application.

For other versions of PGP, consult PGP online help, PGP user guides, and/or PGP Corp Technical support.

Start PGP by clicking on the envelop/lock in lower right hand corner of your desktop (This is the PGPTRAY icon) then pick Launch PGPTOOLS
OR
Use Windows explorer to find the pgptray.exe or pgptools.exe in the PGP folder.

Note that the instructions below may vary depending on the version of PGP.
Once you get to PGPTOOLS, most of what you want to do is in the following:

1 PGP key management (PGPKEY icon with 2 keys)
2 Encrypt & sign (Encrypt + Sign icon with envelop, lock, and feather or pencil)
   After you select the file to encrypt/sign, a Key selection dialog goes up.
   For binary files, make certain that the text option box and the 'Input is text'
      option box (if available) are unchecked.
   For ASCII files, make certain that the text option box and the 'Input is text'
      option box (if available) are checked.
3 Decrypt (Decrypt/Verify icon with envelop and letter flying out or open lock)

If you lose your PGP keys or can not remember your PGP key's passphrase, you will need to create a new PGP key pair. Call the SNET TDI Technical support Line to walk you through generating your key pair and sending your new public key to the SNET TDI group.

Generating a RSA Key Pair

After you receive your PGP encryption software and have installed it on your system, you are ready to generate your RSA keys. Boeing has specific requirements for generating your key pair. Please review the following requirements prior to generating your company key pair:

1. Since you are building your company's key pair, when prompted for "full name" information, you should identify your company name (not an individual's name), followed by your city and State within parenthesis, for example:
   Molded Plastic Company (Seattle, WA)
2. When prompted for an email address, use your company's email address, your private email address, or not specify an address (blank). If you do not specify an email address, you will be asked later "Do you really not want an email address?" so at that time you would enter "no".
3. You must be able to generate an RSA type key that will allow you to Encrypt/Decrypt/Sign/Verify.
   If you are not asked for key type, you need a different version of PGP so cancel the key generation process and contact the SNET TDI Technical Support line.
4. Your key size should be the largest RSA key size possible.
5. Your key must never expire.
6. PGP will ask you to establish a Passphrase.
   Your Passphrase must be:
   • at least 9 characters in length
   • include both alphabetics and numerics
   • part of the Passphrase should not be found in the dictionary
   • choose a Passphrase that is not easily hackable
   Note: The Passphrase is case sensitive.
   Be sure to make note of your Passphrase and store this information in a secure, locked area accessible to authorized personnel only. A Boeing Customized Password Form has been provided in Appendix B – Boeing Limited Customized Password Form.
7. Newer versions of PGP will ask if you want to send your key to the server (meaning the PGP server or your default server). This is your choice, Boeing has no requirement for you to do so. By sending your key to Network Associate's

PGP public server, anyone or any company will be able to get a copy of your public key.

8. If prompted for random bits, these can be collected by moving your mouse or typing random characters on your keyboard.

9. After your RSA key pair is generated, you are ready to exchange public keys with Boeing. Contact the SNET TDI Technical Support line, your SNET TDI new-connection focal, or SNET TDI Coordinator focal to continue the key exchange process.

Backing up your PGP keyrings

It is very important to backup your PGP key ring files (public and private/secret key ring files) onto diskette or tape. This will enable you to recover your PGP key ring in the event you ever need to restore your system.

Refer to your PGP documentation to help you identify the names of the key ring files on your system.

Note: For WIN 95 Version 5.5.x of PGP, the key ring files are called:
PUBRING.PKR & SECRING.SKR (look in the directory where your PGP is installed or use the WINDOWS Explorer FIND command to search for these files using "*ring" as the search parameter).
If you have the version of PGP that has the PGPTRAY, select PGP PREFERENCES and the FILES tab will have the path of your PGP public and private keyrings.

To ensure your key rings and PASSPHRASE (which is required for encryption/decryption) are recoverable, store the backup copy of your key rings along with your PGP PASSPHRASE information in a secured, locked area, accessible to authorized personnel only.

Note the location of your backup key file on the Boeing Customized Password Form which has been provided in Appendix B – Boeing Limited Customized Password Form.

Editing your passphrase

If you need to revise your passphrase after it has been generated, refer to your PGP documentation on Changing Passphrase.

PGP Key Exchange Process

The following is a detailed flow of the key exchange process:

An SNET TDI new-connection focal will work with you and help you step through the key exchange process. The following processes will be covered:

1. Generating your PGP key pair
2. Exporting your public key into a file or pasting into an email to your SNET TDI new-connection focal

3. Connecting to the SNET TDI system
4. FTP commands
5. Exchanging public keys
6. Adding keys to key rings
7. Certifying or signing public keys
8. Verifying key fingerprints
9. Exchanging encrypted files
10. Decrypting files
11. If there are requirements for sending files inbound to Boeing, encrypt/signing files
12. Overview of SNET TDI processes (including information about LOG files in your TDI FTP directory, file deletion, certification process, key ring backup, etc.)

Re-exchange of a trading partner's key

If for any reason a trading partner must re-exchange their public key, the trading partner should notify the SNET TDI Technical Support line. Possible reasons may be that the PGP key may have been compromised, damaged, or lost.

SNET TDI will stop all transfers to and from that trading partner until new keys are generated and exchanged as required.

NOTE: NO DATA WILL BE EXCHANGED WITH THE TRADING PARTNER UNTIL PROPER ACTIONS ARE TAKEN TO RESTORE PGP SECURITY ON THE SNET TDI SYSTEM AND AT THE TRADING PARTNER'S SITE.

4.2.4   Encryption / Decryption Procedure

All files that are encrypted using PGP must use the file signature option. The file signature option signs a data file with the sender's secret key and then encrypts it with the recipient's public key.

In some cases, the Boeing trading partner may have multiple public/private keys for use with different applications. For example, a trading partner may have one public/private key for exchanging CAD/CAM data and a separate public/private key for multi-media data. In this case, the SNET TDI system will encrypt and sign the data for the Boeing trading partner using all the public keys for that trading partner.

4.2.5   Frequency of Public Key Management

The Boeing trading partners on the SNET TDI system will be required to change their public/private key under the following conditions:

- The public / private key has been compromised on the encryption platform at the trading partner site.
- The data that was encrypted using the trading partners public key was compromised by a third party.

The Boeing trading partners are required to change their PGP Passphrase whenever the communications/encryption support personnel change at the trading partner site. It is imperative that the trading partner ensure the SNET TDI group has the correct

focal name and phone number at all times. Call the SNET TDI TECHNICAL SUPPORT number to report focal name/phone changes.

5.   FILE NAME FORMAT

5.1   Purpose

The "file name" is how a trading partner communicates information to the SNET TDI system about the files being sent to Boeing. The trading partner must follow a specific file naming convention in order for their files to be successfully processed and delivered to the appropriate Boeing node and recipient.

Incorrect filenames will result in:

- file transfer failure within the SNET TDI system
  Production Support Analyst will be paged and problem resolution activity will be initiated.

Refer to the Supplier Network Technical Interchange Interface document in Appendix A which describe the interfaces available to SNET TDI users along with sample file names. The File Name Formats for Suppliers (External Interfaces) section explains the file naming format in detail.

SNET TDI supports the following formats:

1. DOS file name format (short)
2. Long format with destination/source information
3. Long format with comment information

DOS file name format (short)

- Used primarily for outbound CATIA data from the Seattle IBM mainframes using the DTU interface.
- Supports inbound CATIA data destined for a Boeing IBM mainframe using the DTU interface (which includes both the Seattle and Wichita mainframes).

Long Format with Destination/Source Information

- Supports PC data exchange (outbound and inbound).
- Supports inbound data destined for delivery to Boeing Group recipients interfacing with SNET TDI via their own SNET TDI FTP account
- Supports inbound data destined for delivery to a Boeing NT server
- Supports inbound data destined for delivery to a Boeing Unix server

Long Format with Comment Information

- Supports inbound IGES data
- Supports outbound data

5.2   File naming conventions

The length of the file name delivered by the SNET TDI system to a trading partner is determined by a value defined within the SNET TDI system itself for each trading partner's FTP account.

> The minimum file name length allowed for an outbound filename is 8 characters plus a 3-character file extension (for example):
>
> bxxx0011.c02

bxxx0021.c18

bxxx0031.i01

The maximum file name allowed in SNET TDI is 39 characters plus a 3-character file extension (for example):

bxxx0041_823r1126s05—d-21_end_frame_de.i01

bxxx0051_823r1126s05—a-21_wing_strut_d.c18

bxxx0061_823r1126s05—b-21_tie_frame_de.c02

The trading partner may have a preference regarding the length of the filename they receive from the SNET/TDI system. Usually the trading partner makes this decision based on their operating system (i.e., whether or not long filenames will display properly) and/or the type of FTP interface used when "pulling" files to their site. Trading partners using a "command-driven" FTP software package often prefer the minimum length filename for ease in keying in the filename.

Trading partners often prefer to see the maximum length filenames in SNET TDI because the filename can include helpful information about the data being sent. The type of information (about the data) passed to the SNET TDI system (by the Boeing sender) is dependent upon the particular interface being used by the Boeing sender. For example: if the sender is using the mainframe application called DDD to send CATIA and/or IGES data, then the DDD application automatically provides model name and/or part number information to SNET TDI. The resulting SNET TDI filename will include the model name and/or part number information if the trading partner's SNET TDI connection is set up to display maximum file lengths. (It is important to note that additional information passed in to the SNET TDI system is always available by viewing the "LOG" files in the trading partner's FTP account. If the trading partner prefers short filenames, they can view their "LOG" files for additional information about each file transferred.)

The following paragraphs describe the various types of Boeing sender's interfaces into the SNET TDI system and the "additional" information commonly passed to the SNET TDI system and displayed in the SNET TDI filename if the trading partner's SNET TDI connection is configured to display maximum filename lengths:

- If a trading partner is receiving CATIA files from the Boeing via the Seattle mainframe application called DDD, and the filename length is set to the maximum allowed, a portion of the CATIA model name and/or part number will be displayed as part of the filename. For example: bxxx0021_W5928_Y5928_FB_192T0101_50_SH.C02

- PC type files (ZIPPED) sent to the trading partner typically make use of the maximum length filename, which is 39 characters plus the 3-character file extension. The information contained in this type of filename will identify the Boeing sender (6-character limit), plus provide information that identifies the destination node and recipient (referred to as "recpnt" in the example shown below due to 6-character limit) at the trading partner's site. An example of a PC type filename would look like this: Bxxx0011_sender_xyz_recpnt_247081015.zip.

- The maximum length filename is often used when the Boeing sender is interfacing directly with the SNET/TDI system to send data outbound to trading partners. This type of interface is called a "Boeing Group" interface and is commonly used when the Boeing Group's data source is an NT or UNIX server, or the data is coming from a mainframe platform that is not supported by the DTU application. For this type of interface, the Boeing Group is assigned a SNET TDI FTP account on the SNET/TDI system. Boeing Groups can either use manual FTP to deliver files to their SNET/TDI FTP account or they may choose to write a customized interface to automate the FTP process. Maximum length filenames are often used for Boeing Group interfaces so that the Boeing sender, destination node and recipient or information about the date being sent will be displayed as part of the SNET TDI filename to assist the trading partner with file processing and/or delivery at their site. Here are some examples of files sent via the Boeing Group interface to the SNET TDI system:

  bxxx0051_TEST_PFD_REPORTS_W306999.TXT

  bxxx0061_brian_GRP_boeing_228120138_test.BIN

  bxxx0071_PART_W65C9999—D-SHT2-WINGNUT.ASC

- For DCAC/PDM files, SNET/TDI recommends the maximum filename length of 39 characters plus the 3 character extension. The information contained in the filename will include a unique identifier: "Message Sync Id", for the DCAC file. This id would help suppliers and Boeing to research and communicate questions about a particular file. We recommend the maximum length; however, any filename length will work. In any case, the supplier history log will contain the full "Message Sync Id". An example of a DCAC type filename would look like:

  Bxxx0011_ SNETDDAT0310199915290112.stp

5.3 Data type examples

The following tables show some examples of the most commonly used data types:

Outbound Filename extension (Data Type)	Inbound Filename extension (Data Type)	Transfer type	Description of Data	Data source	Comments
BIN	BIN	Binary	Binary files		
TXT	TXT	ASCII	Text or ASCII files		
PKG		ASCII	Package list	DCAC PDM	
PS		ASCII	Postscript	DCAC PDM	
STP		ASCII	Step files	DCAC PDM	
ZIP	ZIP	Binary	Zipped binary files (PKZIP compatible)	PC	For inbound, zip file first then encrypt & sign. For outbound, decrypt file first then unzip.
BED		Binary	Scanning data	Seattle & Wichita plotting centers	
I01	I02	ASCII	IGES data	Seattle/Wichita CAD/CAM	
CAD		Binary	CADKEY	Seattle CADKEY system	
C02	C01	Binary	CATIA data in CATEXP SEND format	Seattle CATIA	CATIA Project Files are synched with the trading partner.
C03		Binary	Library & standards files	Seattle	
C18	C20	Binary	CATIA data in CATEXP EXPORT format	Seattle/Wichita CATIA	CATIA Project Files are not synched with the trading partner.
	C30	Binary	CATIA data in CATDATA format	Seattle CATIA	To support plotsheets.
TTT		ASCII	TSO files	Seattle mainframe	

Note: Not every SNET TDI data type is shown in the above matrix. For specific information concerning the data types for your connection, contact the SNET TDI Technical Support line.

