



Companion Guide – Electronic Data Interchange Communications

Library Reference Number: CLEL10010

Document Management System Reference: Companion Guide – Electronic Data Interchange Communications (17841)

Address any comments concerning the contents of this manual to:

EDS Publications Unit
950 North Meridian Street, Suite 1150
Indianapolis, IN 46204
Fax: (317) 488-5169

EDS and the EDS logo are registered marks of Electronic Data Systems Corporation.

EDS is an equal opportunity employer, m/f/v/d.

Copyright © 2005 Electronic Data Systems Corporation. All rights reserved

Current Dental Terminology (CDT) (including procedures codes, nomenclature, descriptors, and other data contained therein) is copyrighted by the American Dental Association. ©2002, 2004 American Dental Association. All rights reserved. Applicable Federal Acquisition Regulation System/Department of Defense Acquisition Regulation System (FARS/DFARS) apply.

Current Procedural Terminology (CPT) is copyright 2004 American Medical Association. All rights reserved. No fee schedules, basic units, relative values, or related listings are included in CPT. The AMA assumes no liability for the data contained herein. Applicable FARS/DFARS restrictions apply to government use.

© 2001-2005 TNS, Inc. © 2002-2004 Transaction Network Services, Inc. All rights reserved. Terms and Conditions : TNS-related marks, logos, and product names, are trademarks of Transaction Network Services, Inc.

*“MOVEit” “MOVEit Freely” and “MOVEit DMZ” are trademarks of Standard Networks, Inc.
Copyright © 2002-2004 by Standard Networks.*

Revision History

Document Version Number	CO	Revision Date	Revision Page Number(s)	Reason for Revisions	Revisions Completed By
Version 1.0		August 2004	All	New document. Formerly sections 2 and 3 of companion guides.	Systems/HIPAA Publications
Version 1.1		April 2005	2-2, 2-3	Updated Tables 2.1 and 2.2	Systems/HIPAA Publications
Version 1.2		May 2005	2-1 to 2-4	Additional information needed in the FTP over SSL and FTP over SSH.	Systems/HIPAA Publications
Version 1.3	295	July 2005	1-1, 1-2, Table 1.1, 2-1, 2-2 Tables 2.1, 2.2	To correct Communication Options and available data ports in the Communication Guide.	Systems/Publications

Table of Contents

Section 1: Introduction.....	1-1
Overview	1-1
Communication Options	1-1
Section 2: Batch Submission – Secure FTP	2-1
File Exchange	2-1
FTP over SSL.....	2-1
FTP over SSH	2-4
HTTP over SSL - Web interChange	2-6
Section 3: Interactive Submission	3-1
POS Device Communications Process	3-1
Protocols	3-2
Communication Formats.....	3-2
DASS Inbound	3-4
DASS Outbound	3-4
TNS Inbound.....	3-4
TNS Outbound.....	3-4
IHCP Inbound	3-4
IHCP Outbound	3-4
Detailed Communication Formats	3-5
TNS Input.....	3-5
TNS Output.....	3-6
IHCP Input	3-6
IHCP Response	3-7
DASS Response	3-7
TNS Response.....	3-8
Routing Response Codes	3-8
Swipe Card Layout	3-9
Index	I-1

Section 1: Introduction

Overview

Trading partners with the Indiana Health Coverage Programs (IHCP) have options for transmitting data electronically. The Electronic Data Interchange (EDI) communication guide identifies the choices available for submitting and receiving transaction data and provides specific details for each option.

Communication Options

Inbound batch transactions and outbound transactions and reports are exchanged through secure File Transfer Protocol (FTP). Additionally, some transactions can be submitted interactively. *Section 2: Batch Submission* of this guide contains information about submitting batch transactions and *Section 3: Interactive Submission* contains information about sending interactive transactions.

The following table identifies submission options available for each transaction.

