FUJ00001624

Post Office Limited

Network Banking Engine

NBE - Horizon Application Interface Specification

Status : Baseline
Version : 2.0c

Version as of February 15, 2002
Printed: April 18, 2002

Author: Jo Down

IBM Global Services
South Bank
76 Upper Ground
London
SE1 9PZ

GRO

Email: GRO

IBM Confidential
ICL Pathway Confidential

Document Control

FUJ00001624

Revision History

Version Number	Revision Date	Summary of Changes	Changes Marked
00.01	21/08/01	Initial draft. This replaces any previously issued interface specification relating to the Horizon – NBE interface.	No
00.02	30/08/01	Update following workshop on data flows with Post Office Limited and ICLP. Also corrections from IBM review.	No
00.03	14/09/01	Update following 2nd workshop with Post Office Limited and ICLP.	No
00.04	21/09/01	Corrections from IBM review.	No
00.05	12/10/01	Update from Post Office Limited and ICLP formal review (see separate file for detailed responses to comments)	No
00.06	19/10/01	Update following approval workshop	No
00.06A	13/11/01	Update following meeting with Bob Booth	Yes
00.07	14/11/01	Update following workshop with ICLP and Post Office Limited	Yes
00.08	15/11/01	Update following comments received on version 00.07	Yes
1.0	16/11/01	Baseline	No
1.1	14/01/02	Update following CR26 Removal of MQ and CR27 Removal of S messages and ICLP comments post version 1.0	No
1.2	28/01/02	Update following ICLP and POL comments and review meeting 23/1/02	No
1.3	5/2/02	Update following ICLP and POL comments	No
1.4	6/2/02	Update following review meeting 6/2/02	No
2.0	8/2/02	Baseline	No
2.0a	11/2/02	Comments incorporated for 2.0	No
2.0b	12/2/02	Comments incorporated for 2.0a	Yes

Please ensure that this document is current. Printed documents and locally copied files may become obsolete due to changes to the master document. The source of the document can be found in the IBM Lotus Notes Project Control Book.

Review status and approvals

This document will require approval from the following before being baselined:

Name	Title
Carl Binnion	IBM Project Manager
Torstein Godeseth	Post Office Limited TDA
Bill Reynolds	ICL Horizon Project Manager

Distribution

This document will be distributed to the following when baselined:

Name	Title
The IBM Project Team	
The Post Office Limited Project Team	
The ICL Horizon Project Team	
The eFunds Project Team	

FUJ00001624

Outstanding Issues
The following issues affect this document, which will require updating when the issues are resolved:

Number	***Description***	***Issue Status and Date***
1.	When the rate of requests received from Horizon exceeds a Maximum, the NBE must respond to sufficient [R] Messages with a [suitable A] Message without passing the [R] Message to a host such that the total rate of Messages being passed to a host a maximum.	The NBE will not monitor the instantaneous transaction rate but if the processing capabilities of the machine are exceeded messages will be queued and subject to delay. Old messages will automatically be declined. 6/2/02 Open Issue – with POL to agree satisfactory response. Due 22/02/02.
2.	Fallback area requires expansion	Raised 6/2/02 Future Work required. POL to define specific requirements. Due 22/2/02
3.	Regarding: 3b) 3.1 has AS but does not define special characters; indeed how do we cope with text with - as yet undefined - reserved characters? I do not believe the clarification on the fourth bullet addresses the "As" and non-binary encoded data. Are there restrictions that, for instance, "<<<Great Credit Deals>>>" would be OK as footer text? etc.	Raised 12/02/02 Future decision required IBM/POL Due 22/2/02
4.	Regarding: 3c) 3.1.1 Is the XML carrying binary or BASE64 encoded binary? This referred to the third bullet in the notes around CDATA.	IBM Due 22/2/02
5.	what fields are duplicated for a second balance. I had assumed Bal, Type, Amt and /Bal giving my 50. In Bob's calculation he has Balce, Bal, /Bal and /Balce giving 26 difference of 24. The fields which are needed for a second balance need to be clarified/agreed.	IBM/POL Due 22/2/02

FUJ00001624

Table of Contents

FUJ00001624

FUJ00001624

FUJ00001624

1 Introduction

1.1 Purpose

The document has been produced by IBM for Post Office Limited as a deliverable from the work defined in the Statements of Work[1], [4], [6].

The purpose of this document is:

- To specify the interface between the NBE and Horizon (Campus)
- To provide the development teams with sufficient detail to develop the NBE - Horizon interface
- To provide a basis of contractual boundaries, and SLA measurement points
- To provide a consistent communications vehicle amongst the development teams that have responsibility for developing the various components comprising the application.

1.2 Scope

This document applies to the interface between the NBE and Horizon Campus only. It includes only those financial transaction messages, network messages, reconciliation and settlement messages sufficient to support the financial products being delivered to Post Office Limited in the first release.

The IBM Application Architect, IBM Business Analyst, Post Office Limited Application Architect, ICL Pathway Application Architect, LINK Application Architect and the IBM, eFunds and ICLP Development Team members should read this document.

This AIS is concerned only with the application messages exchanged over the interface between NBE and Horizon. It does not include system management or the interfaces with LINK and other Financial Institutions. The technical interface between the NBE and Horizon will be specified in a Technical Interface Specification Reference [3].

1.3 Structure

This AIS document follows Post Office Limited's AIS standard Reference [7].

Section 2 contains a high level overview of the Horizon – NBE interface and its context.

Section 3 contains a detailed description of the messages to be exchanged.

Section 4 contains details of the data transfer.

Section 5 contains details of security of the exchanged data items. This section identifies the security needed for data items (e.g. encryption) and details of the method to be used.

Section 6 contains relevant details of any operational procedures relating to the interface.

Section 7 contains response code data and discrepancy response code data

FUJ00001624

1.4 Terms and Abbreviations

See NBE Programme Glossary at Reference [9]

1.5 References

Please note that where no version is specified in the table below, the latest version is assumed.

1.	Title	PONWB – Statement of Work for Requirements Analysis
	Version	01.00
	Date	2 February 2001
	Author	IBM
2.	Title	NB Volumetrics
	Version	2.0A
	Date	
	Author	Post Office Limited
3.	Title	PONWB – Horizon-NBE Technical Interface Specification
	Version	1.03
	Date	02 February 2002
	Author	IBM
4.	Title	PONWB – Statement of Work for Initiate Design Phase
	Version	01.00
	Date	24 September 2001
	Author	IBM
5.	Title	NBE-Horizon Operational Level Agreement
	Version	
	Date	TBD
	Author	TBD
6.	Title	PONWB – Statement of Work To Initiate Phase 0
	Version	01.00
	Date	2 January 2002
	Author	IBM
7.	Title	PONWB - Application Interface Specification Template
	Version	
	Date	
	Author	POL
8.	Title	IBM/POL NBE Functional Solution Definition
	Version	under construction
	Date	
	Author	IBM
9.	Title	NBE Programme Glossary
	Version	1.3
	Date	
	Author	POL

FUJ00001624

2 Overview of the Interface

2.1 Data Description

The following messages are exchanged over the Horizon - NBE interface:

Message Type	Description	Direction
[R2]	Authorisation / Financial Transaction Request: • balance enquiry • withdrawal • withdrawal with balance • withdraw limit • deposit • PIN change	Horizon -> NBE
[A2]	Authorisation/Financial Transaction Request Response: • balance enquiry response • withdrawal response • withdrawal with balance response • withdraw limit response • deposit response • PIN change response Each of the above will have a response code that indicates approve or decline with reason and any required action (e.g. card retention).	NBE -> Horizon
[C2]	Priority confirmation sent: • Where clerk has declined the transaction where [A] Approve has been received at the counter • Where the counter times out as no [A] has been received by the counter [C2] messages are only generated for financial transactions ie not for Balance Enquiries or PIN Change transactions.	Horizon -> NBE

FUJ00001624

[C4]	Confirmation See 3.2.4 for scenarios where this message is generated. [C4] messages are only generated for financial transactions ie not for Balance Enquiries or PIN Change transactions.	NBE	->	Horizon
[D]	Reconciliation Exception. See 3.2.5 for scenarios where this message is generated. [D] messages are only generated for financial transactions ie not for Balance Enquiries or PIN Change transactions.	NBE	->	Horizon
[KT]	Security Key Test	Horizon	->	NBE
[KA]	Security Key Acknowledge	NBE	->	Horizon
[PS]	Echo Test Initiated by Horizon at regular intervals to determine if NBE system is still available. NBE will reply immediately with [PR] message below. The context of [PR]/[PS] messages is local between the Agent and the NBE and has no further end-to-end significance.	Horizon	->	NBE
[PR]	Echo Test Reply	NBE	->	Horizon

Each message will include fields that ensure both the consistency of the interfaces (version number) and the security of sensitive data (message authentication codes and working keys).