5.4 File Acknowledgment

5.4.1 Boeing Files to Trading Partners

For trading partners who access their SNET TDI FTP account on the Boeing firewall and copy files to their site, the files are not acknowledged as being successfully received until the trading partner deletes the files off of their firewall account. Deleting those files triggers an application that writes an entry in the "history.log" showing the files were picked up.

NOTE: Files that remain on the trading partner's firewall account are not acknowledged until they are deleted. Always copy the files to your site, verify that there have been no transmission problems, decrypt, and process the file before deleting the files from your firewall. Within 5 minutes of deleting a file from your FTP account, the SNET TDI system will place a record in the "history.log" file (in your directory) indicating "ack" along with the "date removed", and remove the corresponding record for the deleted file from the "pickup.log" file.

The SNET TDI system will delete any files older than forty-five days, place a record in the trading partner's "history.log" file indicating "purge" along with the "date removed", and remove the corresponding record for the purged file from the "pickup.log" file. The SNET TDI group strongly recommends that each trading partner delete their files from their FTP account instead of depending on our "purge" process.

5.4.2 Boeing Files to Trading Partners

For trading partners where Boeing FTPs files to a firewall account at the trading partner's site, Boeing assumes success upon completion of the file transfer and writes an entry in the "history.log" immediately.

5.4.3 Files sent from Trading Partners to Boeing

Trading partners sending files to Boeing are required to FTP the files from their site to their account on the Boeing firewall. Files received from trading partners are decrypted and routed to the appropriate end-system. Once those files are successfully routed, an entry is written to the "ack.log" file acknowledging the date and time of file receipt.

5.4.4 The Pick-up File

If there are files in your directory on the Boeing firewall awaiting pick-up, the SNET TDI system creates a file called **pickup.log** that contains a list of the file names. You are welcome to use it to automate your system for retrieving files. The **pickup.log** file is an unencrypted ASCII Text file; therefore you must transfer the file in ASCII Transfer Mode. The SNET TDI system updates the "log" files every five minutes. When additional files are delivered to the trading partner's FTP account by the SNET TDI system and/or the trading partner deletes received Boeing files from their account, within 5 minutes of file delivery/deletion the SNET TDI system will update the information in the **pickup.log** accordingly.

All files Boeing sends to you will begin with the letter "B".
This log will contain a record for each file beginning with the letter "B" in your directory. Until you delete the "B" files, they will continue to show up in this log.

If files are pushed directly to your machine, you will not have this log.

The format of **pickup.log** looks like the following:

<u>PICKUP.LOG example</u>

```
FILES FROM BOEING WAITING TO BE PICKED UP:          Wed Mar  3 16:14:50 1999
-----------------------------------------------------------------------------
Prefix        Typ       Date Delivered      Size         Application Data ID
-----------------------------------------------------------------------------
beee0021      I01      Fri Feb 12 05:28:28  00192726     LLR0212A,20453,B844909
beee0011      I01      Fri Feb 12 05:28:24  00001680     LLR0212A,20453,B844909
beee0031      zip      Mon Mar  1 07:01:19  00010759     HARVEY_AFA_KELLEY_60065326
bggg0071      c02      Thu Feb 25 12:48:43  02340376     113N1046M05-FD...BEAM
bggg0081      c02      Thu Feb 25 12:50:47  01257316     115A1110S01-... MLG BEAM
```

5.4.5   The History File

Your Boeing directory contains two files called **history.log** and **history.old** which contain lists of all files exchanged with Boeing for the current and previous months.

If you delete data files from your SNET TDI FTP account or files are pushed to directly to your machine or you send files to Boeing, a record will be placed in the HISTORY.LOG.

At the beginning of each month, the current contents of **history.log** are copied to **history.old**. **History.log** then is archived by Boeing and a fresh copy of **history.log** is started.

The format of **history.log** looks like the following:

<u>HISTORY.LOG example</u>

```
HISTORY OF FILE TRANSFERS WITH BOEING:  Feb  1 1999 08:41 TO Mar  4 1999 15:35
-----------------------------------------------------------------------------
Prefix    Typ  Date Delivered    Size    Application DataID    Status  DateRemoved
-----------------------------------------------------------------------------
baaa0091 c02 Wed Mar310:36:07 00680118  175A1701M07-AD-...  SENT
baaa00a1 c02 Wed Mar310:37:26 00572725  182A2404S01-BDV1 ...SENT
bccc0171 zip  11/23/99 14:50  00008606  JOHSMI_AFA_...      purged Feb14:38:43
bccc0191 zip  11/23/99 10:19  00040361  JOHSMI_AFA_...    purged Feb1412:35:42
SBGA0171 C01 Mon Feb813:40:01 05034546                      ack
SBGR0181 C01 Wed Mar307:18:13 03193960                      ack
bzzz0061 c02 TueFeb231307:43  01863553  SNET DDE...BASELINE  ack Feb2606:08:46
baaa0v61 stp ThuFeb2522:59:56 00002570
ATTNTO_PDM_PDMDIS_5622822_SNETDDAT0225199914082012  ack     Fri Feb 2608:52:42
baaa0v71 pkg FriFeb2602:00:22 00000869
ATTNTO_PDM_PDMDIS_56221457_SNETDDAT0225199914145612 ack     Fri Feb 2608:52:42
baaa0v91 ps  SatFeb2704:21:46 00254659
ATTNTO_PDM_PDMDIS_4723127_SNETDDAT0215199918312612  ack     Sat
bzzz0061 c02 TueFeb2313:07:43 01863553  SNET TDI TEST ...   ack  Feb2606:08:46
```

5.4.6 The ACK File

Your Boeing directory contains two files called **ack.log** and **ack.old** which contain lists of acknowledgments of files received by Boeing for the current and previous months. If you wish to automate your process for receiving acknowledgments of files sent to Boeing, this file is useful. You may retrieve this file and delete the copy in your Boeing directory as often as you like. The Boeing system will create a new **ack.log** file whenever it cannot find an existing one. The **ack.log** file only contains entries for files Boeing has received since the current **ack.log** was created. If you do not send files to Boeing, this log will be empty.

At the beginning of each month, the current contents of **ack.log** are copied to **ack.old**. **Ack.log** then is archived by Boeing and a fresh copy of **ack.log** is started.

The format of **ack.log** looks like the following:

<p align="center">ACK.LOG example</p>

```
FILES RECEIVED BY BOEING:                        Wed Mar  3 16:01:14 1999
-----------------------------------------------------------------------
Prefix     Typ      Date Delivered     Size      Application Data ID
-----------------------------------------------------------------------
SBGA0171   C01    Mon Feb 8 13:40:01   05034546
SBGA0181   C01    Mon Feb  9 11:10:01  05034546
SAFA0191   zip    Mon Feb 15 10:19     00040361   SMITH_AFA_JONES_046101038
```

5.4.7 The FTPSERVER_DTP File

Your Boeing directory shows a file called **FTPSERVER_DTP.log** which contains accounting information about your Boeing FTP directory. Every time you log onto your SNET TDI FTP account on the SNET TDI system, the "version number" after the semicolon will increment by 1. The Boeing system will create a new **FTPSERVER_DTP.log** file whenever it cannot find an existing one.

The format of **FTPSERVER_DTP.log** looks like the following:

<p align="center">FTPSERVER_DTP.LOG example</p>

```
$set noon
%TCPWARE_FTPD-I-FILESENT, SUPPLIER$DISK:[DDE_123456]HISTORY.LOG;1 sent to
111.111.111.111
  DDE_123456   job terminated at 28-APR-2000 04:22:50.23
„…  Accounting information:
  Buffered I/O count:              174      Peak working set size:      2720
  Direct I/O count:                 75      Peak virtual size:        170160
  Page faults:                     343      Mounted volumes:               0
  Charged CPU time:        0 00:00:00.13    Elapsed time:      0 00:00:58.68
```

6.   FILE TRANSFER TEST

6.1   Purpose

The purpose of this section is to outline the methodology and procedures used to test Technical Data Interchange (TDI) connectivity and functionality between BOEING and the target system. Upon successful completion of this test, the established TDI connection will be certified and considered a stable production system. Any scheduled downtimes must be coordinated in advance with the Boeing SNET TDI technical support group.

6.2   Test Methodology

The appropriate communication standards used for this specific installation of TDI connectivity will be tested with regard to functionality, integrity and performance.

6.3   Functionality

The TDI System must be tested to ensure the desired functionality is achieved. Specifically, testing the ability to exchange digital files between the trading partner and the SNET gateway, between the SNET gateway and the trading partner, and end-to-end tests between the Boeing digital file systems and the trading partner digital file system, via the SNET gateway.

6.4   Integrity

Digital files of various sizes will be extracted from the Boeing mainframe digital file systems for the transmission tests. These files will be exchanged between the systems as previously outlined. Any loss of data, formatting changes, etc. must be documented and corrected prior to promotion to "Production" TDI connection status.

6.5   Performance

In order to assure the performance of SNET-TDI and its interaction with the trading partners, the Boeing mainframe system and the selected transport provider must be evaluated. The goal is to transmit all "priority 1" files within two hours, and "priority 2" files within 16 hours of the original request. Total time to transmit the request is the difference between the time the user initiated the electronic request, and the time that TDI receives the acknowledgment from the trading partner.

6.6 Reliability

The reliability and availability of the TDI system is targeted at 98.9%. The reliability is based on the percentage of requests transmitted without error, and without human intervention after the electronic request is started. Availability is based on the time that the hardware and software is running during each day.

6.7 Test Procedures

The following tests will be conducted by the TDI test team and the selected trading partner. Each test file will be transferred between TDI and the selected trading partner(s):

6.7.1 Seattle CATIA File Transfer Tests:

The process for testing the transfer of Seattle files in CATIA native format will proceed as follows:

When you log on to your FTP account and look in the PICKUP.LOG file, you will see three files whose file extension is .CNN (NN=02 for CATIA synchronized supplier sites, NN=18 for CATIA non-synchronized supplier sites) and the APPL ID field says:

SNET TDI TEST MODEL #1 - 51 KB BASELINE
SNET TDI TEST MODEL #2 - 1 MB BASELINE
SNET TDI TEST MODEL #3 - 2.7 MB BASELINE

1. FTP these three files to your site in BINARY transfer mode, (if you are using a Windows type FTP application that has radio buttons for selecting transfer mode, DO NOT PICK AUTO DETECT – pick BINARY)
2. Decrypt the files, if applicable,
3. Convert the models to the ISO code page, if necessary, using the CATAIX utility,
   NOTE: Before the models are copied to your FTP directory, CATAIX is run and they are converted to the ASCII-DS code page. Suppliers typically convert the models to the ISO code page
4. Run CATIMP to import the models to your CATIA workspace just as you would if you received the files on tape or floppy.
   - If the original file had a file extension of .C02, you will do a CATIMP *REC.
   - If the file had a file extension of .C18, you will do a CATIMP *IMP
5. For suppliers testing one-way file exchange, when CATIMP completes and you have verified the model displays ok, call the SNET TDI analyst to report the results.
6. For suppliers with a requirement to send models back to their Boeing FTP directory, complete these additional steps:
(a) Use the CATIA line function to add two lines to each model
(b) Place the lines to form an "X" over the title block
(c) File the model
(d) Run CATEXP using the *SND keyword
(e) Encrypt and sign the files, if applicable,

(f) FTP BINARY (remember, do not use AUTO DETECT) the files back to the supplier FTP account using these file names
- SBGR0011.C01
- SBGR0021.C01
- SBGR0031.C01

(g) Call the SNET analyst to report the results

(h) SNET analyst will compare the models sent back with the original models and report the successful results to the buyer or call the supplier to correct any problems

6.7.2   Seattle CATIA - IGES File Transfer Test

The process for testing the transfer of Seattle CATIA files in IGES format will proceed as follows:

When you log on to your FTP account and look in the PICKUP.LOG file, you will see a file whose file extension is .I01 and the APPL ID field says:

SNET TDI TEST MODEL - MED DRAWING

1. FTP this file to your site in ASCII transfer mode (if you are using a Windows type FTP application that has radio buttons for selecting transfer mode, DO NOT PICK AUTO DETECT – pick ASCII)

2. Decrypt the file, if applicable,

NOTE: Before your IGES processor will see that decrypted file, it
May be necessary to rename the file with a file extension of .IGS or .IGE or whatever other file extension your IGES processor expects to see.