Table 1.1 – Transaction Options

Transaction	Options	
	Secure FTP	Interactive
837I Health Care Claim Institutional	X	
837P Health Care Claim Professional	X	
837D Health Care Claim Dental	X	
835 Remittance Advice (RA)	X	
270/271 Eligibility Benefit Inquiry and Response	X	X
276/277 Claim Status Request and Response	X	X
278 Prior Authorization (PA) Request for Review and Response	X	
834 Managed Care Member Enrollment Roster	X	
834 Primary Care Case Management (PCCM) – Benefit Enrollment and Maintenance	X	
820 Managed Care Capitation Payment Reporting	X	
820 PCCM – Payroll Deducted and Other Group Premium Payment for Insurance Products	X	

All incoming files, such as the 837, 270, 276, and 278 requests, must be wrapped in a compliant interchange envelope. See *Section 3* of the appropriate transaction companion guide for specific instructions.

Section 2: Batch Submission – Secure FTP

File Exchange

File Exchange is an application provided by the Indiana Health Coverage Programs (IHCP) for secure file processing, storage, and transfer. File Exchange is designed to safely and securely collect, store, manage, and distribute sensitive information between IHCP and its trading partners. Web browsers and no- or low-cost secure FTP clients, which are required to transfer files, can quickly, easily, and securely exchange files with File Exchange over encrypted connections using the FTP over SSL (FTPS), FTP over SSH (SFTP), and HTTP over SSL (HTTPS) protocols. Typically, those trading partners that wish to interact systematically with File Exchange (via a batch script) will choose one of the two FTP methods listed above. If a trading partner intends to interact with File Exchange in a manual, or ad-hoc manner, then the HTTPS method (using Web interChange) will be the most desired method.

For data file submission, in addition to accepting normal text files, File Exchange can also accept compressed files submitted in ZIP format. The file name that is submitted must have .zip at the end of the file name. The zip file can contain a single file or multiple files. When these files are processed, File Exchange will extract all files from the ZIP archive and process them as though they were submitted individually. There are no restrictions related to submitted file names other than those for ZIP files discussed above. Any meaningful file name can be chosen by the trading partner. All submitted files must be uploaded to the /Distribution/HIPAA Transactions folder.

All outbound files available for download are created individually with the following naming convention: SSSS.TTT.X.HHMMSS.JJJ (where SSSS = trading partner ID, TTT = transaction type, X = transmission type – always an X, HHMMSS = hours/minutes/seconds, and JJJ = Julian date). All outbound report files available for download are also created individually with the following naming convention: SSSS.TTT.rpt.X.HHMMSS.JJJ (where SSSS = trading partner ID, TTT = transaction type, X = transmission type – always an X, HHMMSS = hours/minutes/seconds, and JJJ = Julian date). Outbound files are not available in a compressed or ZIP format. All outbound files will be placed in the trading partner's home folder. These files will remain available for retrieval for 30 days after they first become available unless they are explicitly deleted from File Exchange by the trading partner.

FTP over SSL

The first File Exchange batch transmission option is FTP over SSL. The following documentation is designed to assist developers with customizing secure FTP clients using FTP over SSL to enable connectivity to File Exchange. File Exchange fully supports a large number of secure FTP clients using FTP over SSL including the following:

- AS/400 native FTPS client
- C-Kermit (command-line, v8.0+, VMS, Linux, Unix, Solaris, and so forth.)
- Cute FTP Pro (GUI, version 1.0 and higher)
- Glub FTP (GUI, Java 2.0 and higher)
- IP*Works SSL (API, Windows, version 5.0)
- LFTP (command-line, Linux, Unix, Solaris, and so forth.)
- MOVEit Buddy (GUI)

- MOVEit Freely (command line)
- NetFinder (GUI, Apple)
- NetKit (command-line, Linux, Unix, Solaris, and so forth.)
- OpenIT (Unisys V-Series, A-Series, Clearpath)
- SmartFTP (GUI, version 1.0 and higher)
- SurgeFTP (command-line, Solaris, and so forth.)
- WS_FTP Pro (GUI, version 7.0 and higher)

The important pieces of information that are needed no matter which FTP over SSL client is used are listed below. Consult the documentation for your specific FTP client to determine how to configure these settings. If the machine that is initiating the FTP connection resides behind a firewall, the firewall must be configured to allow outbound traffic on any of the ports listed below.