2.2 Derivation and Use of Data

2.2.1 Intra-Day

The messages listed above are generally exchanged, as a result of a transaction generated, by either a user at a Post Office outlet, or by LINK/Financial Institution. NBE does not generally initiate messages; rather it acts as a message router, and transforms received messages into the appropriate format for the next system in the message sequence. The following table shows the derivation and use of each banking transaction message exchanged between Horizon and NBE in terms of the received message that causes each Horizon - NBE message to be exchanged, and the transmitted message resulting from the Horizon - NBE message exchange. The shaded columns indicate the systems and connecting interface addressed by this AIS.

Message Sequence						
Horizon Outlet		**Horizon Campus**		**NBE**		**LINK or Financial Institutions**
	[R1] →		[R2] →		[R3] →	
	← [A3]		← [A2]		← [A1]	

FUJ00001624

[C0] →			[C2] →		[E1] → or No message	
					← [E2]	

2.2.2 End of Day - File Transfer

At the end of the day a batch file, relating to reconciliation and settlement messages, is generated. This file is created independently of real time processing, by message matching during settlement. These messages are derived as follows:

- Reconciliation Exception Message [D] – this message informs Horizon that there will be a reconciliation difference and a manual adjustment may be necessary. The reasons for generating a [D] message are described in section 3.2.5
- [C4] – This message informs Horizon of the NBE view of all Financial transactions received during the current Business day where the NBE believes that Horizon and the NBE are aligned. The scenarios where a [C4] is generated are described in section 3.2.4.

The structure and delivery of this file is detailed in section 4.8.

2.2.3 Security Messages

Security key exchange messages are initiated by Horizon and acknowledged by NBE.

The following table shows the derivation and use of each security message exchanged between Horizon and the NBE.

Security Message Sequence						
Horizon Outlet		**Horizon Campus**		**NBE**		**LINK or Financial Institutions**
			[KT] →			
			← [KA]			

Key Test, KT, and Key Acknowledgement, KA, messages are only issued when the Acquirer Zone Master Key, AZMK, is changed. This will normally happen once every six months. The NBE may receive KT messages from all prime and backup Horizon NBS Agents. NBE must respond to all KT messages it receives with a KA message returned on the same connection. The first KA response returned by the NBE will trigger promotion of the new AZMK to current AZMK. The new AZMK promotion will be communicated to all NBE PIs and the new key will be used for MAC creation of responses to all subsequent messages sent by the NBS Agents to NBE. The old key AZMK will continue to be known to the NBE in order to perform cryptographic functions on messages constructed using the old AZMK that remain in enqueue for the NBE.

If no response is received to any KT message sent by the NBS Agents operator intervention will be required to resolve the problem and retry the key test.

2.2.4 Echo Test Messages

The Horizon Agents have identified a need for sending periodic Echo Test messages to the NBE, to check that other applications are in a working state including valid keys, even if there is no business traffic (eg in the middle of the night). Two further messages have been introduced for this :-

a) [PS] Echo Test
b) [PR] Echo Test Reply

(The PS message will be sent to NBE at a configurable interval, at a time to be defined in the OLA).

FUJ00001624

The NBE should be listening for [PS] messages at all times (as it does for [R2] messages) and should respond with a [PR] message as soon as possible to the Horizon Agent, that initiated the PS message. These messages are very similar to the KT and KA messages identified by Key management. A common structure is defined, though separate message types are maintained to simplify processing.

The following table shows the derivation and use of each security message exchanged between Horizon and the NBE.

Echo Test Message Sequence						
Horizon Outlet		**Horizon Campus**		**NBE**		**LINK or Financial Institutions**
			[PS] →			
			← [PR]			

The Horizon prime and backup NBS Agent send application Echo Test messages at regular configurable intervals to NBE. If a timeout of this Echo Test is detected then the application software can close the connection (if appropriate) in order to reset the current session.

2.3 Non Computer Data

All data relating to this interface (with the exception of security (zone) keys) is originated/received from a connected computer system or from internal reference data.

The manual exchange of security (zone) keys is described in Section 5 - ZMK Distribution.

FUJ00001624

3 Data Items

3.1 Data Item List

3.1.1 General Message Element Definitions and Abbreviations

The following sections define the list of Horizon Campus Message Elements for each group of transactions, together with which message(s) they are present in. Each message is classified and identified using the RACE (Request / Authorise / Confirm / Exception) model.

The Horizon Message Element name has been included for ease of reference.

The entry in the format column corresponds to any of the abbreviations shown in the following table:

Abbreviation	Description
A	Alphabetic characters only
N	Numeric characters only
An	Alphabetic or Numeric characters
As	Alphabetic or Special characters
Ans	Alphabetic, Numeric or Special characters
B	Binary
DD	Day
MM	Month
YY	Year
CC	Century
HH	Hour
MM	Minutes
SS	Seconds
H	Hexadecimal representation of the data
T	XML Tag

The Field Size column gives the number of characters (octets) required for the data excluding XML tag names, as shown in the table below. Note that this value does not take into account the effect of encryption, which will increase the size of the sensitive data. For further detail see Section 5.6.1.

Abbreviation	Description
3	Fixed Length field. Numeric fixed length fields are right justified and zero padded. Fixed length string fields are left justified and space padded.
.. 10	Variable length field (up to a maximum of 10 characters in this example).

The Source column indicates the system or user originating the data.

The Notes column contains a brief description of the field, together with any additional comments.

The Required column in the message definition tables within this section contain the following codes:

Code	Meaning
M	The element is mandatory for this message
C	The element is conditional for this message, and the condition to be applied is stated in the Conditions column. It should be noted that the receiving system

FUJ00001624

	may not be able to assess whether the condition has been met, in which case it must be able to interpret the presence or non-presence of the element according to appropriate business rules.

Notes

- The FAD Code, at an instance in time, unambiguously identifies an outlet. A FAD code may be reused, but because there is a hygiene period before reuse, this should not cause any problems. The current assumption is that the FAD code will continue to be used to uniquely identify an outlet, as many Horizon functions rely on this.

- Null fields (i.e. that are not required) need not be transmitted over this interface. It is the responsibility of the receiving system to interpret null fields appropriately. If an amount field contains a zero, this will be treated as a numeric amount and not a null value.

- The term “CDATA” is used to indicate to XML that the field contains binary values.

- XML requires that all data is printable. Base64 encoding of binary data allows the data to be presented as a printable string of ASCII characters. The character set is the ASCII code page, ISO 8859. Base64 encoding results in a 3:4 expansion of data. The 64 "digits" used when encoding are:

  ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

  and the equals character is used for padding.

FUJ00001624

3.1.2 Horizon-NBE Message Elements

The Horizon Message Elements used in Horizon-NBE messages are listed below (see section 3.1.1 for explanation of columns).

The information presented here is also included in different contexts in other sections, mainly 3.2 and 4.3. However, the information in 3.1.2 takes precedence over any other section, where the information is included.

The table includes Horizon element names, descriptions, XML tag names, maximum length of each element (including XML tag names). The XML names have been developed as follows:

- Where possible, the LINK/ISO name has been used as the starting point
- Where no (suitable) LINK/ISO name is available, the Horizon name has been used as the starting point
- The XML names have been shortened as much as possible, whilst still retaining meaning in the name. Sometimes this has been achieved by removing vowels in the words, except where they occur at the beginning or end of a word. More often the first 3 or 4 characters of each word have been selected
- Each shortened word begins with a capital letter
- There are no delimiters between words
- The words were re-arranged so that the class word (identifier, number, date, amount, etc.) occurred at the end of the name for consistency and reference purposes. Class words in XML were amended where appropriate to ensure consistency in XML.
- XML structures are hierarchical. For each XML tag, the higher level XML names are shown in brackets. XML structures are to be included in this specification.
- To further reduce the length of XML tag names certain abbreviations were adopted, as follows:
  - Cd Code
  - Id Identifier
  - MAC Message Authentication Code
  - Msg Message
  - Num Number

FUJ00001624

- PAN Primary Account Number
- PIN Personal identification number
- STAN System Trace Audit Number
- Trnsm Transmission
- Txn Transaction.