3. Perform the IGES conversion and display the file on your CAD system

4. Call the SNET analyst to report the results

5. SNET analyst calls the buyer with the successful results or calls the supplier to correct any problems

6.7.3   Wichita CATIA File Transfer Test

The process for testing the transfer of Wichita files in CATIA native format will proceed as follows:

When you log on to your FTP account and look in the PICKUP.LOG file, you will see a file whose file extension is .C18.

1. FTP the .C18 file to your site in BINARY transfer mode (if you are using a Windows type FTP application that has radio buttons for selecting transfer mode, DO NOT PICK AUTO DETECT – pick BINARY)

2. Decrypt the file, if applicable,

3. Convert the model to the ISO code page, if necessary, using the CATAIX utility
   NOTE: Before the models are copied to your FTP directory, CATAIX is run and they are converted to the ASCII-DS code page. Suppliers typically convert the models to the ISO code page

4. Run CATIMP using the *IMP keyword to import the models to your CATIA workspace just as you would if you received the files on tape or

floppy.

    5. When complete, call the SNET analyst to report the results

6. For suppliers with a requirement to send models back to their Boeing FTP directory, complete these additional steps:

  (a) Use the CATIA line function to add two lines to each model

  (b) Place the lines to form an "X" over the title block

  (c) File the model

  (d) Run CATEXP using the *EXP keyword

  (e) Encrypt and sign the files, if applicable,

  (f) FTP BINARY (remember, do not use AUTO DETECT) the files back to the supplier FTP account using these file names

- SBGR0011.C20
- SBGR0021.C20
- SBGR0031.C20

  (g) Call the SNET analyst to report the results

  (h) SNET analyst will compare the models sent back with the original models and report the successful results to the buyer or call the supplier to correct any problems

6.7.4 Wichita CATIA - IGES File Transfer Test

The process for testing the transfer of Wichita CATIA files in IGES format will proceed as follows:

When you log on to your FTP account and look in the PICKUP.LOG file, you will see a file whose file extension is I01.

1. FTP this file to your site in ASCII transfer mode. (if you are using a Windows type FTP application that has radio buttons for selecting transfer mode, DO NOT PICK AUTO DETECT – pick ASCII)

2. Decrypt the file, if applicable,

    NOTE: Before your IGES processor will see that decrypted file, it needs to be renamed with a file extension of .IGS or .IGE or whatever other file extension your IGES processor expects to see.

3. Call the SNET analyst to report the results

7.   PRODUCTION SUPPORT

SUPPLIER NETWORK - TECHNICAL DATA INTERCHANGE (SNET-TDI)
Production problems of any kind MUST go through the SNET TDI Technical Support
line listed below. For maximum visibility and efficiency please phone all production
support problems into the SNET TDI Tech line and the support analyst will forward the
problem to the appropriate individual for closure.

7.1.   Supplier Network (SNET-TDI Availability and Support Schedule)

Supplier Network Gateway Availability: The SNET TDI system is available 24
hours a day, 7 days a week, Monday through Sunday with some exception on
Fridays.

> The SNET TDI System Administrator reserves the right to take the SNET
> TDI system down on Fridays between the hours of 5:00pm and 8:00pm
> (Pacific time) to perform system maintenance tasks (as required). Not all
> system maintenance tasks require that the SNET TDI system be
> completely shut down, but if you are connected to the SNET TDI system
> during this window and your connection is dropped, or if you encounter
> connection problems during this timeframe, it may be the result of the
> System Administrator taking the SNET TDI system down. If you suspect
> this may be the problem, please do not attempt to reconnect until after
> 8:00pm (Pacific time).

**Supplier Network Technical Support Line (425) 237-6092 or SNET TDI
Group email address is tdi@boeing.com:** The messaging service can be
accessed 24 hours a day, 7 days a week and a support analyst will answer your call
during normal business hours (Pacific time).

> Normal business hours are: Monday through Friday, 7:00am until 4:00pm
> (Pacific time).
> Messages left outside of normal business hours will be responded to
> during the next business day.
> Holiday support is considered the same as weekend support (i.e., outside
> normal business hours).

We find that most SNET TDI-related problems and questions received outside of
normal business hours can be handled the next business day. We also understand
that some problems are more critical in nature if the problem severely impacts a
business process and in such cases, an SNET TDI response is required before the
next business day. We rely on our customers and Boeing trading partners to
evaluate the situation and make a logical decision when requesting urgent
response to a problem that has occurred outside normal business hours.

For calls requiring an urgent response, call the SNET TDI Technical Support number (425) 237-6092, leave a message, then press 1 for more options. Listen and follow the instructions for sending your message with "urgent delivery." Upon delivery of your message, an on-call analyst will be paged and appropriate action (best effort) will be taken to assist you outside normal business hours.

7.2   General Coordination and Support

Non-production problems, such as: SNET TDI questions, downtime requests, and general information of a non-critical nature are directed through the SNET TDI Coordinators identified below.

SNET TDI Coordinators:

Steve Perry   (425) 234-2922
                     (206) 416-0128 (pager)

Boeing customers and suppliers with known support requirements falling outside normal business hours should coordinate these specific requirements in advance with the SNET TDI Coordinators. Anticipated high volumes of data transfer activity should be coordinated well in advance of the target delivery date/time to ensure best effort can be made to support this type of activity.

NOTE: Periodic downtimes will be scheduled and coordinated with trading partners in advance.

7.3   Comments, Questions and Corrections

User comments, questions, corrections or any other information that the end user may wish to communicate to the editors of the document, "Boeing Commercial Airplane Group, Supplier Network, Technical Data Interchange - User Manual" may be submitted on the form located as the last page of this document.

Please fill out, fold and mail to the undersigned or Email to: **Steve Perry**:
Internet Address: *steve.c.perry@boeing.com*

APPENDIX A

Boeing Commercial Airplane Group

Supplier Network Technical Data Interchange Interfaces

Introduction

The Supplier Network Technical Data Interchange application, SNET TDI, is used by Boeing employees and Boeing applications to exchange files with Boeing's trading partners. This document describes the interfaces available to SNET TDI users. The interfaces into SNET TDI are divided into two groups—**internal** interfaces used by Boeing groups, and **external** interfaces used by Boeing's trading partners. A summary of internal and external interfaces appears on the next page. The selection of an interface is determined case-by-case for each SNET TDI user based on the user's business needs.

Boeing's electronic trading partners include suppliers, customers, banks, and utility companies. However, most SNET TDI trading partners are suppliers, and for convenience this document often uses the term 'supplier' instead of the more generic 'trading partner'.

Summary of SNET TDI Interfaces (See next page for graphical representation of SNET TDI interfaces)

Internal Interfaces (for Boeing Groups)

	Name of Interface	Operating System	Direction	Comments
I-1	DTU on IBM Mainframe	MVS	Two-Way	Outbound: Boeing App submits JCL to call DTU, and DTU calls TDI Inbound: TDI calls DTU, and DTU calls Boeing App's receiving JCL.
I-2	SNETPC	WIN2K or greater	Two-Way	VB front end installed on user's desktop. Uses Dynazip.
I-3	Direct Delivery Outbound and Inbound FTP	Any Platform	Two-Way	Outbound: Boeing App copies files to their TDI "Direct Delivery" directory, earmarked for a designated trading partner (one-to-one relationship). TDI's VB Special handling zip daemon uses Dynazip to zip the files into one package and the TDI process pulls from their "Direct Delivery" directory on TDI's NT server. Inbound: Supplier FTPs files to TDI. TDI processes then FTPs the files from the supplier directory to a server (path, account & password) specified by Boeing group during the setup of this interface. Supplier does not need to zip files when sending inbound. For Windows servers, TDI will unzip any zipped files from the supplier for the receiver.
I-4	Outbound and Inbound FTP	Any Platform	Two-Way	Outbound: Boeing App FTPs DAT and REQ files to TDI server. Boeing App needs FTP account on TDI server. Inbound: Supplier FTPs data file to TDI server. Supplier needs FTP account on TDI server.
I-5	DCAC/PDM to MOM Interface	UNIX	Outbound	DCAC/PDM sends files to TDI using MOM/AI. Used only by DCAC/PDM.
I-6	Outbound_dat_node 5??update later	Any	Outbound	Boeing App FTPs DAT FILE to TDI server. Boeing app needs FTP account on TDI server.
See E-4	DDISUB	Windows or UNIX	Inbound	TDI delivers files to the Boeing group's Windows or UNIX sub-directory that is assigned to a specific supplier code
See E-5	MDDI	External: any Internal: IBM mainframe	Inbound	TDI delivers files to the IBM mainframe with a static filename per pre-agreement between Boeing customer and SNET TDI

External Interfaces (for Boeing's Trading Partners)

	Name of Interface	Operating System	Direction	Comments
E-1	Outbound FTP	Any platform	Outbound	TDI FTPs files to a secure Boeing account on a server at trading partner's site. TDI needs FTP account at trading partner's site. OR Trading partner FTPs files from TDI Server. Trading partner needs FTP account on TDI Server.
E-2	Outbound DTU	MVS	Outbound	TDI submits JCL to DTU. DTU transfers files to trading partner. Trading partner must have IBM mainframe with DTU installed. Used for SNET to DTU type outbound suppliers.
E-3	Inbound FTP	Any Platform	Inbound	Trading partner FTPs files to TDI Server. Trading partner needs FTP account on TDI Server.
E-4	DDISUB	Windows or UNIX	Inbound	Trading partner FTPs files to TDI Server. Trading partner needs FTP account on TDI Server. TDI delivers files to the Boeing group's Windows or UNIX sub-directory that is assigned to a specific supplier code
E-5	MDDI	External: any Internal: IBM mainframe	Inbound	Trading partner FTPs files to TDI Server. Trading partner needs FTP account on TDI Server. TDI delivers files to the IBM mainframe with a static filename per pre-agreement between Boeing customer and SNET TDI
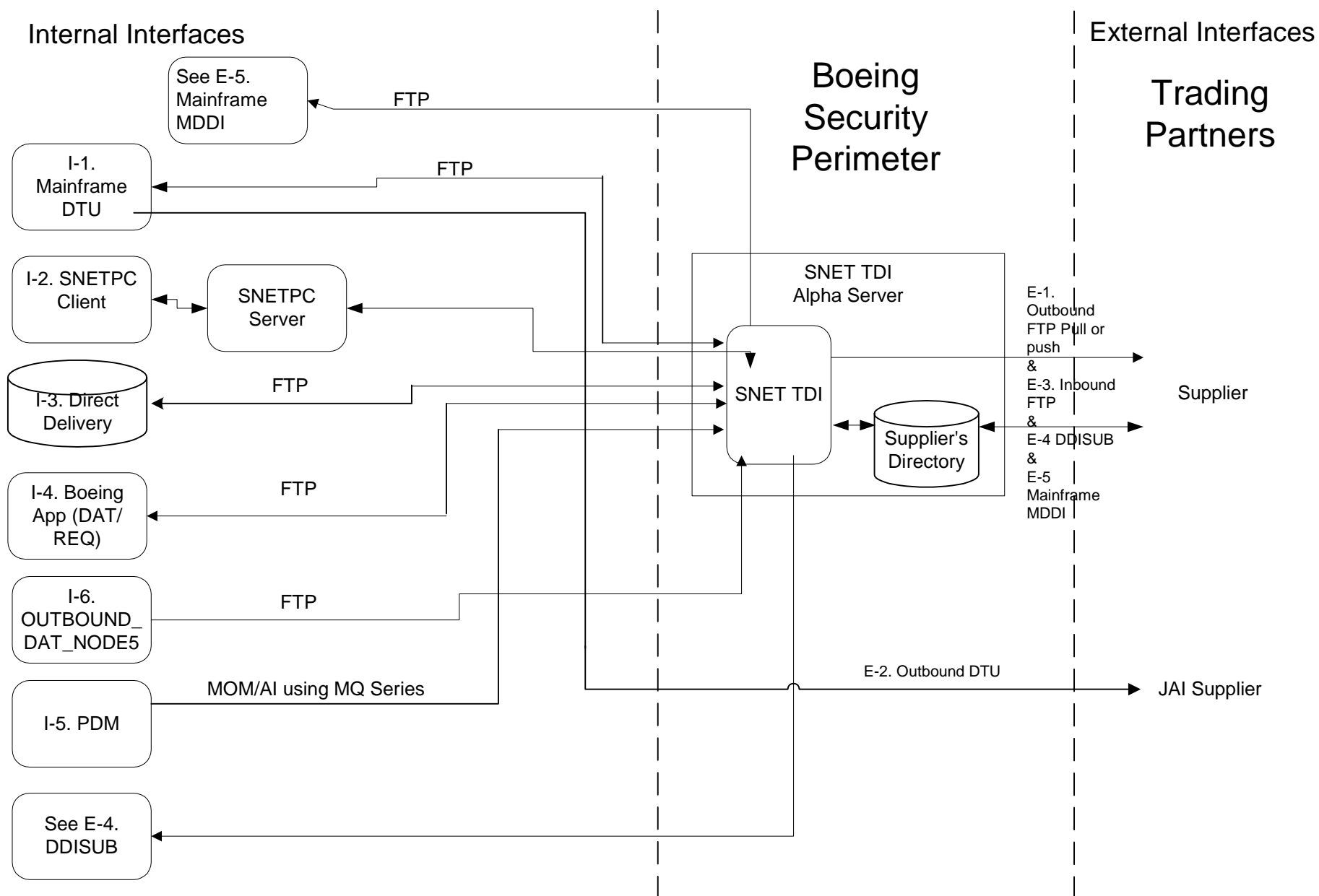
I-1. DTU on IBM Mainframe (Internal Interface)