- Host – xfile.indianamedicaid.com
- Control Connection Ports
- 990 if using implicit encryption (recommended)
- 21 if using explicit encryption
- Data Connection Ports – 3000-3100 (any port in this range)
- Transfer mode – Passive (Active mode transfers will not be accepted)

The following examples were tested using the MOVEit Freely[®] command-line client in a Windows environment. Note that in these examples, the *mput*, *mget* and *mdelete* commands were used with a file mask to process multiple files at a single time. Not all secure FTP clients support these commands. It is recommended that the FTP client used to communicate with File Exchange support these commands. If an FTP client that does not support these multiple file commands is used to communicate with File Exchange, then the sample scripts will need to be modified to create multiple *put*, *get*, and *delete* statements that are input into the FTP client. Check the documentation for the specific FTP client being used for more information on commands supported by the FTP client. *Figures 2.1* and *2.2* are examples of data file submission and retrieval using FTPS.

```

@echo off
rem * * * * *
rem * Example DOS batch script that will copy all files
rem * containing a certain file mask from
rem * a local directory to File Exchange.
rem * (via secure FTP over SSL using MOVEit Freely)
rem *
rem * Usage:
rem * "putfiles (username) (password) (filemask)"
rem * ex. putfiles john123 mypass *.*
rem * * * * *
echo cd "/Distribution/HIPAA Transactions" > temp.txt
echo prompt >> temp.txt
echo mput "C:\temp\upload\%3" >> temp.txt
echo quit >> temp.txt
ftps -e:implicit -a -user:%1 -password:%2 -s:temp.txt xfile.indianamedicaid.com
del temp.txt

```

Figure 2.1 – Data File Submission Using FTPS

```

@echo off
rem * * * * *
rem * Example DOS batch script that will get all files
rem * containing a certain file mask from a user's
rem * File Exchange home directory and save them to
rem * the current local directory.
rem * (via secure FTP over SSL using MOVEit Freely)
rem *
rem * Usage:
rem * "getfiles (username) (password) (filemask)"
rem * ex. putfiles john123 mypass *.*
rem * * * * *
echo cd /Home/%1 > temp.txt
echo prompt >> temp.txt
echo mget %3 >> temp.txt
rem ** Optional: Uncomment line below to delete the files from File Exchange
rem **           after they are retrieved
rem echo mdelete "%3" >> temp.txt
echo quit >> temp.txt
ftps -e:implicit -a -user:%1 -password:%2 -s:temp.txt xfile.indianamedicaid.com
del temp.txt

```

Figure 2.2 – Data File Retrieval Using FTPS

FTP over SSH

Another File Exchange batch transmission option is FTP over SSH. The following documentation is designed to assist developers with customizing secure FTP clients using FTP over SSH to enable connectivity to File Exchange. File Exchange fully supports the most popular secure FTP clients using FTP over SSH including the following:

- F-Secure SSH (command-line, 3.2.0 Client for Unix)
- OpenSSH SFTP (command-line, Unix)
- OpenSSH for Windows (command-line, Windows)
- PSFTP/PSCP (command-line, Windows)
- SSH Communcations SSH Secure Shell FTP (GUI, Windows)
- WS_FTP (GUI, Windows)

The important pieces of information that are needed no matter which FTP over SSH client is used are listed below. Consult the documentation for your specific FTP client to determine how to configure these settings. If the machine that is initiating the FTP connection resides behind a firewall, the firewall must be configured to allow outbound traffic on the port listed below.

- Host – xfile.indianamedicaid.com
- Port – 22 (this is the default SSH port)

The following examples were tested using the PSFTP/PSCP command-line client. Note that the standard commands included with FTP over SSH clients do not include the multiple file commands (mput, mget, and mdelete) used in the SSL examples above. To retrieve or send multiple files at a time, use the Secure Copy (SCP) feature of SSH. *Figures 2.3 and 2.4* are examples of data file submission and retrieval using SCP.

```
@echo off
rem * * * * *
rem * Example DOS batch script that will copy all files
rem * containing a certain file mask from
rem * a local directory to File Exchange.
rem * (via secure Copy over SSH using PSCP)
rem *
rem * Usage:
rem * "putfiles (username) (password) (filemask)"
rem * ex. putfiles john123 mypass *.*
rem * * * * *
pscp -sftp -l %1 -pw %2 -batch -q C:\upload\%3
      xfile.indianamedicaid.com:/Distribution/HIPAA Transactions
```