HorizonMessageElement	Parent XML Tag Name	XMLTagName	Calculated Tag+ data size	Max data size	Description	Format	Size	Source	[R2]	[A2]	[C2]	[C4]	[D]	[KT]	[KA]	[PS]	[PR]
_XBal	Balce	Bal	11	0	This XML tag is used to group repeatable Balance fields	T	0			C							
_XBalce	Txn	Balce	15	0	This XML tag is used to group Balance fields	T	0			C							
_XCtrl	NBAMsg	Ctrl	13	0	Defines the Control Data for the message	T	0		M	M	M	M	M	M	M	M	M
_XId	NBAMsg	Id	9	0	Defines the business data needed to uniquely identify the transaction	T	0		M	M	M	M	M	M	M	M	M
_XNBAMsg	TOPLevel	NBAMsg	17	0	The top level XML tag that identifies the XML structure for all the messages in this AIS	T	0		M	M	M	M	M	M	M	M	M
_XSec	NBAMsg	Sec	11	0	This XML tag is used to group Security-related fields	T	0		M								
_XTxn	NBAMsg	Txn	11	0	This XML tag holds the non-key fields for an individual message	T	0		M	M	M	M	M	M	M	M	M
Agent_Date	Ctrl	AgDte	23	8	UTC date. Synched with a time source – Rugby.	CCYYMMDD	8	Campus Agent	M								

FUJ00001624

Agent_Time	Ctrl	AgTme	21	6	UTC time. Synched with a time source – Rugby	HHMMSS	6	Campus Agent	M								
Amount_Authorised	Txn	AuthAmt	31	12	An amount of money that a bank will allow a Post Office customer to deposit/withdraw in a specific transaction. Expressed in the minor unit of currency (i.e. GBP pence or EUR cents)	N	.. 12	FI		C			C				
Amount_Confirmed	Txn	ConfAmt	31	12	An amount of money that a Post Office customer has confirmed that they have deposited/withdrawn in a specific transaction. Expressed in the minor unit of currency (i.e. GBP pence or EUR cents).	N	.. 12	Clerk			M	M	M				
Amount_Discrepancy	Txn	DiscAmt	31	12	This amount of money is the net result of a transaction, as far as the bank is concerned. It will contain the Amount_Confirmed, Amount_Authorised or Amount_Requested, depending on the reason for the [D] message. Expressed in the minor unit of currency (i.e. GBP pence or EUR cents), it does not contain a sign.	N	.. 12	NBE					M				
Amount_Requested	Txn	ReqAmt	29	12	An amount of money that a Post Office customer wishes to deposit/withdraw in a specific transaction. Expressed in the minor unit of currency (i.e. GBP pence or EUR cents)	N	.. 12	Clerk	C				C				
Auth_Code	Txn	AuthCd	23	6	A value generated by the Bank to be printed on the receipt passed to the Customer. Usually this field is reserved for EFTPoS transactions, but it may also be used in the direct bank Interface.	Ans	.. 6	FI		C							
Balance_Type	Bal	Type	15	2	Classifies account balances, according to their usage, using ISO / LIS5 equivalent enumerators. Please refer to Appendix A for enumerated values.	N	2	FI		C							

FUJ00001624

Balance_Value	Bal	Amt	24	13	The monetary balance for a customer's bank account, for a balance type, at a point in time. Contains "C" (optional) = credit "D" = debit, followed by up to 12 digits amount in the minor unit of currency (i.e. GBP pence or EUR cents)	A n s	.. 13	FI		C							
Bank_Transaction_Id	Id	STAN	19	6	Message sequence number assigned by the message originator (except Horizon), to assist in identifying a transaction uniquely. Stays unchanged through the life of the transaction.	n	.. 6	NBE		M	C	M	M				
Clerk_Identity	Ctrl	User	19	6	Records identity of clerk operating at the outlet workstation (also known as node or counter). This is required for audit purposes.	A n	6	Outlet from system	M		M		M				
Client_Id	Txn	ClientId	31	10	Identifies a client of Consignia that is the end bank (card issuer) for a transaction . This element is needed for reconciliation and reports.	N	.. 10	Horizon from Ref Data	M		M	M	M				
Currency	Txn	CurrCd	20	3	Code defining the currency used to represent the transaction amount. Will be GBP, may be EUR later. ISO4217 format to LINK & Fis	A	3	Clerk	C	C	M	M	M				
Discrepancy_Reason_Code	Txn	DscRsnCd	24	3	Shows why a reconciliation error occurred for a transaction. Please refer to Appendix A for enumerated values.	N	3	NBE					M				
Encrypt	Sec	Encrypt	187	168	This contains the Encrypted Sensitive Data passed by Horizon to NBE. The encrypted fields are Track 2 data (Expiry Date, and optionally Issue Number and Start Date). These fields are passed from the counter to Horizon in an XML structure, called Encdata (see 4.3.2.1). The Encdata XML tag is also included in Encrypt.	T	0		M								
Entry_Method	Txn	EtyMde	18	1	Specifies how a transaction was entered by a clerk at a Point of Service. Value: 1 = manual, 2 = magnetic card. Note that magnetic card data entry will always be from Track 2.	N	1	Outlet from system	M								

FUJ00001624

Expiry_Date	N/A	ExpDte	0	4	Contains the year and month after which the card is deemed to have expired. Card front format is (MMYY), but needs to be converted to ISO format (YYMM) in Horizon, so this AIS handles the date in ISO format. This field is passed to the NBE within the Encrypt field and, therefore, does not have an XML length.	Y Y M M	4	Outlet from card	C								
Fee	Txn	FeeAmt	29	12	Value of the issuer charge for processing a transaction in the minor unit of currency (i.e. GBP pence or EUR cents). This is not included in Transaction Amount, as the value is applied by the issuer. The value of the fee sign will indicate whether the fee is credited to or debited from the customer. Field is variable length and will have the following format: Digit 1 = C (Credit) or D (Debit) Digits 2-n = numeric	A N	.. 12	FI		C							
Group_Id	Ctrl	AcptrId	25	6	Uniquely identifies the party accepting the card and presenting transaction data to an acquirer. Currently, it will be an outlet, which is a Consignia organisational unit, providing face-to-face customer services. Contains FAD code bytes 1-6	N	6	Outlet from Ref Data	M		M	M	M				
Horizon_Txn_Num	Id	HTxnNum	51	32	Unique transaction number to be used in all messages between Horizon and the NBE relating to the transaction. Generated by Horizon and provided in the request message initiating the transaction. Will be generated using Group_Id, Node_Id (Outlet Workstation Identifier) and an incrementing number, however no assumptions should be made about the internal structure of this element - it must be regarded as a unique alphanumeric string.	A n s	.. 32	Outlet from system	M	M	M	M	M				
Issue_Number	N/A	IssNum	0	3	A number distinguishing between separate cards with the same primary account number. It is entered when requested (when swipe fails). This field is passed to the NBE within the Encrypt field and, therefore, does not have an XML	N	3	Outlet from card	C								

FUJ00001624

					length.												
Issuer_Scheme_Id	Txn	IssSchId	31	10	A unique system generated code to identify the Issuer Scheme. An example of an Issuer scheme might be Barclays' Standard Current Account.	N	10	Outlet from Ref data	M		M						
Language_Code	Txn	LangCd	18	1	Identifies the language to be used for printing text on receipt . The values 1-4 are set in reference data to indicate regions, the value 2 (= Wales) is the only value actioned by this interface	N	1	Outlet from Ref data	M								
Maximum_Withdrawal	Txn	MaxWdrw	31	12	Maximum withdrawal for an individual transaction, in the minor unit of currency (i.e. GBP pence or EUR cents). This is set by the outlet and is passed to the Bank.	N	.. 12	Outlet from Ref data	C								
Message_Authentication_ Code	NBAMsg	MAC	51	40	Used to validate the source and the text of the message between the sender and receiver. (see ISO 9807). Value is held as Base64 encoded binary. See Section 5.6.5 for additional details	encrypted	40	Sending System	M	M	M			M	M	M	M
Message_Type	Ctrl	MsgType	23	4	Classifies the type of message being sent. Enumerators are listed in section 7.7	An	.. 4	Outlet from system	M	M	M	M	M	M	M	M	M
Network_Management_Txn _Num	Id	NetTxnNum	55	32	Unique transaction number to be used in all network management messages between Horizon and the NBE. The same overall size field is used as Horizon_Txn_Num, but the internal structure of the identifier (i.e. the value) may be different from those generated at the counter			Campus Agent						M	M	M	M