IBM Mainframe (MVS)   SNET TDI Server (OpenVMS)

Boeing App —JCL— DTU —TCP Socket→ SNET TDI ←move→ Supplier's Directory ←FTP→ Supplier

JCL over FTP

FTP
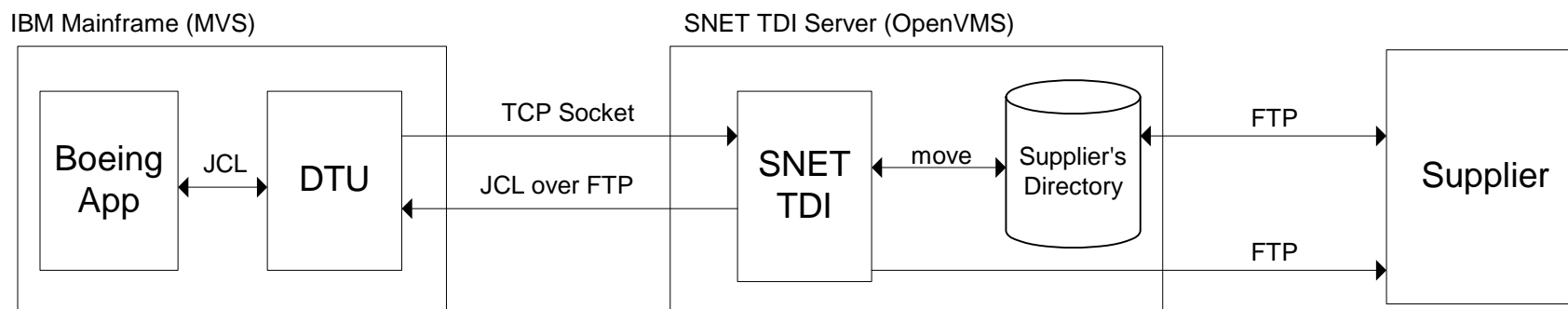
Outbound to Supplier

A. Boeing Application submits JCL to invoke DTU.

B. DTU sends request to TDI using socket program to send file from mainframe to TDI server

C. TDI encrypts and signs file and places the file in the supplier directory on the TDI server or FTPs the file to a secure Boeing account on the supplier machine.

D. Supplier receives and decrypts file.

Inbound from Supplier

A. Supplier encrypts and signs file and FTPs to supplier account on the TDI server.

B. TDI decrypts and submits JCL to invoke DTU.

C. DTU submits application JCL to move file to the mainframe.

I-2. SNETPC (Internal Interface)

Desktop
(WIN2K/NT)

SNET TDI File server
(WIN2K/NT)

SNET TDI
(Open VMS)

Node xyz

Node abc

SNETPC

Drop off
Directory
(IB & OB)

FTP

move

Supplier's
Directory

FTP

SNET
TDI

FTP
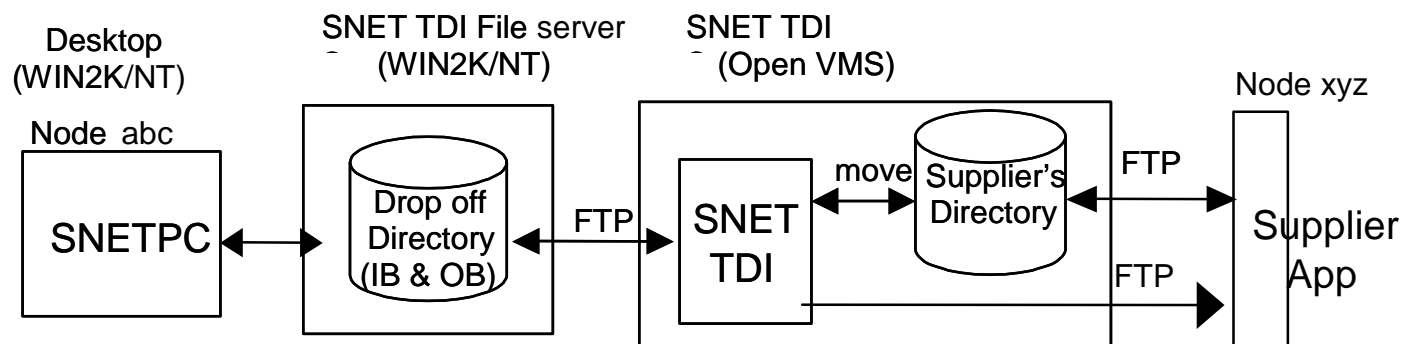
Supplier
App

Outbound to Supplier

A. User runs SNETPC (installed on desktop), selects files and clicks "SEND".

B. SNETPC zips the files into a package and places the package in the SNET TDI outbound drop off staging directory.

C. TDI encrypts and signs the zipped package and either places the package in the supplier directory on the TDI server or FTPs the package to a secure Boeing account on the supplier machine. Sample file names to George on supplier node xyz from David on Boeing node abc:
   bxyz0011_george_abc_david_177143005.zip
   or bxyz0011.zip

D. Supplier receives, decrypts and unzips package.

Inbound from Supplier

A. Supplier creates zipped package, encrypts and signs the package and FTPs to supplier account on the TDI server. Sample file name:
   sabc0021_david_xyz_george_178023503.zip

B. TDI decrypts and delivers package to SNET TDI inbound drop off directory.

C. Boeing user runs SNETPC, clicks "RECEIVE FILES", selects the desired package and clicks "RECEIVE"

SNETPC File Exchange

OUTBOUND:

Any files residing on a Win2Kor NT machine can be sent outbound to suppliers using the SNETPC transfer system. The SNETPC software must be installed on the Boeing user's Win2K/NT desktop.

The user runs SNETPC, and selects any files on any drives—including network drives—to which the user's desktop is attached. When the user clicks "send", SNETPC uses Dynazip to zip all selected files into a package and put them into SNET TDI outbound drop-off directory, as illustrated on the preceding page. The zipped package is encrypted and either placed in the supplier's account on the SNET TDI server or is FTP'd to a secure Boeing account on the supplier machine. The supplier decrypts the file, and unzips the package.

INBOUND:

The process also works in the inbound direction from suppliers to Boeing SNETPC users.

The supplier zips one or many PC files into a package using PKZIP, Dynazip, Winzip, or compatible software. The supplier encrypts and signs the zipped package, and FTPs the encrypted file to Boeing.

SNET TDI decrypts the package and sends it to SNET TDI inbound drop-off directory. The Boeing SNETPC user periodically checks for inbound files. When the file arrives, the user selects it and clicks "receive" to unzip the package into a local directory.

FILE NAME FORMAT:

Suppliers FTPing files to Boeing SNETPC users must use the proper file name format, called the **Long Format with Source Information**, described in section 6B below. This file name format allows multiple users on multiple servers at Boeing to exchange PC files with multiple users on multiple servers at the supplier site. Essential to this file name format are "node codes" and "userids" which are summarized below.

Node Codes

A 3-character **node code** is assigned to each file server at Boeing and at the supplier site that will serve as a source or destination of SNETPC file transfers. Boeing node codes must be unique within Boeing, and supplier node codes must be unique within the supplier site.

Userids

A 1 to 6 character **userid** is assigned to each user (sender or receiver) at Boeing and the supplier site. Userids must be unique within each node. However, two users on different nodes could have the same userid.

Userids for a given node can be assigned using any scheme that provides a unique userid for each user. Userids may contain personal initials, first names, last names, nicknames, arbitrary values, or combinations of these.

I-3. Direct Delivery Outbound and Inbound FTP - DDO & DDI (Internal Interface)
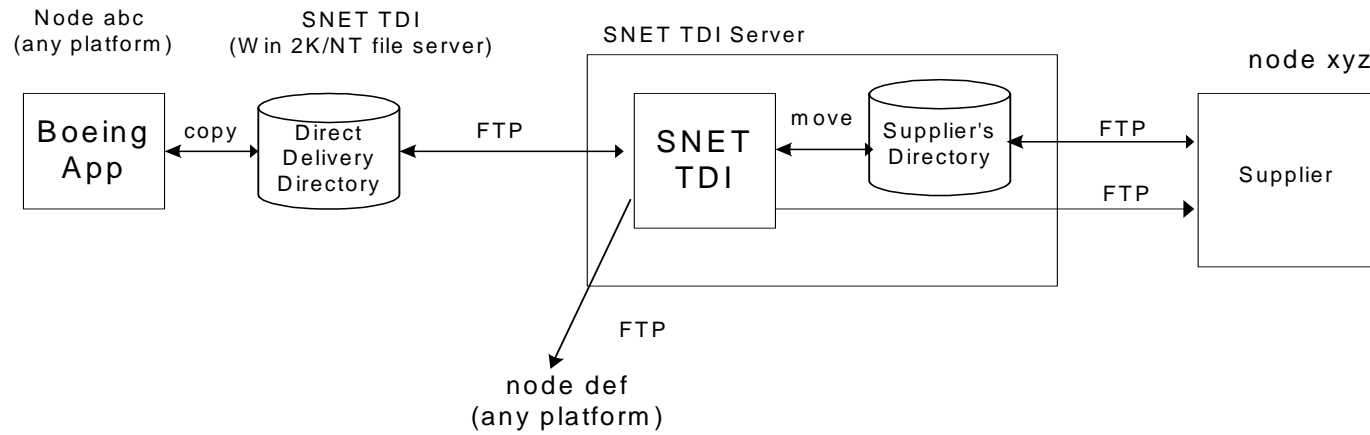
Outbound to Supplier

A. Files are copied to a supplier specific directory on the SNET TDI Direct Delivery (WIN2K/NT) server. Any file name may be used with the exception of the file extension .zip.

B. TDI uses Dynazip to zip together into one package all files found in the directory.

C. TDI encrypts and signs the package then either places the package in the supplier directory on the TDI server or FTPs the package to a secure Boeing account on the supplier machine.

Sample file names to George on supplier node xyz from David on Boeing node abc:
    BXYZ0011_GEORGE_ABC_DAVID_351085355.ZIP
    BXYZ0011.ZIP

D. The supplier downloads the file, decrypts it if necessary and unzips it.

Inbound from Supplier

A. The supplier encrypts and signs the file, if required, and FTPs it to the supplier account on the TDI server. Note that the file does not need to be zipped.