Figure 2.3 – Data File Submission Using SCP

```

@echo off
rem * * * * *
rem * Example DOS batch script that will get all files
rem * containing a certain file mask from a user's
rem * File Exchange home directory and save them to
rem * the a local directory.
rem * (via secure Copy over SSH using PSCP)
rem *
rem * Usage:
rem * "getfiles (username) (password) (filemask) "
rem * ex. putfiles john123 mypass *.*
rem * * * * *
pscp -sftp -l %1 -pw %2 -batch -q xfile.indianamedicaid.com:/Home/%1/%3
C:\download

```

Figure 2.4 – Data File Retrieval Using SCP

To delete all files retrieved from File Exchange, the script must create a text file with the delete command for each file that was retrieved. *Figures 2.5 and 2.6* are examples of text files and the scripts to execute the delete commands.

```

del 997.124733.223.123456
del 997.152317.224.136723
del 997.144403.225.139932

```

Figure 2.5 – Example Text File with FTP Delete Commands

```

@echo off
rem * * * * *
rem * Example DOS batch script that will execute FTP
rem * commands contained in a text file against files in a user's
rem * File Exchange home directory.
rem * (via secure FTP over SSH using PSFTP)
rem *
rem * Usage:
rem * "delfiles (username) (password) (command_file) "
rem * ex. delfiles john123 mypass C:\download\delete.txt
rem * * * * *
psftp -l %1 -pw %2 -batch -b %3 xfile.indianamedicaid.com

```

Figure 2.6 – Data File Deletion Using SFTP

HTTP over SSL - Web interChange

The final File Exchange batch transmission option is Web interChange. All trading partners can log on to Web interChange using the same ID and password that is used to access File Exchange in the FTP methods listed above. This ID only has permission to access File Exchange. It cannot access the other functions of Web interChange. Accessing File Exchange via Web interChange allows each trading partner to pick up or drop off files outside of an automated script. If there is an additional file that needs to be sent to the IHCP, or if a response file is lost and needs to be retrieved again, these types of ad-hoc transmissions can be done using Web interChange. By logging on to Web interChange, the trading partner must adhere to the password requirements of Web interChange including changing passwords every 90 days. If it has been more than 90 since the password was changed, Web interChange prompts the trading partner to change the password. This may cause any automated FTP scripts to not connect to File Exchange. If the password is changed in Web interChange, the same change must be applied to any automated scripts to ensure uninterrupted service.

A *File Exchange Help* document is available upon connection to Web interChange. This document contains detailed instructions for using File Exchange through Web interChange.

Section 3: Interactive Submission

All interactive transactions are routed through the EDS/Delivery and Support System (DASS) corporate electronic transaction processing facility in Auburn Hills, MI. Transactions are then routed to the Indiana Health Coverage Programs (IHCP) operation in Indianapolis, where responses are prepared, returned to Michigan, and ultimately returned to the requester. EDS has contracted with Transaction Network Services® (TNS) to provide service for point of service (POS) transaction routing from the provider to Auburn Hills, MI. Commercial switching companies also have direct links into the EDS Michigan facility.

As mentioned above, TNS provides X.25 Network telecommunication services between the provider and the EDS corporate switching facility. Transactions routed through TNS are transmitted at a maximum speed of 2400 bps. Configure modems using the following settings:

- Data Bits = 7
- Parity = Even
- Stop Bits = 1

The TNS telephone number for submitting interactive transactions is 9505829. There is no service charge for using this number.

Note: It is not necessary to dial 1 + area code, 1, or 800 before the TNS telephone number.

The communications process required for transmitting ANSI X12 request transactions from a POS device to the IHCP and transmission of the response X12 transaction to the POS device follows. This document describes communications through TNS using a POS device. Entities connecting directly to DASS through X.25 circuits in Auburn Hills, MI should refer only to the sections describing data and communications with DASS.

