

2	DATA COMMUNICATIONS	2-2
2.1	GENERAL	2-2
2.2	ENCRYPTION	2-2
2.3	USER IDENTITY	2-2
2.4	THE ADMINISTRATION OF AUTHORIZATION	2-2
2.4.1	<i>Central authorization administration (CA)</i>	2-2
2.5	AUTHORIZATION CHECK IN CONJUNCTION WITH 3270 COMMUNICATION	2-2
2.6	AUTHORIZATION CHECK IN CONJUNCTION WITH NON-3270 COMMUNICATION	2-2
2.7	ONLINE PRINTERS	2-3
2.8	COMMUNICATION VIA FILE TRANSFER.....	2-3
2.8.1	<i>FTP</i>	2-3
2.8.2	<i>NetviewFTP</i>	2-3
2.9	COMMUNICATION VIA MQ.....	2-4
2.9.1	<i>Name standard</i>	2-4
2.9.2	<i>Local receiving queue at VPC</i>	2-4
2.9.3	<i>Remote queues at VPC</i>	2-5
2.9.4	<i>Values in MQMD headers</i>	2-5
2.9.5	<i>Values in MQIHH header</i>	2-7
2.9.6	<i>Overview</i>	2-8

2 DATA COMMUNICATIONS

2.1 General

VPC's computer equipment is the host system for the data communication network that forms the basis of the VPC system. The network is FrameRelay-based, with an inbuilt redundancy which embraces VPC and all the AOs.

2.2 Encryption

In accordance with VPC's policy regarding the security of data communications, the communication connections in VPC's external network shall, at the basic protection level, provide a reliable protection against change. Fixed passwords may not be sent over the network in plain text.

In order to meet these security demands, VPC has chosen to protect all data traffic by the use of encryption. All communication links from AOs that wish to connect up to VPC's central data system are therefore encrypted with communication equipment that VPC provides and for which VPC retains responsibility.

2.3 User identity

VPC makes it possible for external users to choose, within given limits, a user identity according to its own organisation standards.

2.4 The administration of authorization

The administration of protected resources is handled by VPC, whereas the processing of users and their authorization is handled either by VPC or by each AO respectively.

2.4.1 Central authorization administration (CA)

VPC's central authorization administration is the function that deals with the protection of transactions and the grouping of offices for those AOs that have chosen access control at the office level.

2.5 Authorization check in conjunction with 3270 communication

An authorization checking system (RACF) exists in VPC's computer system. A user check occurs when logging on. Access control occurs at the transaction level. A check is made that the user is authorized to make the requested transaction and that the required VPC account belongs to the user's AO. All users, both at VPC and at the AO, are defined in VPC's authorization checking system.

2.6 Authorization check in conjunction with non-3270 communication

In the case of application-to-application communication between AO and VPC, only limited authorization checks are made centrally at VPC. One requirement, therefore, for enabling interactive communication with VPC other than by 3270 is that the AO in question possesses an authorization system that is in every way equivalent to that of VPC.

Where interactive communication is concerned, VPC checks that the information is coming from an authorized AO, using a communications connection designed for that AO, and in which the information is encrypted in the manner specific to that AO. This provides an assurance that no unauthorized person may gain access to VPC's central data system. Furthermore, there is a check in the application programs to ensure that the AO's user is entitled to receive a reply to the enquiry made or to make the update requested.

As can be seen from the term description in the transaction header that must accompany any such communication, there must be information in the transaction to VPC for identifying the person who has generated the transaction at the AO. Such information is not used by VPC for identification and authorization checking, but is stored for use in the event of a possible follow-up.

As regards interactive communication by other means than via 3270, VPC presumes that the AO takes over responsibility for the required authorization check and that this is conducted to at least the same extent as occurs at VPC in conjunction with 3270 communication.

2.7 Online printers

Printers can be directly connected online to the VPC system, on condition that they emulate in accordance with the protocol defined in SNA for printers of type LU1 or LU3.

Whenever a printer is to be connected up to the VPC system, the network group at VPC must be contacted.

2.8 Communication via file transfer

There are two different types of file transfer to VPC; FTP (IP) and NetviewFTP (SNA).

2.8.1 FTP

For customers to be able to connect up to VPC's FTP server, VPC makes the following demands:

- that the FTP client is run from an IP address authorized by VPC
- that the FTP client must be able to perform in the passive mode

VPC's FTP server

IP address (Prod): 194.132.134.82

IP address (Test): 194.132.134.81

Port no: 5021

Protocol: IP

From VPC, the customer receives a userid and a password for logging on to the FTP server. After logging on, the customer is linked up to its own home library where the file is placed according to the following format:

File name.P

File name = no limitation on appearance

P = environment code for Prod

Code page for file transfer via VPC's FTP server shall be ISO88591 according to ANSI standard. This applies both in to VPC and out from VPC.