Sample file name: Note that zipped file will have file extension of ZIP regardless of whether file is encrypted or not.
    SDEF0011.TXT
    SDEF0011.ZIP
    SDEF0011*.TXT
    SDEF0011*.zip

* max of 31 additional characters in file name excluding the period and file extension (.txt). Allowable chars are (0-9, a-z, hypen).

Inbound from Supplier (continued from previous column):

B. TDI decrypts if necessary and delivers package to any server that the Boeing group had specified during this interface setup.

Depending on TDI table settings, sample file names delivered to the Boeing group may:

    Same as "From Supplier" file name
    S_DEF_DAVID_suppliercode_XYZ_GEORGE_351085355.txt
    For zipped files: original file names prior to zipping (only on Boeing groups with Windows server)

C. **For Boeing groups with Windows server:** Supplier files that require unzipping (ZIP in Step A) will be renamed when placed on their Windows server directory.

Sample file name as a result of rename:
     DDIUNZIP_200500614540012.ZIP where generated timestamp format is yyyyjjjhhmmssmm

This DDIUNZIP file is strictly used for an audit trail, sorting and identification by the VB Unzip program. The end user should not attempt to access this file. This Dynazip utility is invoked by a TDI UnZip daemon.

TDI uses Dynazip utility for UNZIPPING supplier files.. Once the TDI UnZip daemon processes the DDI UNZIP file, the original file names will be placed on the file server.

THE BOEING COMPANY

I-4. Outbound and Inbound FTP (Internal Interfaces): DAT and REQ files

Node abc (any platform)   SNET TDI Server (OpenVMS)

node xyz

Boeing App — FTP → Boeing App's Directory ← move → SNET TDI ← move → Supplier's Directory — FTP → Supplier ... FTP
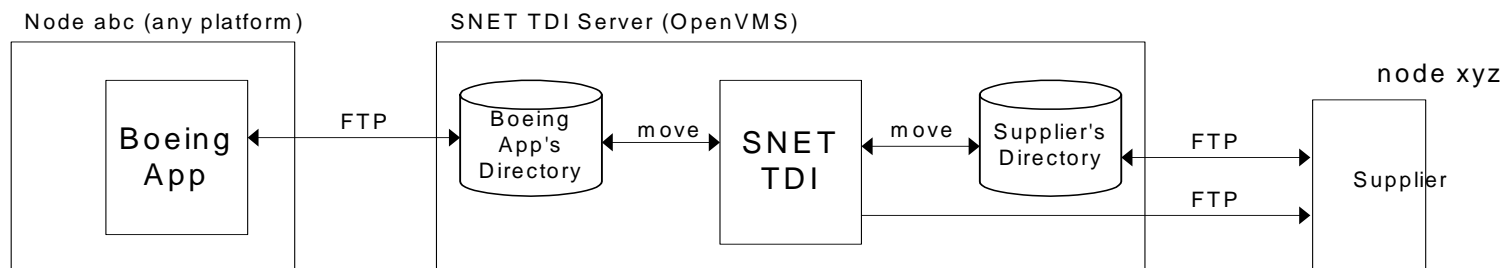
Outbound to Supplier
A. Boeing App has FTP account on SNET TDI server, with default login directory.

B. Boeing App builds "request file" for each data file, and FTPs DAT and REQ pairs to TDI Server. Sample filenames:
        b_abc_david_177143005.dat
        b_abc_david_177143005.req

C. TDI encrypts and signs DAT file and either places the file in the supplier directory on the TDI server or FTPs the file to a secure Boeing account on the supplier machine. Sample filenames:
        bxyz0011.bin
        or bxyz0011_george_abc_david_177143005.bin
        or bxyz0011_some-airplane-drawings.bin

D. Supplier receives and decrypts files.

Inbound From Supplier
A. Supplier encrypts and signs file and FTPs to TDI Server. Sample filenames:
        sabc0021_david_xyz_george_178023503.bin

B. TDI decrypts and delivers DAT and REQ files to Boeing App's default login directory on TDI Server.
        s_abc_david_178023503.dat
        s_abc_david_178023503.req

C. Boeing App FTPs DAT and REQ files from SNET TDI Server.

DAT and REQ Files

As illustrated on the previous page, a Boeing application using the Outbound and Inbound FTP Interfaces will have an FTP account on the SNET TDI server with a default login directory. The Boeing application FTPs outbound files (files sent from Boeing to the supplier) to SNET TDI. SNET TDI encrypts and signs the files and FTPs them to the supplier. The supplier decrypts the files. Likewise, the supplier encrypts and signs files and FTPs them to SNET TDI as inbound files (files sent from the supplier to Boeing). SNET TDI decrypts them and delivers them to the Boeing application's login directory. The Boeing application FTPs inbound files from its login directory.

To send an outbound file to a supplier, a Boeing application transfers **a data file and a matching request file** to the SNET TDI server. The data file is the file to be sent to the supplier. The matching request file is a one-line text file containing addressing information that tells SNET TDI where to send the data file. The names of the data file and matching request file are identical except for the file extension--the data file has a file extension of "dat" and the request file has a file extension of "req". The formats for these file names are described below.

Please note:
1. The Boeing group must first send the complete Data file (DAT file) must be sent to the SNET TDI server and then when the ftp process for the Data file is complete, the Boeing group should send the Request file. If the Request file is received by the SNET TDI server before the Data file, then the file could be processed as an error, and there would be a delay before the error would be resolved.
2. The Request file should be only one line of data, not padded with extra blank lines.

Data File Name Format:
   sender_localnode_localuser_timestamp.dat
Request File Name Format:
   sender_localnode_localuser_timestamp.req

sender	=	1 character sender indicator (b = Boeing is the sender, s = supplier is the sender.)
localnode	=	3 character node code for the local node (Boeing server) that is sending or receiving this file. (Must be a valid node listed in the TDI Node Table.)
localuser	=	1 to 6 character userid for the Boeing employee or application that is sending or receiving this file. (Assigned by Boeing Group.)

timestamp = 9 character timestamp indicating the current time, using the format: jjjhhmmss

         jjj   =   Julian day
         hh   =   hours
         mm   =   minutes
         ss   =   seconds

The timestamp is used to make unique filenames. Therefore, it is essential that the Boeing application never use the same timestamp twice.

Sample File Names:

b_abc_willy_195103501.dat
  outbound data file sent from user willy on Boeing node abc
b_abc_willy_195103501.req
  matching request file

s_rtn_susan_203124505.dat
  inbound data file sent to user susan on Boeing node rtn
s_rtn_susan_203124505.req
  matching request file

Contents of the Request File: The request file will contain one line of text, consisting of the following alphanumeric fields delimited by spaces:

sender localnode localuser suppliercode remotenode remoteuser day time enc datatype transfermode comment

sender   =   same as sender indicator used in filename
localnode   =   same as localnode used in filename
localuser   =   same as localuser used in filename
suppliercode =   1 to 8 character code identifying the supplier that is sending or receiving the data file (must be valid supplier code in TDI Supplier Table and Node Table)

remotenode	=	3 character node code representing the sending or receiving node at the supplier site (assigned by the supplier)
remoteuser	=	1 to 6 character userid for person or application that sent or will receive this file at the supplier site. (assigned by the supplier)
day	=	3 character Julian day, same as value used in filename
time	=	time in hhmmss format, same as value used in filename
enc	=	1 character encryption flag
		0 = software encryption not needed for this file
		1 = software encryption needed for this file
datatype	=	3 character field indicating the type of data being sent (must be valid TDI data type such as txt, bin, doc, cat, cad, mrl, zip, etc.)
transfermode	=	1 character flag indicating binary or ascii transfer mode
		1 = binary mode
		2 = ascii mode
comment	=	1 to 30 characters describing the contents of the file. The comment field is optional. It should consist of alphanumeric characters (0-9, A-Z) and dashes—no spaces or underscores are allowed.

Sample Request Files:

b_abc_willy_195103501.req

    b abc willy 232292 xyz sally 195 103501 1 txt 2 parts-list-for-777

Outbound request file from user willy on Boeing node abc sent to user sally on node xyz at supplier 232292. The file was sent on Julian day 195 at 10:35:01. The data file will be encrypted by SNET TDI. It is a "txt" file transferred in ascii mode, and contains a parts list for the 777.

s_rtn_susan_203124505.req

    s rtn susan 635432 nyc thomas 203 124505 1 cad 1 cadkey-drawings-for-737

Inbound request file sent to user susan on Boeing node rtn from user thomas on node nyc at supplier 635432. The file was sent on Julian day 203 at 12:45:05. The data file was encrypted while in transit to Boeing. It is a "cad" file transferred in binary mode, and contains CADKEY drawings for the 737.

I-5. DCAC/PDM to MOM Interface (Internal Interface): Files from DCAC/PDM through MOM/AI

node xyz

UNIX Server

SNET TDI Server (OpenVMS)

Supplier

PDM

MOM AI

SNET TDI

FTP

DTU Outbound_type Supplier via TDI external interface for Outbound DTU
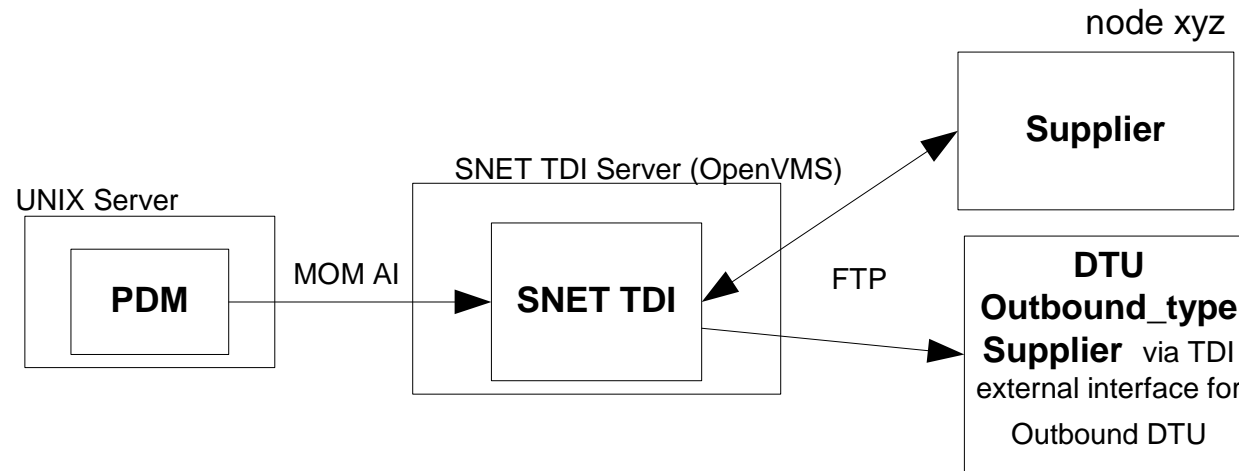
Outbound Supplier Process
A. PDM pushes files to TDI Server using MOM Send.

B. TDI receives files using MOM Receive.

C. TDI encrypts and signs files as needed, and either places the
files in the supplier directory on the TDI server, FTPs the files to
a secure Boeing account on the supplier machine, or sends them
to
DTU for delivery to Snet_to_DTU_outbound_type Suppliers.
Sample filenames (see TDI external interface #7 (Outbound DTU)
for details):
        bxyz0011.stp
   or   bxyz0011_SNETDDAT0301199908301214.stp

D. Supplier receives and decrypts the files.
Data types: STP, PS, PKG, YN.

Internal Boeing Routing for files:
DAT and REQ Files For DCAC/PDM files to SNET to Suppliers.

    As illustrated on the previous page, the DCAC/PDM Boeing application uses the MOM interface to send files to Snet/Tdi for Push, Pull and Dtu-type suppliers. The supplier will be listed in Snet/Tdi tables. Dcac/Pdm sends the file to Snet/Tdi hrough the MOM interface. (files sent from Boeing to the supplier) to SNET TDI.

    To send an outbound file to a supplier, the DCAC/PDM transfers **a data file and a matching request file** to MOM-AI & who sends the file pair to the SNET TDI server. The data file is the file to be sent to the supplier. The matching request file is a one-line text file containing addressing information that tells SNET TDI where to send the data file. The names of the data file and matching request file are identical except for the file extension--the data file has a file extension of "dat" and the request file has a file extension of "req". The formats for these file names are described below.