POS Device Communications Process

1. Message is sent from the POS device to TNS using phone line (TNSInput)
2. Message is sent from TNS to EDS/DASS using X.25 circuits (DASSInput)
3. Message is sent from EDS/DASS to EDS/IHCP using TCP connection (IHCPInput)
4. Transaction is processed by EDS/IHCP (ANSI X12 270/271 Transaction)
5. Response is sent from EDS/IHCP to EDS/DASS using TCP connection (IHCPReply)
6. Response is sent from EDS/DASS to TNS using X.25 circuit (DASSReply)
7. Response is sent from TNS to POS Device using phone line (TNSReply)

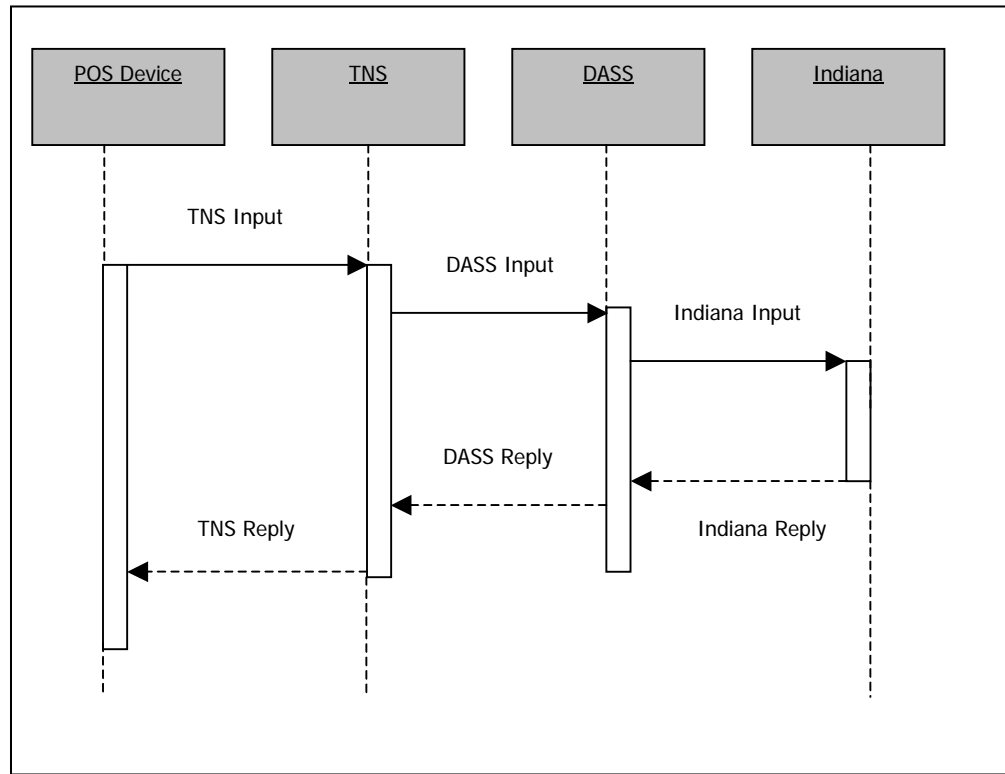


Figure 3.1 – POS Device Communications Process

Protocols

- TNS Input/Output (VISAI)
- DASS Input/Output (X25 24-byte header to be returned with response)
- IHCP Input/Output (TCP/IP)

Communication Formats

Refer to the previous process steps and *Figure 3.1* indicating the format at given process steps.

High-level communication formats used in the process and detailed definitions of individual components are as follows:

- TNSInput:** <STX>TNSHeader IHCP Header | X12Message(270)<ETX><LRC>
- DASSInput:** <STX> IHCP Header | X12 Message(270) <ETX><LRC>
- IHCPInput:** <ML>DASSHeader | IHCP | X12Message(270)
- IHCPREPLY:** <ML> DASSHeader | X12Message(271)
- DASSReply:** <STX><RC>X12Message(271)<ETX><LRC>
- TNSReply:** <STX><RC>X12Message(271)<ETX><LRC>
- X12Message:** ANSI X12 270/271 transaction.

<STX> binary character 02

<ETX>binary character 03

<LRC> Longitudinal Redundancy Check byte

<ML> Message Length (two-byte binary integer), number of bytes in the message. The two-byte length field is not included in the length calculation.