FUJ00001624

Network_Response_Code	Txn	NetRespCd	25	2	This allows the NBE to report Status information in Echo Tests and the response to a Security Key Test message. Please refer to Appendix A for enumerated values.	N	2	NBE							M		M
Node_Id	Ctrl	TermId	19	2	Uniquely identifies a point of service workstation (counter/node) within a Consignia outlet	N	2	Outlet from system	M		M		M				
PAN	Txn	PAN	30	19	A series of up to 19 digits on a card used to identify a particular card, customer account or relationship. It is.embossed on card or first *n* digits on track 2. Manually entered when card swipe fails Full name is Primary Account Number.	N	.. 19	Outlet from card	M		M	M	M				
PIN_Block_1	Sec	PIN1	57	44	Encrypted PIN block value Used to identify the cardholder at the point of service. Value is held as Base64 encoded binary	encrypted	44	Entered by cust	C								
PIN_Block_2	Sec	PIN2	57	44	When customer enters value for changed PIN, the new encrypted PIN is entered here. Value is held as Base64 encoded binary.	encrypted	44	Entered by cust.	C								
Receipt_Text	Txn	RcptTxt	99	80	Card issuer data to be printed on the Point of Service workstation. Comprises 2 lines of 40 characters of information, e.gBank marketing material, festive message etc.	Ans	..80	FI, via look up		C							
Receipt_Transaction_Date	Id	LclDte	25	8	As printed on receipt, transaction date on a Request, in Local Time	CCYYMMDD	8	Outlet from system	M	M	M	M	M				
Receipt_Transaction_Time	Id	LclTme	23	6	As printed on receipt, transaction time on a Request, in Local Time	HHMMS	6	Outlet from system	M	M	M	M	M				

FUJ00001624

						S											
Reference	Txn	Ref	75	64	Reference data that is to be reflected back in the response message. Allocated by Horizon, it is to be used in Security Key and Echo Test and Acknowledgement messages.	A n s	.. 64	Horizon / NBE						M	M	M	M
Response_Code	Txn	RespCd	19	2	A code to show the Authorisation response to a previous request message. (ie whether it has been Authorised or Declined, of Failed). Please refer to Appendix A for enumerated values	N	2	FI/NBE		M							
Routing_Gateway	Txn	RtngGwy	29	10	Identifies a system, where the authorisation for a specific transaction should be sought . This element is needed to specify where the NBE should route requests and for reconciliation and reports. Enumerators to be allocated. Value indicates destination address. Routing address, to be used in conjunction with reference data relating to organisational unit	N	.. 10	Outlet from system	M		M	M	M				
Settlement_Date	Txn	SettDte	27	8	The calendar date, for which funds shall be transferred between acquirer and card issuer (i.e. when LINK/FI brings transaction to account). Where the NBE is acting as the slave, this element is provided (or overwritten) by the client for settlement, which may be LINK, the FI or (as an option for directly connected FIs) the NBE. Where the NBE is acting as the master, the NBE will provide this date not the Client.	C C Y Y M M D D	8	Settlement Client		M		M	M				
Start_Date	N/A	EfctDte	0	4	Contains the year and month upon which the card is valid for use. Card front format is (MMYY), but needs to be converted to ISO format (YYMM) in Horizon, so this AIS handles the date in ISO format. This field is passed to the NBE within the Encrypt field and, therefore, does not have an XML length.	Y Y M M	4	Outlet from card	C								

FUJ00001624

Track_2_Image	N/A	T2	0	37	Contains the information encoded on track 2 of the magnetic stripe card, excluding beginning and ending sentinels and longitudinal redundancy check (LRC) characters. Any transaction entered by magnetic stripe will be declined if this element is not present. This field is passed to the NBE within the Encrypt field and, therefore, does not have an XML length.	N	37	Outlet from card	C								
Transaction_Result_Code	Txn	TxnRsltCd	25	2	Shows the transaction outcome. Please refer to Appendix A for enumerated values.	N	2	Outlet from clerk / application			M						
Transmission_Date_And_Time	Id	TrnsmDteTm	39	14	Date and time the message initiator sends a message, specified in UTC.	CCYYMMDDHHMMSS	14	LINK / FI / NBE / Horizon						M	M	M	M
Txn_Type	Txn	TranType	23	2	Identifies the type of transaction being undertaken ; See Appendix 7.1 for enumerated values.	N	2	Clerk	M		M	M	M				
Version_Number	Ctrl	VersNum	21	2	Version of the message definition. . Any changes to a message definition will result in a change to the version number for that message.	N	2		M	M	M	M	M	M	M	M	M
ZMK_Identifier	Txn	ZMKId	27	12	The identity of the ZMK being tested copied from the corresponding Key Test Message MAC “blob” and Base64 encoded.	An s	12	NBE							M		M

3.1.3 Horizon-NBE File Elements

FUJ00001624

Message Element	Description	Format	Size	S H	ST	C H	CF
CF_Serial_Number	X starts at 001 for first Transfer	CCYYMMDDXXX	11			M	
End_Signing_Date_Time	Latest Signing_Date_Time from control file body records	CCYYMMDDHHMMSS	14			M	
EOL	End of Line	Carriage Return/Line Feed 0xD0A	2	M	M	M	M
File_Length	Length of segment file in bytes	N	..12				M
File_Name	File name of the segment file without path name or suffixes	See TIS					M
FS	Field Separator	0x3B (semi-colon)	1	M	M	M	M
Generation_Date_and_Time	Date and time at which the sequence file was generated	CCYYMMDDHHMMSS	14	M		M	
MAC_File	A Base 64 encoded version of the MAC result of the segment file	Base64	40				M
MAC_Record	The MAC, in order, of the fields that precede the MAC_Record (including field separators)	Base64	40			M	M
Number_Records	Number of body records in the control	N	..4			M	
Record_Type	Refer to section 7.8 for enumerators	N	2	M	M	M	M
Sequence_Number_of_File	Sequence number of the file being transferred	n	..4	M			
Signing_Date_Time	Signing_Date and Time of the segment file	CCYYMMDDHHMMSS	14				M
Start_Signing_Date_Time	Earliest Signing_Date_Time from control file body records	CCYYMMDDHHMMSS	14			M	
Total_Records	Total number of XML records on the file	N	..8		M		
Version_Number	Version number of the file	N	2	M		M	

FUJ00001624

3.2 Data Interpretations

This section contains the definition of each message type to be sent over this interface. The Message Element column lists those elements required for the message by Horizon name, and relates to list in Section 3.1.

The Required column in the message definition tables within this section contain the following codes:

Code	Meaning
M	The element is mandatory for this message
C	The element is conditional for this message, and the condition to be applied is stated in the Conditions column. It should be noted that the receiving system may not be able to assess whether the condition has been met, in which case it must be able to interpret the presence or non-presence of the element according to appropriate business rules.

The Conditions column lists the conditions for inclusion of a conditional message element; inclusion of the element may depend on details of the transaction type, or simply whether the data is available to the sending system.

It should be noted that any changes to a message definition will result in a change to the version number for that message. A history of version numbers is maintained in this document.

In the message definitions below, XML Tags are not included, as only data content fields are considered.

FUJ00001624

3.2.1 [R2] - Authorisation / Financial Transaction Request

3.2.1.1 Overview

This message is sent by the Horizon Campus to the NBE. The message requests a financial transaction or authorisation.

Please note that Transmission Date and Time is not included in the [R2] message. In order to measure if a message is stale, the NBE will use the Agent Date and Time. This time will be added by the Horizon Agent.

3.2.1.2 Message Definition

Message Element	Required	Notes / Conditions
Agent_Date	M	
Agent_Time	M	
Amount_Requested	C	Required for Deposit, Withdrawal and Withdrawal with Balance transactions, as indicated by the Txn_type field in this message.
Clerk_Identity	M	
Client_Id	M	
Currency	C	
Entry_Method	M	
Expiry_Date	C	Required, if manually entered and specified in reference data
Group_Id	M	
Horizon_Txn_Num	M	
Issue_Number	C	Required, if manually entered and specified in reference data
Issuer_Scheme_Id	M	
Language_Code	M	
Maximum_Withdrawal	C	Required for Withdraw Limit transaction type, as indicated by the Txn_type field in this message.
Message_Authentication_Code	M	
Message_Type	M	
Node_Id	M	
PAN	M	
PIN_Block_1	C	Required for PIN change transaction, or if verification is by PIN, as indicated by the Txn_type field in this message.
PIN_Block_2	C	Required for PIN change transaction, as indicated by the Txn_type field in this message.
Receipt_Transaction_Date	M	
Receipt_Transaction_Time	M	
Routing_Gateway	M	
Start_Date	C	Required, if manually entered and specified in reference data
Track_2_Image	C	Required, if Entry_Method = 2 (magnetic card)
Txn_type	M	
Version_Number	M	Set to 01

FUJ00001624

3.2.2 [A2] - Authorisation/Financial Transaction Request Response

3.2.2.1 Overview

This message is sent by the NBE to Horizon Campus on receipt of an [A1] message from LINK or a Financial Institution or on timeout for the [A1]. The message contains the authorisation verdict to a request.