Data File Name Format:

    sender_localnode_localuser_message-sync-id.dat

Request File Name Format:

    sender_localnode_localuser_message-sync-id.req

    Sample File Names:

    B_PDM_PDMDIS_SNETDDAT0201199916574332.DAT

    Example of req file name:

    B_PDM_PDMDIS_SNETDDAT0201199916574332.REQ

    Filename must follow this format:

sender	=	1 character sender indicator (b = Boeing is the sender, s = supplier is the sender.)
localnode	=	3 character node code for the local node (Boeing server) that is sending or receiving this file. (Must be a valid node listed in the TDI Node Table.) The value used in this case must be: PDM
localuser	=	1 to 6 character userid for the Boeing employee or application that is sending or receiving this file. The value used is PDMDIS
message_sync_id	=	24 character Message Sync Id indicating a unique id with the a date & time stamp, using the format:

    SNETDDATmmddyyyyhhmmssff

SNETDDAT	=	SNETDDAT literal
mm	=	month
dd	=	day
yyyy	=	year
hh	=	hours
mm	=	minutes
ss	=	seconds
ff	=	fraction of second

The message-sync-id is used to make unique filenames. Therefore, it is essential that the Boeing application never use the same message-sync-id twice.

Period-delimiter	=	. (period delimiter separates name from data type)
Data type	=	nnn, where data-type is req for request file, and dat for data file.

Contents of the Request File: The request file will contain one line of text, consisting of the following 12 alphanumeric fields delimited by spaces: All 12 fields are required. The file will fail & send a nak if any one of these 12 fields is not present in the request file.

sender localnode localuser suppliercode remotenode remoteuser day time enc datatype transfermode comment

sender	=	same as sender indicator used in filename
localnode	=	same as localnode used in filename
localuser	=	same as localuser used in filename
suppliercode	=	1 to 8 character code identifying the supplier that is sending or receiving the data file (must be valid supplier code in TDI Supplier Table and Node Table)
remotenode	=	3 character node code representing the sending or receiving node at the supplier site (assigned by the supplier)
remoteuser	=	1 to 6 character userid for person or application that sent or will receive this file at the supplier site. (assigned by the supplier)
day	=	3 character Julian day, same as value used in filename
time	=	time in hhmmss format, same as value used in filename
enc	=	1 character encryption flag
		0 = software encryption not needed for this file
		1 = software encryption needed for this file
datatype	=	3 character field indicating the type of data being sent (must be valid TDI data type such as txt, bin, doc, cat, cad, mrl, zip, etc.)
transfermode	=	1 character flag indicating binary or ascii transfer mode
		1 = binary mode
		2 = ascii mode
		3 = ascii variable mode
message sync id	=	24 characters describing the contents of the file. This field is required.

Example of contents of request file:
b PDM PDMDIS 111111 CLJ ATTNTO 033 015816 1 STP 3 SNETDDAT0201199916574332

In this example, an outbound request file from user PDMDIS on Boeing node PDM sent to user attnto on node CLJ at supplier 111111. Snet/tdi edits the file for valid supplier, data-type and valid message-sync-id.

If the file does not pass these edits, snet/tdi will send a nak back to MOM to DCAC/PDM.

Else if the file does pass the edits, Snet/Tdi will continue to process the file to send to the supplier.

The data file will be encrypted by SNET TDI. It is a "STP" file transferred in ascii variable mode. The message id is: SNETDDAT0201199916574332; this is a unique identifier supplied by DCAC/PDM to Snet/Tdi. The dat file is sent on to DTU, who then sends the file to the receiving DTU who sends the file to the supplier.

I-6. Outbound FTP (Internal Interfaces): OUTBOUND_DAT_NODE5 interface.

Node abc (any platform)   SNET TDI Server (OpenVMS)

Boeing
App
    FTP   Boeing
App's
Directory

move

SNET
TDI

move

Supplier's
Directory

node xyz

FTP

Supplier

FTP
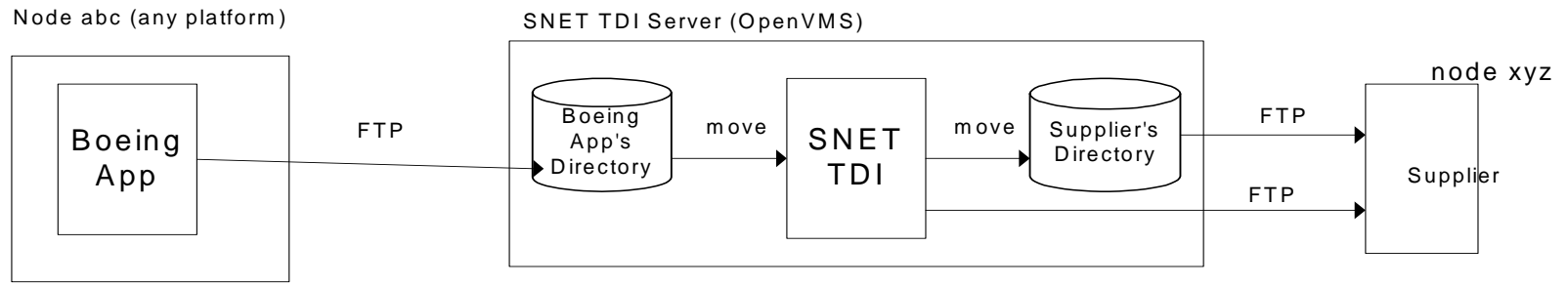
Outbound FTP (Internal Interfaces): OUTBOUND_DAT_NODE5 interface.

A. Boeing App has FTP account on SNET TDI server, with default login directory.

B. Boeing App sends a data file, and FTPs the file to the TDI server.

    Sample filenames:

        0733AA_Model777-2004101204061214.pdf   where the supplier code is 0733AA

        0123BB_Model333-part1.txt   where the supplier code is 0123BB

    Format of filename:

        Field 1. valid TDI supplier code

        Field 2. underscore " _ " character

        Field 3. comments - Value to be determined by Boeing group.

            Allowable alphanumeric characters are 0-9, A-Z, and hypen.

            Total number of characters of field 1, 2, and 3 is not greater than 33 characters.)

        Field 4. decimal point

        Field 5. valid TDI file extension

C. TDI encrypts and signs file and either places the file in the supplier directory on the TDI server or FTPs the file to a secure Boeing account on the supplier machine.

    Sample filenames and format:

        For 1: BXYZ2341_0123BB_Model333-part1.txt

            TDI generates this file name **if the comments value in Step B field 3 is equal or less than 30 characters.**

            Field 1. Letter B

            Field 2. xyz is the supplier node code generated by TDI based on the supplier code

            Field 3. Three character alphanumeric file sequence number generated TDI

            Field 4. Encryption flag – Encrypted data has value 1 (one) and unencrypted data has value 0 (zero)

            Field 5. underscore " _ " character

            Field 6. supplier code from Step B field 1

            Field 7. underscore " _ " character

            Field 8. comments - from Step B field 3.

               TDI will truncate comments value if total number of characters in field 1 through 8 exceeds 39.

            Field 9. decimal point

            Field 10. Valid TDI file extension from Step B field 5.

        For 2: B0381_0733AA_ Model777-2004101204061214.pdf

            TDI generates this file name **if the comments value in Step B field 3 is greater than 30 characters.**

            Field 1. Letter B

            Field 2. Three character alphanumeric file sequence number generated the TDI

Field 3. Encryption flag – Encrypted data has value 1 (one) and unencrypted data has value 0 (zero)
Field 4. underscore " _ " character
Field 5. Supplier code from Step B field 1
Field 6. underscore " _ " character
Field 7. comments - from Step B field 3.
> TDI will truncate comments value if total number of characters in Field 1 through 7 exceeds 39.

Field 8. decimal point
Field 9. Valid TDI file extension from Step B field 5.

D. Supplier receives and decrypts files.

*Note to SNET TDI group: The supplier must be set up for SIF1 and 30 extra characters.

E-1. Outbound FTP (External Interfaces)

Node abc (any platform)   SNET TDI Server (OpenVMS)
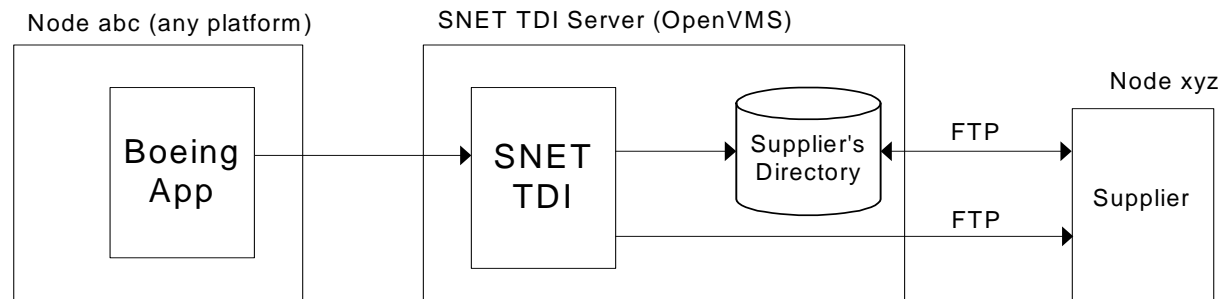
Outbound to Supplier

A. Boeing App sends files to SNET TDI using any internal interface.

B. TDI encrypts and signs files and either moves them to Supplier's directory on SNET TDI Server or FTPs the files to a secure Boeing account on the supplier machine. Sample filenames:
    bxyz0011.bin
    or bxyz0011_george_abc_david_177143005.bin
    or bxyz0011_some-airplane-drawings.bin

C. Supplier receives and decrypts the files.

File Name Formats for Suppliers (External Interfaces)

Three file name formats are available for suppliers who receive files from SNET TDI: (a) the short format, (b) the long format with source information, and (c) the long format with a comment field. These formats are described below. Suppliers may select the file name length (short or long) they want to receive based on their own business needs. Suppliers who elect to receive long file names should be prepared to receive both long formats, because some internal interfaces use source information whereas others use the comment field.

A. Short Format

sdddnnne.ttt

s   =   sender (B = Boeing, S = Supplier)
ddd =   destination node (Boeing node or Supplier Node)
nnn =   unique file id (000 to ZZZ)
e   =   encrytion flag (0 = not encrypted, 1 = encrypted)
ttt   =   data type (CAD, ZIP, BIN, TXT, etc.)

Sender (1 character): Indicates which party is sending the file. The value "B" indicates that Boeing is the sender. The value "S" indicates that the Supplier or Trading Partner is the sender.

Destination Node (3 characters): Contains an abbreviation for the node (machine) that is the ultimate destination of the file transfer. If Boeing is the sender, the destination node will be a Trading Partner node. If the Trading Partner is the sender, the destination node will be a Boeing node. This field is intended to be used for internal routing within the receiving site.

Unique File ID (3 characters): The Unique File ID is a value from 000 to ZZZ, used to ensure unique file names. Each of the three characters is increased from 0 to 9, and then from A to Z. The value increases from '000' to '00Z', then from '010' to '01Z', then from '020' to '02Z', and so on. After '0ZZ' is reached, it increases from '100' to '1ZZ', then from '200' to '2ZZ', and so on. After 'ZZZ' is reached, the entire sequence is repeated beginning with '000'. Filenames are in uppercase on VMS and NT, and lowercase on UNIX. For this reason, the letter 'L' is not used because a lowercase 'l' is easily confused with the number '1'. Likewise, the letter 'O' is not used

because it is easily confused with the number '0'. The rotation from 000 to ZZZ allows for over 39,000 values before the entire cycle is repeated.

Encryption Flag (1 character): Indicates whether the file was encrypted using software encryption. A value of '1' indicates that the file is encrypted. A value of '0' indicates that the file is NOT encrypted.

Data Type (3 characters): Describes the type of data being sent. The values must be valid SNET TDI data types. Some examples are:

C01   CATIA file sent from Trading Partner to Boeing.
C02   CATIA file sent from Boeing to Trading Partner.
I01   IGES file sent from Boeing to Trading Partner.
I02   IGES file sent from Trading Partner to Boeing.
ZIP   Zipped file (PKZIP compatible).
CAD   CADKEY file.
TXT   Generic text file.
STP   STEP file.
PS   Postscript file.

Sample File Names:

bxyz0011.txt   Outbound "txt" file sent to a supplier, to be routed to supplier node xyz. This file is encrypted and signed.
sbga0021.c01 Inbound CATIA file sent to Boeing, to be routed to Boeing node bga. This file is encrypted and signed.