<RC> Reply Code (two-byte binary numeric)

Table 3.1– Header Formats

Note: All values are in binary text

Header Formats and Values				
Start Position	Length	Value	Field Name	Required By
TNS Header				
1	5	edsin	Routing Code	TNS
6	2	10 – Production 12 – Testing	Port Code	TNS
EDS Header				
1	4	INEV	Txn code	EDS/DASS
5	2	10	Version	EDS/DASS
7	2	IN	State Code	EDS/DASS
9	6	000001 – Assigned for testing Unique terminal number is assigned for production.	Terminal Number	IHCP
DASS Header				
1	24	Binary-HEX	DASSHeader	EDS/DASS

DASS Inbound

- Use the first five bytes after the <STX> character for routing messages. For IHCP Eligibility, the routing code is INEV0.
- Strip off three bytes from the VISAI protocol: (<STX>, <ETX>, <LRC>)
- Add a 24-byte header, that must also be present in the return packet for routing.
- Maintain open connection with TNS until the outbound reply is sent, or a timeout within DASS disconnects.
- Determine routing to test or production based upon the incoming circuit. This does not change from current processing.

DASS Outbound

- Strip off 24-byte header
- Add three bytes for VISA1 protocol (<STX>, <ETX>, <LRC>)
- Send response message to the open channel with TNS

TNS Inbound

- Strip off seven-byte TNSHeader recalculate LRC

TNS Outbound

- None

IHCP Inbound

- Strip off <ML>
- Strip off DASSHeader and save
- Process Transaction

IHCP Outbound

- Attach DASSHeader saved from the inbound transaction
- Set <RC> Value
- Build <ML>

Detailed Communication Formats

TNS Input

Table 3.2 describes the format for Health Information Portability and Accountability Act (HIPAA)-compliant inbound data sent to TNS for use by the IHCP.

Table 3.2 – Inbound Data Format

Inbound Data Format				
Start Position	Length	Value	Field Name	Required By
1	1	Binary '02'	<STX>	VISA Protocol
TNS Header				
2	5	edsin	Routing Code	TNS
6	2	10 – Production 12 – Testing	Port Code	TNS
EDS Header				
8	4	INEV	Txn code	EDS/DASS
12	2	10	Version	EDS/DASS
14	2	IN	State Code	EDS/DASS
16	6	000001 – Assigned for testing. Unique terminal number is assigned for production.	Terminal Number	EDS/Indiana
X12Message				
22	15978		Message	HIPAA
Variable	1	Binary '03'	<ETX>	VISA Protocol
Variable	1		Longitudinal Redundancy Check	VISA Protocol

TNS Output

Table 3.3 describes the format for outbound transactions sent by the TNS system to the EDS system in Auburn Hills, MI.

Table 3.3 – Outbound Data Format

Outbound Transaction Data Format				
Start Position	Length	Binary '02'	<STX>	VISA Protocol
1	1	Binary '02'	<STX>	VISA Protocol
DASSHeader				
2	24	Binary-HEX	DASS Header	EDS/DASS
EDSHeader				
26	4	INEV	Txn code	EDS/DASS
30	2	10	Version	EDS/DASS
32	2	IN	State Code	EDS/DASS
34	6	Assigned	Terminal Number	EDS/Indiana
X12Message				
40	15960		Message	HIPAA
Variable	1	Binary '03'	<ETX>	VISA Protocol
LastCharacter	1		Longitudinal Redundancy Check	VISA Protocol

IHCP Input

Table 3.4 describes the information sent from the Auburn Hills system to the IHCP.

Table 3.4 – Auburn Hills to IHCP Data Format

Auburn Hills Data Format				
Start Position	Length	Value	Field Name	Required By
1	2	Binary	Two-byte length	EDS/DASS
DASSHeader				
3	24	Binary-HEX	DASS Header	EDS/DASS
EDSHeader				
35	6	000001 – Assigned for testing Unique terminal number is assigned for production.	Terminal Number	EDS/Indiana
X12Message				
41	15959	270	Message	HIPAA

IHCP Response

Table 3.5 describes the IHCP response to Auburn Hills.

Table 3.5 – IHCP to Auburn Hills Data Format

IHCP Response Format				
Start Position	Length	Value	Field Name	Required By
1	2	Binary	Two-byte length	EDS/DASS
DASS Header				
3	24	Binary-HEX	DASS Header	EDS/DASS
X12 Response				
27	15971		X12 271 response	HIPAA

DASS Response

Table 3.6 describes the DASS response format.

Table 3.6 – DASS Response Format

DASS Response Format				
Start Position	Length	Value	Field Name	Required By
1	1	Binary '02'	<STX>	Visa Protocol
Reply Code				
2	2	NN	Txn code (Numeric)	EDS/DASS
X12Message				
4	15996		271 Message	HIPAA
Variable	1	Binary '03'	<ETX>	VISA Protocol
Last Character	1		Longitudinal Redundancy Check	VISA Protocol

TNS Response

Table 3.7 describes the format of the message sent to the terminal device or remote system.