Transactions supported by the [A2] message are listed in Section 2.1above.

3.2.2.2 Message Definition

Message Element		Required	Notes / Conditions
Amount_Authorised		C	Required for Deposit, Withdrawal, Withdraw Limit and Withdrawal with Balance transactions, as indicated by the Txn_type field in this message. Will be set to zero if the request is declined, (as indicated by the Response Code field in this message)
Auth_Code		C	Required, if available from LINK/Bank
Balance	Balance_Type	C	Required, if balance enquiry or financial transaction with balance, as indicated by the Txn_type field in this message (see 7.1 for enumerators) . Up to 2 balances will be passed to Horizon (each will be processed by Horizon) This field may be repeated to provide multiple balances. Refer to section 7.5 for values.
	Balance_Value	C	
Bank_Transaction_Id		M	
Currency		C	Required, if Amount_Authorised or Balance or Fee is present in message (i.e. not null)
Fee		C	Required, if issuer charges fee on this transaction
Horizon_Txn_Num		M	
Message_Authentication_Code		M	
Message_Type		M	
Receipt_Transaction_Date		M	
Receipt_Transaction_Time		M	
Receipt_Text		C	Required, if available from issuer
Response Code		M	See Appendix A for enumerated values
Settlement_Date		M	
Version_Number		M	Set to 01

FUJ00001624

3.2.3 [C2] - Confirmation

3.2.3.1 Overview

These messages are sent by the Horizon Campus to the NBE for financial transactions only.

[C2] nulls are generated from the counter where:

1. the clerk has declined the transaction where an [A] Approve has been sent
2. the counter times out as no [A] has been received

If the NBE receives duplicate [C2]s, any second or subsequent [C2] will appear on an exception report during end of day processing. Duplicates will have the same Horizon Transaction Number.

Transactions supported by the [C2] message are listed in Section 2.1above.

3.2.3.2 Message Definition

Message Element	Required	Notes / Conditions
Amount_Confirmed	M	Will be set to zero if the transaction is declined, (as indicated by the Transaction Result Code field in this message)
Bank_Transaction_Id	C	Required, if [A2] is available
Clerk_Identity	M	
Client_Id	M	
Currency	M	
Group_Id	M	
Horizon_Txn_Num	M	
Issuer_Scheme_Id	M	
Message_Authentication_Code	M	
Message_Type	M	
Node_Id	M	
PAN	M	
Receipt_Transaction_Date	M	Used to detect age of message for matching with request
Receipt_Transaction_Time	M	
Routing_Gateway	M	
Transaction_Result_Code	M	
Txn_type	M	
Version_Number	M	Set to 01

FUJ00001624

3.2.4 [C4] - Confirmation

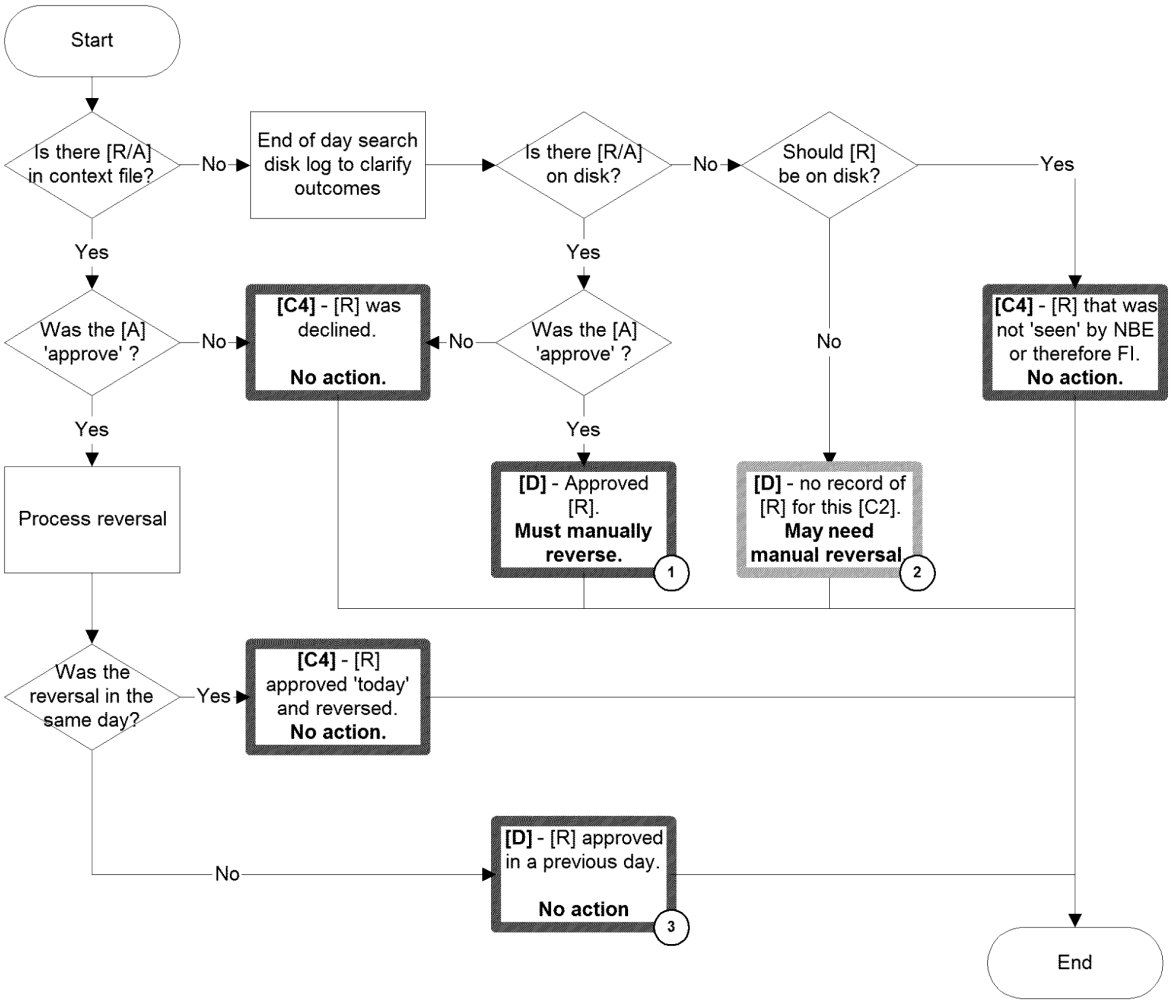
3.2.4.1 Overview

NBE sends a [C4] message when:

1. There is a [R/A] pair at the End of Day for which no reversal was required (either no [C2] message has been received, or a [C2] message has been received and the [A] was a decline).

Where there is a [C2] in the message set:

2. The [C2] message requires a reversal and the reversal is actioned, even if the NBE cannot complete delivery to the Financial Institution;
3. There is no [R] or [A] in the log and the [C2] message is recent i.e. if there was a [R] message that reached the NBE it would have been found. As such the [C4] message closes the transaction that never got to the Financial Institution;
4. There is a [C2] message with a corresponding [R/A] pair in the log for the same day, but no reversal is needed (i.e. [A] was a decline).



FUJ00001624

3.2.4.2 Message Definition

Message Element	Required	Notes / Conditions
Amount_Confirmed	M	
Bank_Transaction_Id	M	
Client_Id	M	
Currency	M	
Group_Id	M	
Horizon_Txn_Num	M	
Message_Type	M	
PAN	M	
Receipt_Transaction_Date	M	
Receipt_Transaction_Time	M	
Routing_Gateway	M	
Settlement_Date	M	
Txn_type	M	
Version_Number	M	Set to 01

FUJ00001624

3.2.5 [D] - Reconciliation Exception

3.2.5.1 Overview

The NBE sends this message to Horizon Campus at the end of the day as part of the batch file generated during settlement to inform Horizon that there will be a reconciliation difference. This indicates that manual inspection may be required to see what action is required to reconcile the transaction. This message is only sent for financial transactions.