B. Long Format with Source Information

sdddnnne_destuser_sourcenode_sourceuser_time.ttt

s   = sender (B = Boeing, S = Supplier)
ddd   = destination node
nnn   = unique file id

e   = encryption flag (0 = no software encryption, 1 = software encryption)
destuser   = 1 to 6 character user id for recipient
sourcenode = 3 character node id for source node
sourceuser = 1 to 6 character user id for sender
time   = 9 character timestamp in the format jjjhhmmss, where:
                        jjj   julian day
                        hh   hours
                        mm   minutes
                        ss   seconds
ttt   = data type

sdddnnne: Same as short format.

destuser (1 to 6 characters): Userid representing the person or application intended to receive the file.

sourcenode (3 characters): Node id representing the source of the file transfer.

sourceuser (1 to 6 characters): Userid representing the person or application sending the file.

time (9 characters): The timestamp represents the time the file transfer was initiated. It has the form "jjjhhmmss", and contains the Julian day, hours, minutes, and seconds. The sourcenode, sourceuser, and timestamp are used together to identify the file transfer within Boeing. Therefore, each file sent from a given sourcenode and sourceuser must have a unique timestamp.

ttt (3 characters): Same as the data type used in the short format.

Sample File Names:

bxyz0011_george_abc_sally_218123010.zip

Zip file sent from Boeing to a supplier, to be routed to user george on supplier node xyz, from user sally on Boeing node abc. The file is encrypted and signed, and was sent on Julian day 218 at 12:30:10.

sabc0021_sally_xyz_george_219142315.zip

Zip file sent from a supplier to Boeing, to be routed to user sally on Boeing node abc, from user george on supplier node xyz. The file is encrypted and signed, and was sent on Julian day 219 at 14:23:15.

C. Long Format with Comment Field

sdddnnne_comment.ttt

s	=	sender (B = Boeing, S = Supplier)
ddd	=	destination node
nnn	=	unique file id
e	=	encryption flag (0 = no software encryption, 1 = software encryption)
comment	=	1 to 30 characters describing the contents of the file
ttt	=	data type

sdddnnne: Same as the short format.

comment (1 to 30 characters): The comment field is used by the sending application to help the recipient identify or classify the file. It may contain any information agreed to by sender and recipient. It should contain only alphanumeric characters (0-9, A-Z), and dashes. For CATIA files, it often contains an initial segment of the CATIA model number. In other cases, it contains a "package id" used to identify the contents.

ttt (3 characters): Same as the data type used in the short format.

Sample File Names:

bxyz0031_142U3761S12-BD-12_skin_assy.c02

> Encrypted CATIA file sent from Boeing to a supplier, to be routed to supplier node xyz. The comment field indicates that the file contains CATIA model number 142U3761S12-BD-12 which is a Skin Assembly.

bzzz0041_Y5910-173W0010S01-CD-1V1.c02
bzzz0051_Y5910-184W0020S01-BD-1V1.c02

> Two encrypted CATIA files sent from Boeing to a supplier, to be routed to supplier node zzz. The comment fields indicate that both files are part of package Y5910, and each contains a different model number.

sbga0041_142U3761S12-BD-12.c01

> Encrypted CATIA file sent from a supplier to Boeing, to be routed to Boeing node bga. The comment field indicates that the file contains CATIA model number 142U3761S12-BD-12.E2

E-2. Outbound DTU (External Interface)

Unix Server

SNET TDI Server
(OpenVMS)

IBM Mainframe
(MVS)

PDM → MOM/AI → SNET TDI → JCL → DTU → Netview FTP → JAI / DTU outbound type Suppliers
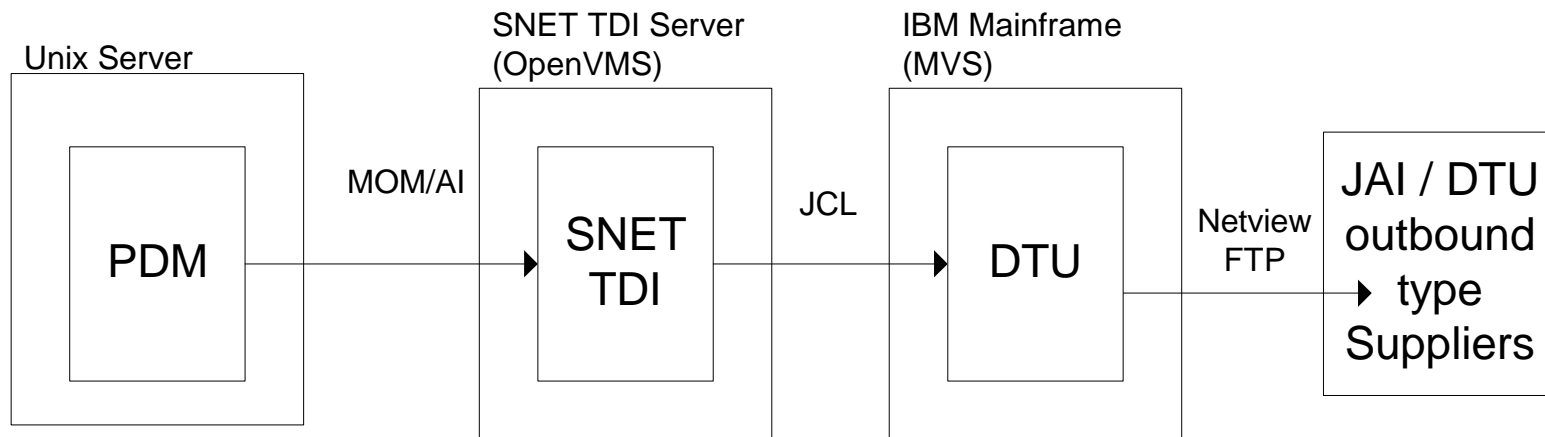
Outbound to JAI Supplier

A.   PDM sends files to SNET TDI through MOM-AI.
B.   SNET TDI submits DTU-TYPE SUPPLIER JCL to DTU.
C.   DTU transfers files to supplier using Netview FTP.

.

Data types: STP, PS, PKG, YN.

Internal Boeing Processing:
DAT and REQ Files For DCAC/PDM files to SNET to Push & Pull type suppliers.

As illustrated on the previous page, the DCAC/PDM Boeing application uses the MOM interface to send files to Snet/Tdi for DTU-type suppliers. The DTU-type supplier will be listed in Snet/Tdi tables. Dcac/Pdm sends the file to Snet/Tdi through the MOM interface. (files sent from Boeing to the supplier) to SNET TDI. SNET TDI sends the files to DTU. DTU sends the files through netview ftp to the supplier. The supplier receives the file, and an acknowledgement is sent to DTU, to Snet/Tdi, to MOM, to DCAC/PDM.

To send an outbound file to a supplier, the Boeing application transfers **a data file and a matching request file** to MOM-AI who sends the file tothe SNET TDI server. The data file is the file to be sent to the supplier. The matching request file is a one-line text file containing addressing information that tells SNET TDI where to send the data file. The names of the data file and matching request file are identical except for the file extension--the data file has a file extension of "dat" and the request file has a file extension of "req". The formats for these file names are described below.

Data File Name Format: sender_localnode_localuser_message-sync-id.dat
Request File Name Format: sender_localnode_localuser_message-sync-id.req
Sample File Names: example of dat file name: B_PDM_PDMDIS_SNETDDAT0201199916574332.DAT
         Example of req file name: B_PDM_PDMDIS_SNETDDAT0201199916574332.REQ
Filename must follow this format:

sender   = 1 character sender indicator (b = Boeing is the sender, s = supplier is the sender.)
localnode = 3 character node code for the local node (Boeing server) that is sending or receiving this file. (Must be a valid node listed in the TDI Node Table.) The value used in this case must be: PDM
localuser = 1 to 6 character userid for the Boeing employee or application that is sending or receiving this file. The value used is PDMDIS
message_sync_id = 24 character Message Sync Id indicating a unique id with the a date & time stamp, using the format:
      SNETDDATmmddyyyyhhmmssff
      SNETDDAT = SNETDDAT literal
        mm = month
        dd = day
        yyyy = year

hh	=	hours
mm	=	minutes
ss	=	seconds
ff	=	fraction of second

The message-sync-id is used to make unique filenames. Therefore, it is essential that the Boeing application never use the same message-sync-id twice.

Period-delimiter   =   .   (period delimiter separates name from data type)

Data type   =   nnn, where data-type is req for request file, and dat for data file.

Contents of the Request File: The request file will contain one line of text, consisting of the following 12 alphanumeric fields delimited by spaces: All 12 fields are required. The file will fail & send a nak if any one of these 12 fields is not present in the request file.

sender localnode localuser suppliercode remotenode remoteuser day time enc datatype transfermode comment

sender	=	same as sender indicator used in filename
localnode	=	same as localnode used in filename
localuser	=	same as localuser used in filename
suppliercode	=	1 to 8 character code identifying the supplier that is sending or receiving the data file (must be valid supplier code in TDI Supplier Table and Node Table)
remotenode	=	3 character node code representing the sending or receiving node at the supplier site (assigned by the supplier)
remoteuser	=	1 to 6 character userid for person or application that sent or will receive this file at the supplier site. (assigned by the supplier)
day	=	3 character Julian day, same as value used in filename
time	=	time in hhmmss format, same as value used in filename
enc	=	1 character encryption flag
		0 = software encryption not needed for this file
		1 = software encryption needed for this file
datatype	=	3 character field indicating the type of data being sent (must be valid TDI data type such as txt, bin, doc, cat, cad, mrl, zip, etc.)
transfermode	=	1 character flag indicating binary or ascii transfer mode
		1 = binary mode

                  2 = ascii mode

                  3 = ascii variable mode

message sync id   =   24 characters describing the contents of the file. This field is required.

Example of contents of request file:

     b PDM PDMDIS 111111 CLJ ATTNTO 033 015816 1 STP 3 SNETDDAT0201199916574332

     In this example, Outbound request file from user PDMDIS on Boeing node PDM sent to user attnto on node CLJ at supplier 111111.   Snet/tdi edits the file for valid supplier, data-type and valid message-sync-id.
If the file does not pass these edits, snet/tdi will send a nak back to MOM to DCAC/PDM.
Else if the file does pass the edits, Snet/Tdi will continue to process the file to send to the supplier.

     The data file will be encrypted by SNET TDI. It is a "STP" file transferred in ascii variable mode. The message id is: SNETDDAT0201199916574332; this is a unique identifier supplied by DCAC/PDM to SNET-TDI. The dat file is sent to the supplier.
When the supplier acknowledges receipt of the file, Snet/Tdi sends an acknowledgement to MOM who sends the ack file to DCAC/PDM.

E-3. Inbound FTP (External Interface)

Three filename formats are available for this interface: (a) the Short Format, (b) the Long Format with Source Information, and (c) the Long Format with Comment Field. These filename formats are the same as those for the external Outbound FTP interfaces described above in sections 6.
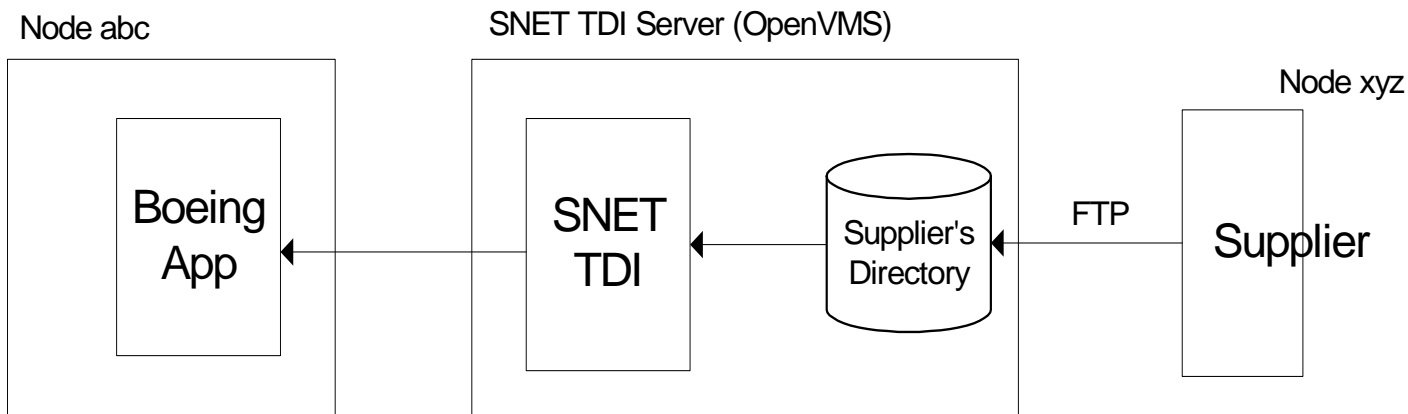
Inbound from Supplier

A. Supplier encrypts and signs files and FTPs them to Supplier's directory on SNET TDI Server.
Sample filenames:
  sabc0011.bin
  or sabc0011_david_xyz_george_177143005.bin
  or sabc0011_some-airplane-drawings.bin

B. TDI decrypts files and delivers to Boeing App on node abc using the internal interface defined for that App.

E-4. Direct Delivery Inbound Sub- Directory (DDISUB) FTP (External Interface)

Supplier Parent directory contains the following logs genterated by TDI for this Sub_Directory process : There are other logs in the directory. For more details regarding all the logs, see the TDI user guide.
  * History_sub_directory.log
  * Ack_sub_directory.log
  The logs will contain lists of files sent by the supplier.