Table 3.7 – TNS Response Format

TNS Response Format				
Start Position	Length	Value	Field Name	Required by
1	1	Binary-STX '02'	<STX>	VISA Protocol
Reply Code				
2	2	NN	Error code (Numeric)	EDS/DASS
X12Message				
4	15996		271 Message	HIPAA
Variable	1	Binary '03'	<ETX>	VISA Protocol
LastCharacter	1		Longitudinal Redundancy Check	VISA Protocol

Routing Response Codes

The routing response is a two-character field, returned by the routing systems between the terminal and the EDS host. These response codes are returned for any interactive transaction. Defined values are listed in the Table 3.8.

Table 3.8 – Routing Response Codes

Routing Response Codes	
Value	Description
00	Success
01	Device handler returning scheduled download time
02	Device handler returning region parameters
10	POS device error - no response from device
11	POS device error - communication error
12	POS device error - protocol timeout
13	Line Handler timeout waiting for reply from bridge
20	Host not available
21	Wrong software version running on POS device
40	Timeout waiting for foreign host to reply
42	No available slots in host process
44	Invalid transaction type - unable to route
50	Timeout waiting for server class to reply

Table 3.8 – Routing Response Codes

Routing Response Codes	
Value	Description
51	No available slots in bridge process
52	Invalid transaction type – no known server class
53	Pathway send error
54	Server Class not available (all busy)
55	Timeout waiting for host response
60	Host not available
61	No SVC or PVC available (all busy)

Note: No response is sent for receipt of a partial transaction.

Swipe Card Layout

Providers have the option of using a swipe card device to read the magnetic information from a member ID card. Information is encoded on Track 1 according to the ISA 7813 standards. The maximum length of Track 1 data is 76 bytes. The magnetic strip on the plastic card is encoded as shown in Table 3.9.

Table 3.9 – Magnetic Strip Encoding

Name	Length	Position	Value
Start Sentinel	1	001-001	ASCII "%"
Format Code	1	002-002	"B"
BIN	6	003-008	610467
RID	12	009-020	021-021
Field Separator	1		ASCII "^"
Member Last Name	Variable *		
Name Separator	1		ASCII "/"
Member First Name	Variable *		
Member Middle Initial	1		
Field Separator	1		ASCII "^"
Expiration Date	4		YYMM format
Service Code	3		
Card Number	3		
End Sentinel	1		ASCII "?"

** The total characters for the combination of the member last name and member first name cannot exceed 41.*

Sample encoding:

`%B610467999999999999^DOE/JOHN J^9412120123?`

B		L	
Batch submission.....	2-1	Layout	
C		Swipe card	3-9
Communication formats	3-2, 3-5	M	
Communication options	1-1	Magnetic strip encoding	3-9
D		P	
DASS.....	3-1	Point of service, <i>See POS</i>	3-1
Inbound	3-4	POS device.....	3-1
Outbound.....	3-4	Protocols	3-2
Response	3-7	R	
Response format.....	3-7	Revision history	i
Deliver.....	3-1	Routing response codes.....	3-8
F		S	
File Exchange.....	2-1	Secure file transfer protocol, <i>See SFTP</i>	1-1
FTP over SSH.....	2-4	SFTP	1-1
FTP over SSL.....	2-1	Batch submission	2-1
H		Swipe card	
HTTP over SSL.....	2-6	Layout.....	3-9
I		Magnetic strip encoding.....	3-9
IHCP		T	
Inbound	3-4	Table of contents	iii
Input	3-6	TNS	3-1
Input format.....	3-6	Inbound	3-4
Outbound.....	3-4	Inbound format	3-5
Response	3-7	Input.....	3-5
Response format.....	3-7	Outbound	3-4
Index.....	I-1	Outbound format.....	3-6
Interactive submission	3-1	Output	3-6
Introduction		Response	3-8
Overview.....	1-1	Response format	3-8
L		Transaction Network Services, <i>See TNS</i>	3-1
M		Transaction options	1-1
P		W	
R		Web interChange.....	2-6
S			
T			
W			