NBE sends a [D] message when:

1. There is a [C2] message with a corresponding [R/A] pair on disk and reversal is needed; it was too late for the on-line to reverse and therefore needs manual intervention. The NBE does not generate a reversal.

This would have a code 01 with a value of the approved amount.

2. There is a [C2] message that refers to a [R] message that is older than that held on disk and therefore not known if a reversal is needed or not. The NBE does not generate a reversal.

This would have a code 02 with a value of zero.

3. There is a [C2] message with a corresponding [R/A] pair still in the context file that was approved in a previous day i.e. a value [C4] message would have been sent in an earlier day (typically a cut-over event, and seen as a stand-alone reversal). The NBE also generates a reversal.

This would have a code 03 with a value of zero, as this is the resultant FI position.

The reason codes are listed in section 7.2.

3.2.5.2 Message Definition

Message Element	Required	Notes / Conditions
Amount_Authorised	C	Required if available from [A] message
Amount_Confirmed	M	
Amount_Discrepancy	M	It will contain the Amount_Confirmed, Amount_Authorised or Amount_Requested, depending on the reason for the [D] message (please refer to Appendix 7.2 for the list of reasons).
Amount_Requested	C	Required if available from [R] message
Bank_Transaction_Id	M	
Clerk_Identity	M	
Client_Id	M	
Currency	M	Currency relates to Amount_Discrepancy and will always be present.
Discrepancy_Reason_Code	M	Refer to 7.2 for values
Group_Id	M	
Horizon_Txn_Num	M	
Message_Type	M	
Node_Id	M	Please note it is possible for there to be a change in the value of Node_Id between the [R2] and the [C2] message. It does not matter to Horizon which of the two values is passed back in a [D] message (should they differ).
PAN	M	
Receipt_Transaction_Date	M	
Receipt_Transaction_Time	M	
Routing_Gateway	M	
Settlement_Date	M	
Txn_Type	M	
Version_Number	M	Set to 01

FUJ00001624

3.2.6 [KT] - Security Key Test

3.2.6.1 Overview

This message is sent by Horizon Campus to the NBE to confirm that a new ZMK has been correctly installed, and that Horizon is ready to receive Working Keys encrypted using it.

3.2.6.2 Message Definition

Message Element	Required	Notes / Conditions
Message_Authentication_Code	M	
Message_Type	M	
Network_Management_Txn_Num	M	
Reference	M	
Transmission_date_and_time	M	
Version_Number	M	Set to 01

3.2.7 [KA] - Security Key Acknowledge

3.2.7.1 Overview

This message is sent by the NBE to Horizon Campus to acknowledge correct receipt of a Key Test Message, and to confirm that NBE is ready to receive Working Keys encrypted using the ZMK identified in the message.

3.2.7.2 Message Definition

Message Element	Required	Notes / Conditions
Message_Authentication_Code	M	
Message_Type	M	
Network_Management_Txn_Num	M	
Network_Response_Code	M	
Reference	M	
Transmission_date_and_time	M	
Version_Number	M	Set to 01
ZMK_Identifier	M	

FUJ00001624

3.2.8 [PS] – Echo Test

3.2.8.1 Overview

The Horizon Agents have identified a need for sending periodic [PS] Echo Test messages to the NBE so as to be able to check that all is well in the connections even if there is no business traffic (eg in the middle of the night). The NBE should be listening for [PS] messages at all times (as it does for [R2] messages) and on receipt return a response to the ICLP agent indicating its alive status using the same connection.

3.2.8.2 Message Definition

Message Element	Required	Notes / Conditions
Message_Authentication_Code	M	
Message_Type	M	
Network_Management_Txn_Num	M	
Reference	M	
Transmission_date_and_time	M	
Version_Number	M	Set to 01

3.2.9 [PR] – Echo Test Response

3.2.9.1 Overview

The Horizon Agents will send periodic [PS] Echo Test messages to the NBE, to check that all is well in the connections even if there is no business traffic (e.g. in the middle of the night). The NBE should be listening for [PS] messages at all and should respond with a [PR] message as soon as possible.

3.2.9.2 Message Definition

Message Element	Required	Notes / Conditions
Message_Authentication_Code	M	
Message_Type	M	
Network_Management_Txn_Num	M	
Network_Response_Code	M	
Reference	M	
Transmission_date_and_time	M	
Version_Number	M	Set to 01
ZMK_Identifier	M	

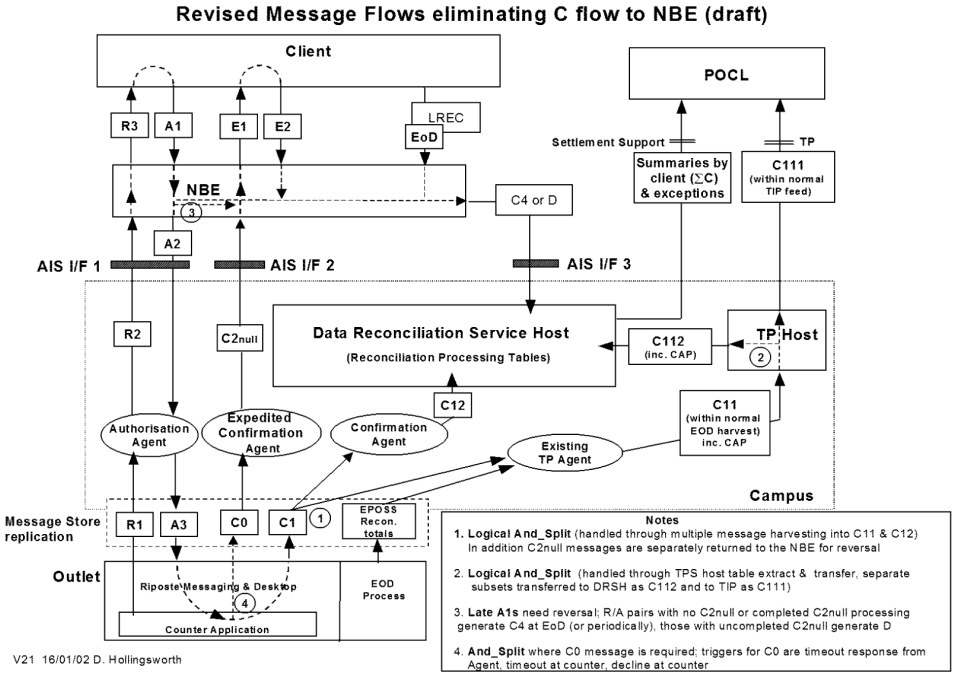
FUJ00001624

4 Transfer Structure

4.1 Transfer Grouping

4.1.1 Overview of the Interface

The following figure shows the end to end message sequences, using the RAC (Request / Authorise / Confirm) model, across all components of the Network Banking environment. This AIS addresses all application messages between the NBE and the Horizon Campus. The network messages [KT], [KA], [PS], [PR] are not included in this diagram, but are included in the PONWB – Horizon-NBE Technical Interface Specification [3].



The diagram (taken from ICL Pathway) shows that the NBE exchanges messages with the Horizon Campus over three distinct interfaces.

AIS I/F 1 is used to exchange messages between the PO Outlet and the NBE through an Authorisation Agent within the Horizon Campus. This interface carries the transaction request messages from Horizon to the NBE, and the related authorisation messages that authorise or decline the transaction.

AIS I/F 2 is used for expedited confirmation messages that originate at the Outlet, requiring the NBE to possibly reverse a transaction.

AIS I/F 3 is used to send the batch file which is created during End of Day reconciliation containing [C4] and [D] messages to the Data Reconciliation Service Host in Horizon.

All these interfaces should be resilient to the transfer of duplicate messages; in practice, however, this should only happen after failure and recovery of either end of the interface.

Horizon can initiate an Echo test ([PS] / [PR] exchange) or a Security test ([KT] / [KA] exchange) at any time with the NBE using a specific Systems Management interface (not shown in the diagram) for this

FUJ00001624

purpose. Since Horizon is a distributed system, these exchanges, which may take place from any Horizon Agent Server to the NBE, provide an appropriate "return address" for the reply by means of an Agent_Identifier.

4.1.2 Authorisation Agent Interface (Interface 1)

This interface supports [R2] and [A2] messages only. The messages are exchanged online, as a single message transfer in each direction.

Horizon campus initiates all transactions by issuing an [R2] message from a request from a clerk at a PO Outlet of behalf of a card-holding customer. NBE forwards the request as an [R3] message to the authorising institution and under normal circumstances waits for an [A1] response, which it then passes to Horizon as an [A2] message.