The Supplier Parent directory also contain Sub-directory(s) in which the supplier must put their files to be sent. See the Overall process to the right and the detail process in the following pages.

Supplier's Overall process to put files in their sub-directory:
1. ftp to parent directory
2. change directory to sub directory
3. set correct transfer mode
4. put file to sub directory
5. TDI will process the file and put an entry in the History_Sub_Directory and Ack_Sub_directory logs.

<u>Inbound from Supplier</u>
    A. Supplier prepares the file, encrypts and signs (if encryption is required), and renames the file with the following TDI file naming convention.

        TDI file naming convention rules:
- Valid file name characters are alphanumeric, hyphen, underscore. No blanks or other special characters allowed. Only one decimal or period allowed.
- Unique filenames are preferred otherwise TDI will assign a version number.
- Supplier contact will be given the name of the sub-directory within their parent account. The following are the rules for the types of files to be put into the sub-directory based on a particular string of characters within the sub-directory name:
    1) ASC string (for example – IN_ASC_KENTPRT): Put only ASCII files into this sub-directory with any valid file name and any file extension. (File extension is optional, it can be omitted).
    2) BIN string (for example – IN_BIN_KENTPRT): Put only BINARY or IMAGE files into this sub-directory with any valid file name and any file extension (File extension is optional, it can be omitted).
    3) EXT string (for example – IN_EXT_KENTPRT: Any file type (ASCII or Binary) with a valid file extension in our TDI data type table. File extension for this version is required.

        Sample file name: Mymodel-12.pic

    B. Supplier FTPs to their parent account (dde_xxxxxx) on the SNET TDI server.
    C. Supplier does change directory to the sub-directory, sets the transfer mode to ASCII or Binary. Do not use the auto setting in ftp: you must specify either ASCII or BINARY. Supplier then puts the files into the sub-directory.
    D. TDI decrypts if necessary.

F.   TDI delivers the file to the Boeing group NT or UNIX sub-directory that is assigned to this supplier code.
The Boeing group's sub-directory will either have a suffix of ASC, BIN, or EXT. SNET TDI will deliver the files to the appropriate sub directory for that Boeing group from a particular supplier.

TDI filename format for files sent to the Boeing group's NT or UNIX server:
(note: in this explanation, the + (plus sign) does not appear in the file name. The plus sign is only used to show that these pieces of information are appended together.

supplier's original filename + _ + their file extension if one is given + _ + version number + _ + trantime + _ comment + ** TDI's generated file extension .

** TDI will put either one of these file extensions depending on what sub-directory the supplier had put their file in step C. (.txt for ascii files,.bin for binary files, valid TDI file extension for files in the ext directory)

Example of supplier's original filename from step A –
In this example, the supplier had sent files with the same name four times, and this file is the 4th file with that filename. (version 4).
Mymodel-12.pic;4

Example filename sent to Boeing Group's NT or UNIX server
Note that TDI appends the version number to the supplier's original file name. This example indicates that this is version 4 of a file with the same file name of other files in the supplier's sub-directory.

Mymodel-12_pic_4_200416608110013_comment.txt

Using TDI filename format explained above, the following are the values used in this example:
- supplier's original filename is Mymodel-12
- original file extension is pic
- version number is 4
- trantime is 200416608110013

  Trantime is a unique date/time field that TDI will append to the file to help keep the filenames unique and provide history and tracking.

- comment is comment

  Comment is an optional field that allows the supplier and Boeing group to share information about the file. If a comment is specified, the comment will be included in ALL files for that supplier to this Boeing group. Its value must be coordinated between the supplier and Boeing group then put into our TDI table.

- TDI's generated file extension is .txt   (txt for asci,.bin for binary files, for files to ext directory, use given data type extension.)

History_sub_directory.log: The supplier parent directory will have this log that shows the supplier what files were processed.
An Ack_sub_directory.: This log is also generated by TDI. At this time, it will contain the same information as the History_sub_directory.log.

Example of an entry in the history_sub_directory.log for supplier code SUPP23:

```
supp23 FILE TRANSFERS WITH BOEING:  Jul  6 2004 08:49 TO Jul 12 2004 13:42 d
---------------------------------------------------------------------------------------------------------------`
Prefix   Typ  Date Delivered    Size        Application Data ID                                   Status Date Removed       d
---------------------------------------------------------------------------------------------------------------`
SDIR WAK TXT Tue Jul  6 09:09:14 000000001668 BPHP1ZN1_IGES-RAINBOW-MODEL-IGES3-TEST_I01_4_2004188090900120.TXT       KENTPRT  `
SDIR WAK TXT Tue Jul  6 09:09:16 000000000512 TEST_TXT_1_2004188090900220.TXT                              KENTPRT  `
```

For the first file in this sample log, the original file would have been:
```
BPHP1ZN1_IGES-RAINBOW-MODEL-IGES3-TEST.I01;4   (Version 4)
```

The second file would have had an original file name of:
```
TEST.TXT;1 (Version 1)
```

E-5.   Mainframe Direct Delivery Inbound: MDDI (external interface)

The supplier puts a file in his supplier directory on the SNET TDI server, with a data type extension agreed upon by SNET TDI, the Boeing customer, and the supplier.

The filename delivered to the mainframe for the Boeing customer will be a static filename, pre-agreed to by the Boeing customer and SNET TDI.

Node abc IBM
MAINFRAME

SNET TDI Server (OpenVMS)

node xyz

Boeing
App

FTP

SNET
TDI

move

Supplier's
Directory

FTP
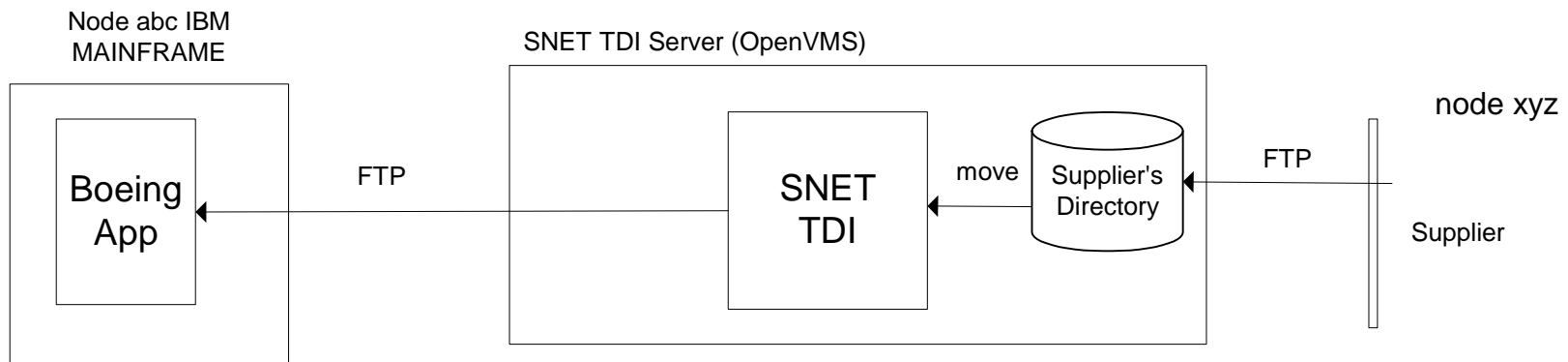
Supplier

Inbound from Supplier

The supplier can use the naming convention of the free filename formats available to this interface:

(a). short format

(b). long format with source information

(c). long format with comment field.

These filename formats are the same as those for the external outbound FTP interfaces described above in section 6. SNET TDI delivers the inbound files to the mainframe specified in the filename, using a name agreed to between the Boeing Customer and SNET TDI. The Boeing customer can use OPC to notify them that the file has been delivered to the mainframe.

A. supplier encrypts and signs files and FTPs (using ascii mode for ascii files, binary mode for binary files). FTP the files to the Suppliers's directory on SNET TDI server.

    Sample filename: SABCI0031.WIR

                    SABC2241_david_xyz_george_214131221.wir

                    SABC2251_some-airplane-drawing.wir

B. Example of supplier ftp command:

      FTP tdi.boeing.com

      Account

      Password

      Ascii   *(for ascii files,   binary for binary files)*

      Put   supplier_filename.txt   sabc2251_some-airplane-drawing.wir

C. SNET TDI stores the mainframe filename in the SNET TDI appl table.

D. SNET TDI decrypts the file, if needed.

E. Example of the static filename delivered to the Boeing customer, to the mainframe:

    `DATALIB.WIRS.TEST.SUPPL23.AWTFEED`

NOTE: this is a static filename – the filename delivered to the Boeing customer will always be the same static filename for that supplier and that data type extension. All three of the filenames sent by the supplier as noted in section A, would have this same name delivered to this Boeing customer and this supplier for the data type extension of WIR.

++

APPENDIX B: BOEING LIMITED Customized Password Form (when information is filled in)

To assist you in keeping track of your SNET TDI - related information, I am providing you with the following form to help you record this important information for your company.

Important: Password information is considered BOEING LIMITED.
You must store the following information in a secure, locked area, accessible to authorized personnel only.

==

This is my FTP userid(s) and password(s) on the SNET TDI system on domain tdi.boeing.com:
          For Seattle (dde_   **)** _____
          For Wichita (dde_   **)** _____

If applicable, Boeing will be pushing to: IP address   _____
                            Account name _____
                            Password   _____

My PGP PASSPHRASE is: _____

==

KEY RING BACKUP: File name _____
                   is stored on (media type as floppy, zip drive disk, tape, etc) _____
                   in location (where it is stored) _____

   Important: Once you have created your PGP key pair and added your Boeing public key, please backup your PGP key ring files (public and private/secret key ring files) onto diskette or tape. This will enable you to easily recover your PGP key ring in the event you ever need to restore PGP on your system.

   For WIN95/NT Version 5.5.x of PGP (or higher), the key ring files created when you generated your key ring are called: PUBRING.PKR & SECRING.SKR. These are the 2 files you need to copy onto disk or tape and store in a locked, secure area, along with the PASSPHRASE information.

==
Supplier focal change

   Since the SNET TDI group maintains a list that identifies the primary and backup focals at each supplier site who are authorized to receive FTP account/password information, it is imperative that suppliers notify us whenever there is a "focal" change and/or address, email, phone number change. If you are no longer responsible for the SNET TDI electronic connection for your company, please call the SNET TDI Technical Support LINE and provide updated information concerning any focal changes.

   As the primary focal, you are our single point of contact for your company. You are responsible for any communication between SNET TDI and your company and for ensuring that the backup knows where your paper copy info regarding SNET TDI is located, the SNET TDI FTP account & password, the SNET TDI's account/password on your machine (if Boeing pushes data to you), your company's PGP passphrase, location of this email, location of the PGP keyring backup file, and all the functions that you perform to exchange data with the SNET TDI system.

Our designated primary SNET TDI password focal is: _____

Our designated backup SNET TDI password focal is: _____

BOEING LIMITED
(when information is filled in)
++

Appendix C: SNET TDI Comment, Questions, and Corrections

--------------------------------------- *<fold>* ---------------------------------------

_____

_____

_____

_____

_____

_____

_____

_____

Note: Please be as specific as you can so that your information will be interpreted correctly. Thank you!

Originator: (optional): _____Phone (optional): _____

--------------------------------------- *<fold>* ---------------------------------------

_____

_____

_____

place
stamp
here

STEVE C. PERRY
Boeing Commercial Aircraft Group
P.O. Box 3707, #MS 67-HJ
Seattle, WA   USA   98124-2207