If you have any enquiries relating to the above, please contact VPC's network group.

2.8.2 NetviewFTP

For customers to be able to connect up to VPC's NFTP server, VPC makes the following demands:

The LU-name used by the customer must be known in the VPC system.

VPC's NFTP server

LU name: SEVPCNP1 (Receiving)

LU name: SEVPCNP2 (Sending)

Protocol: LU6.2

The appearance of the file name, etc. can be found in chapter 3.

If you have any enquiries relating to the above, please contact VPC's network group.

Transactions to the computer-to-computer queue are placed in a separate processing queue at a calmer pace. The purpose is to achieve a shorter queuing time for real time transactions.

2.9.3 Remote queues at VPC

For those services that generate data to an AO, VPC sets up remote queues based on the incoming requests from AOs. This does not, however, apply to enquiry-reply from an AO. VPC can set up only one remote queue at most per service that the AO subscribes to. It is up to the AO to choose whether more than one service is to use the same remote queue or not.

2.9.4 Values in MQMD headers

Field name	When customer creates trans and VPC replies	When VPC creates trans
StrucId	MQMD-STRUC-ID	MQMD-STRUC-ID
Version	MQMD-VERSION-1	MQMD-VERSION-1
Report	According to choice. Steers reportmsg, processing of dead-q and how msgid and correlid are to be processed when VPC replies. MQRO-NEW-MSG-ID MQRO-PASS-MSG-ID MQRO-COPY-MSG-ID-TO-CORREL-ID MQRO-PASS-CORREL-ID MQRO-DEAD-LETTER-Q MQRO-DISCARD-MSG	MQRO-NONE
MsgType	MQMT-REQUEST VPC always gives an answer.	MQMT-DATAGRAM VPC does not require an answer.
Expiry	MQEI-UNLIMITED. If a limited duration is desired for the message, this is expressed in 1/10's second	MQEI-UNLIMITED
Feedback	MQFB-NONE	MQFB-NONE
Encoding	MQENC-NATIVE	MQENC-NATIVE
CodedCharSetId	MQCCSI-Q-MGR	MQCCSI-Q-MGR
Format	MQFMT-STRING (VPC itself creates an IIH header if necessary on the incoming message). If the customer specifies an IIH header this field must be filled in with MQFMT-IMS.	MQFMT-STRING or MQFMT-IMS
Priority	MQPRI-PRIORITY-AS-Q-DEF	MQPRI-PRIORITY-AS-Q-DEF
Persistence	MQPER-PERSISTENT MQPER-NOT-PERSISTENT if logging of msg is not desired. Default on incoming queue at VPC is always PERSISTENT.	MQPER-PERSISTENT
MsgId	According to choice. Preferably MQMI-NONE so that a unique id is generated by MQ.	MQMI-NONE
CorrelId	According to choice. VPC replies according to the Report field.	MQCI-NONE
BackoutCount	0	0
ReplyToQ	Name of local queue to which the reply from VPC is to be sent.	blank
ReplyToQmgr	Own qmgr name.	blank
UserIdentifier	Valid user ID at VPC. The same user ID will be returned in the reply. A different user ID can be obtained in the reply if the field ID-TERMINAL-USER in the transaction header of the incoming message is set at a non-blank value. Then that user ID will be returned instead in the reply.	Valid user ID at the customer according to the customer's own choice.
AccountingToken	Not used by VPC.	generated by MQ

Field name	When customer creates trans and VPC replies	When VPC creates trans
ApplIdentityData	Reserved for VPC.	blank
PutApplType	Not used by VPC.	generated by MQ
PutApplName	Not used by VPC.	generated by MQ
PutDate	Should be set by MQ.	Set by MQ.
PutTime	Should be set by MQ.	Set by MQ.
ApplOriginData	Not used by VPC.	generated by MQ

2.9.5 Values in MQIIH header

It is not necessary for the customer to create this header on messages to VPC. VPC will generate the header as required if it is missing. If the customer uses a header on messages to VPC, it should look like the examples in the table below. VPC will consequently let the header remain in place in its reply to the customer.

In those cases where the customer requests an MQIIH header on messages created at VPC, VPC will create a header like those shown below.

Field name	Value
Strucid	MQIIH-STRUC-ID
Version	MQIIH-VERSION-1
Struclength	MQIIH-LENGTH-1
Encoding	MQENC-NATIVE
Codedcharsetid	MQCCSI-Q-MGR
Format	MQFMT-IMS-VAR-STRING
Flags	MQIIH-NONE
Ltermoverride	space
MFSmapname	space
Replytoformat	MQFMT-IMS-VAR-STRING
Authenticator	MQIAUT-NONE
Traninstanceid	MQITII-NONE
Transtate	MQITS-NOT-IN-CONVERSATION
Commitmode	MQICM-COMMIT-THEN-SEND
Securityscope	MQISS-CHECK
Reserved	space

2.9.6 Overview