Both NBE and Horizon will detect and discard stale messages, and each will apply a timeout to the expected reply. Activation of the timeout will cause a transaction to be declined by the NBE (on non-receipt of the [A1]) by sending an [A2] decline message to Horizon, and by Horizon (on non-receipt of the [A2]) by initiating an [A3] decline. If a connection no longer exists to deliver the [A] message then automatic reversal by the NBE is required.

This interface is to be operational throughout the Post Office trading day, which, for a few outlets (e.g. Heathrow airport), is 24 hours. This means that “business as usual” must be accommodated during settlement.

4.1.3 Expedited Confirmations (Interface 2)

This interface supports expedited confirmation [C2] messages only. They are ‘priority’ messages generated either because the counter decision is different from that on the authorisation due to a clerk decision or because of a failure in communications and it is unclear as to whether the transaction has been authorised or not.

4.1.4 Batch Interface (Interface 3)

This interface supports the file transfer of the batch file containing the Confirmation [C4], and Reconciliation Exception [D] messages. Either a [C4] or a [D] message is needed to complete the “message set” for each transaction. The scenarios where a [C4] is generated is described in section 3.2.4 and [D] scenarios are described in section 3.2.5. There will only be one [C4] or [D] message in one business day for one message set.

4.1.5 Network Management

The Authorisation Agent and Expedited Confirmation Interfaces support Network Management application Ping [PS], [PR] messages in addition to their primary message set. These Network Management messages flow in real time. Ping [PS] messages originate in Horizon Agents. Each agent will generate a [PS] message at a regular, configurable interval. This interval will typically be a number of minutes. The NBE should respond immediately with a [PR] message to the originating agent to confirm it is available to process business messages. If the Horizon Agent does not receive a [PR] message it should log an event and send another message after waiting for the configured interval. Any response must be received on the same connection.

Key Test messages and their responses [KT] and [KA] are used to verify that a new acquirer ZMK has been exchanged successfully. The period between ZMK changes must be agreed by Horizon and NBE. It is normally occurs every six months. Keys will only be changed at other times, if key compromise or a Disaster Recovery action is required. The [KT] message includes a working key encrypted under the new Zone Master Key. The NBE decrypts and verifies the working key and responds to the originating agent, using a [KA] message.

FUJ00001624

4.2 Transfer Structure

The messages defined in this AIS will be exchanged using XML The message definitions in Section 3.2 specify the mandatory and conditional elements comprising each message.

4.3 Record Structure

4.3.1 XML Structures

For each message type in this specification, an equivalent XML structure is provided below in XML tag language. Please refer to the Data Dictionary in this specification for details of the derivation of the XML tag names and maximum length of each field (including XML tags).

A maximum length for the XML structure is normally included.. In the XML structures below, there are two types of elements

- XML structure headings, which do not have any associated values
- XML attributes that do have any associated values. These names are followed by the XML delimiter for the field followed by the Horizon Message Element e.g. <AcptrId>value</AcptrId>. // Group_Id

The XML structures accommodate sensitive data encryption operations, which will include whichever fields are present of Track_2_Image, Expiry_Date, Issue_Number and Start_Date.

"Empty" fields will be omitted in XML.

4.3.2 Message Structures

4.3.2.1 [R2] - Authorisation/Financial Transaction Request

Maximum Length of [R2] XML Structure is 923 octets

```
<NBAMsg>
        <Ctrl>
                <VersNum>value</VersNum>        // Version_Number
                <MsgType>value</MsgType>        // Message_Type
                <AcptrId>value</AcptrId>        // Group_Id
                <TermId>value</TermId>          // Node_Id
                <User>value</User>              // Clerk_Identity
                <AgDte>value</AgDte>            //Agent_Date
                <AgTme>value</AgTme>            //Agent_Time

        </Ctrl>

        <Id>
                <HTxnNum>value</HTxnNum>        // Horizon_Txn_Num
                <LclDte>value</LclDte>          // Receipt_Transaction_Date
                <LclTme>value</LclTme>          // Receipt_Transaction_Time
```

FUJ00001624


```
        </Id>
        <Txn>
                <TranType>value</TranType>          // Txn_Type
                <PAN>value</PAN>                    // PAN
                <ReqAmt>value</ReqAmt>              // Amount_Requested
                <CurrCd>value</CurrCd>              // Currency
                <EtyMde>value</EtyMde>              // Entry_Method
                <IssSchId>value</IssSchId>          // Issuer_Scheme_Id
                <LangCd>value</LangCd>              // Language_Code
                <MaxWdrw>value</MaxWdrw>            // Maximum_Withdrawal
                <ClientId>value</ClientId>          // Client_Id
                <RtngGwy>value</RtngGwy>            // Routing_Gateway
        </Txn>
        <Sec>
                <PIN1>value</PIN1>          // PIN_Block_1       CDATA as encrypted
                <PIN2>value</PIN2>          // PIN_Block_2       CDATA as encrypted
                <Encrypt>value</Encrypt>    // Encrypted data (see below) CDATA as encrypted
        </Sec>
        <MAC>value</MAC>                    // Message_Authentication_Code
</NBAMsg>
```

<Encrypt> is a single encrypted field, the source of which is the following structure, (passed from the counter to Horizon):-

```
                <EncData>
                        <T2>value</T2>              // Track_2_Image
                        OR
                        [ <ExpDte>value</ExpDte>    // Expiry_Date
                        [ <IssNum>value</IssNum>    // Issue_Number
                        [ <EfctDte>value</EfctDte>  // Start_Date
                </EncData>
```

Please refer to 5.6.4 for the exact structure of <Encrypt>

FUJ00001624

4.3.2.2 [A2] - Authorisation/Financial Transaction Request Response

Maximum Length of [A2] XML Structure is 602 octets. The length assumes 2 balances are passed in the message.

```
<NBAMsg>
        <Ctrl>
                <VersNum>value</VersNum>            // Version_Number
                <MsgType>value</MsgType>            // Message_Type
        </Ctrl>
        <Id>
                <HTxnNum>value</HTxnNum>            // Horizon_Txn_Num
                <LclDte>value</LclDte>              // Receipt_Transaction_Date
                <LclTme>value</LclTme>              // Receipt_Transaction_Time
                <STAN>value</STAN>                  // Bank_Transaction_Id
        </Id>
        <Txn>
                <RespCd>value</RespCd>              // Response_Code
                <AuthAmt>value</AuthAmt>            // Amount_Authorised
                <CurrCd>value</CurrCd>              // Currency
                <FeeAmt>value</FeeAmt>              // Fee
                <Balce>                             // Balance
                        <Bal>                       // (can repeat)
                                <Type>value</Type>  // Balance_Type
                                <Amt>value</Amt>    // Balance_Amount
                        </Bal>
                </Balce>
                <AuthCd>value</AuthCd>              // Auth_Code
                <RcptTxt>value</RcptTxt>            // Receipt_Text
                <SettDte>value</SettDte>            // Settlement_Date
        </Txn>
        <MAC>value</MAC>                            // Message_Authentication_Code
</NBAMsg>
```

FUJ00001624

4.3.2.3 [C2] - Confirmation

Each [C2] message will have a Maximum Length of 546 octets

```
<NBAMsg>

        <Ctrl>
            <VersNum>value</VersNum>          // Version_Number
            <MsgType>value</MsgType>          // Message_Type
             <AcptrId>value</AcptrId>         // Group_Id
            <TermId>value</TermId>            // Node_Id
            <User>value</User>                // Clerk_Identity
        </Ctrl>
        <Id>
            <HTxnNum>value</HTxnNum>          // Horizon_Txn_Num
            <LclDte>value</LclDte>            // Receipt_Transaction_Date
            <LclTme>value</LclTme>            // Receipt_Transaction_Time
            <STAN>value</STAN>                // Bank_Transaction_Id
        </Id>
        <Txn>
            <IssSchId>value</IssSchId>        // Issuer_Scheme_Id
            <TranType>value</TranType>        // Txn_Type
            <TxnRsltCd>value</TxnRsltCd>      // Transaction_Result_Code
            <ConfAmt>value</ConfAmt>          // Amount_Confirmed
            <CurrCd>value</CurrCd>            // Currency
            <ClientId>value</ClientId>        // Client_Id
            <PAN>value</PAN>                  // Primary Account Number
            <RtngGwy>value</RtngGwy>          // Routing_Gateway
        </Txn>
        <MAC>value</MAC>                      // Message_Authentication_Code
</NBAMsg>
```

FUJ00001624

4.3.2.4 [C4] - Confirmation

Each [C4] message will have a Maximum Length of 428 octets.

```
<NBAMsg>
        <Ctrl>
                <VersNum>value</VersNum>          // Version_Number
                <MsgType>value</MsgType>          // Message_Type
                <AcptrId>value</AcptrId>          // Group_Id
        </Ctrl>
        <Id>
                <HTxnNum>value</HTxnNum>          // Horizon_Txn_Num
                <LclDte>value</LclDte>            // Receipt_Transaction_Date
                <LclTme>value</LclTme>            // Receipt_Transaction_Time
                <STAN>value</STAN>                // Bank_Transaction_Id
        </Id>
        <Txn>
                <TranType>value</TranType>        // Txn_Type
                <ConfAmt>value</ConfAmt>          // Amount_Confirmed
                <CurrCd>value</CurrCd>            // Currency
                <ClientId>value</ClientId>        // Client_Id
                <PAN>value</PAN>                  // Primary Account Number
                <RtngGwy>value</RtngGwy>          // Routing_Gateway
                <SettDte>value</SettDte>          // Settlement_Date
        </Txn>
</NBAMsg>
```

FUJ00001624

4.3.2.5 [D] - Reconciliation Exception

Each [D] message will have a Maximum Length of 581 octets

```
<NBAMsg>

        <Ctrl>
                <VersNum>value</VersNum>        // Version_Number
                <MsgType>value</MsgType>        // Message_Type
                <AcptrId>value</AcptrId>        // Group_Id
                <TermId>value</TermId>          // Node_Id
                <User>value</User>              // Clerk_Identity
        </Ctrl>
        <Id>
                <HTxnNum>value</HTxnNum>        // Horizon_Txn_Num
                <LclDte>value</LclDte>          // Receipt_Transaction_Date
                <LclTme>value</LclTme>          // Receipt_Transaction_Time
                <STAN>value</STAN>              // Bank_Transaction_Id
         </Id>
        <Txn>
                <TranType>value</TranType>      // Txn_Type
                <DscRsnCd>value</DscRsnCd>      // Discrepancy_Reason_Code
                <ReqAmt>value</ReqAmt>          // Amount_Requested
                <AuthAmt>value</AuthAmt>        // Amount_Authorised
                <ConfAmt>value</ConfAmt>        // Amount_Confirmed
                <DiscAmt>value</DiscAmt>        // Amount_Discrepancy
                <CurrCd>value</CurrCd>          // Currency
                <ClientId>value</ClientId>      // Client_Id
                <PAN>value</PAN>                // Primary Account Number
                <RtngGwy>value</RtngGwy>        // Routing_Gateway
                <SettDte>value</SettDte>        // Settlement_Date
        </Txn>
</NBAMsg>
```

FUJ00001624

4.3.2.6 [KT] - Security Key Test

[KT] messages have a Maximum Length of 314 octets.

Please note that [KT] and [PS] messages will have the same format.

```
<NBAMsg>
        <Ctrl>
                <VersNum>value</VersNum>    // Version_Number
                <MsgType>value</MsgType>    // Message_Type
        </Ctrl>
        <Id>
                <NetTxnNum>value</NetTxnNum>        // Network_Management_Txn_Num
                <TrnsmDteTme>value</TrnsmDteTme>            // Transmission_Date_And_Time
        </Id>
        <Txn>
                <Ref>value</Ref>                    // Reference
        </Txn>
        <MAC>value</MAC>                            // Message_Authentication_Code
</NBAMsg>
```

FUJ00001624

4.3.2.7 [KA] - Security Key Acknowledge

[KA] messages have a Maximum Length of 366 octets.

Please note that [KA] and [PR] messages will have the same format.

```
<NBAMsg>
    <Ctrl>
        <VersNum>value</VersNum>   // Version_Number
        <MsgType>value</MsgType>   // Message_Type
    </Ctrl>
    <Id>
        <NetTxnNum>value</NetTxnNum>       // Network_Management_Txn_Num
        <TrnsmDteTme>value</TrnsmDteTme>           // Transmission_Date_And_Time
    </Id>
    <Txn>
        <Ref>value</Ref>                   // Reference
        <NetRespCd>value</NetRespCd>       // Network_Response_Code Code
        <ZMKId>value</ZMKId>               // ZMK Id
    </Txn>
    <MAC>value</MAC>                       // Message_Authentication_Code
</NBAMsg>
```

4.3.2.8 [PS] Message

[PS] messages have a Maximum Length of 314 octets.

Please note that [KT] and [PS] messages will have the same format.

```
<NBAMsg>
    <Ctrl>
        <VersNum>value</VersNum>   // Version_Number
        <MsgType>value</MsgType>   // Message_Type
    </Ctrl>
    <Id>
        <NetTxnNum>value</NetTxnNum>       // Network_Management_Txn_Num
        <TrnsmDteTme>value</TrnsmDteTme>           // Transmission_Date_And_Time
    </Id>
    <Txn>
        <Ref>value</Ref>               // Data to be reflected back in the response
    </Txn>
    <MAC>value</MAC>                   // Message_Authentication_Code
</NBAMsg>
```

FUJ00001624

4.3.1.9 [PR] Message

[PS] messages have a Maximum Length of 36 octets.

Please note that [KA] and [PR] messages will have the same format.

```
<NBAMsg>
    <Ctrl>
        <VersNum>value</VersNum>   // Version_Number
        <MsgType>value</MsgType>   // Message_Type
    </Ctrl>
    <Id>
        <NetTxnNum>value</NetTxnNum>       // Network_Management_Txn_Num
        <TrnsmDteTme>value</TrnsmDteTme>           // Transmission_Date_And_Time
    </Id>
    <Txn>
        <Ref>value</Ref>                   // Data sent in the echo response
        <NetRespCd>value</NetRespCd>        //  Network_Response_Code
        <ZMKId>value</ZMKId>           // ZMK_Id
    </Txn>
    <MAC>value</MAC>                   // Message_Authentication_Code
</NBAMsg>
```

4.4 Sequences

Figure 1 above (see Section 4.1) shows the end-to-end message sequences of all the messages supported by this AIS, from the PO Outlet to the issuing financial institution. This AIS addresses the interaction and related behaviour only of the Horizon Campus systems and the NBE.

4.5 Data Volumes

Volumes are based on information provided by Post Office Limited in NB Volumetrics, Reference [2].

4.6 Data Authentication

Data authentication is described in Section 5.3.3.

4.7 Data Dictionary

This section has now been merged into 3.1.2.

FUJ00001624

4.8 End of Day Batch Transfer

4.8.1 Overview

The NBE will send all [C4] and [D] messages at End of Day in a batch file to the Horizon FTMS Server for onward delivery to the DRS. This will be a single logical file to include all [C4] and [D] messages for every direct interface i.e. Financial Institutions and LINK. This file may be split into several smaller physical files (determined by the size of the file). Each segment file will have a header, body and trailer. In addition a control file will be sent. For those non-business days for Post Office Limited, ie where there has been no financial activity for the day, then the NBE will send a control file with a segment file containing no data.

4.8.2 Segment File Format

Each Segment file will have a header and trailer. There may be zero or more segment files. No single segment file will exceed 200 MB in size.

4.8.2.1 Segment File Header

Message Element		***Notes***
Record_Type		Refer to section 7.8.
FS		
Version_Number		Set to 01
FS		
Sequence_Number_of_File		
FS		
Generation_Date_ and_ Time		
EOL		

4.8.2.2 Segment File Body

There will be zero or more segment file body records (See section 4.3.2.4 and 4.3.2.5 for XML structure) each of which will be terminated with a carriage return line feed. The records will be in date time order within the file(s).

4.8.2.3 Segment File Trailer

Message Element		***Notes***
Record_Type		Refer to section 7.8.
FS		
Total_Records		Total number of XML records on the file
EOL		

FUJ00001624

4.8.3 Control File Format

The MAC_File is calculated over the binary representation of the file, including EOL characters, together with elements 1 to 3 in the Message Authentication Code Transport Fields, represented in their binary form. Please refer to 5.3.3 for further details

Both the MAC_File and MAC_Record are calculated over ASCII representations of the File and record respectively.

The format of the data in MAC_File and MAC_Record are as defined in section 5.6.5.

4.8.3.1 Control File Header

This section defines the structure of the file used to carry the list of segment files and their associated MACs.

Message Element		***Notes***
Record_Type		Refer to section 7.8.
FS		
Version_Number		Set to 01
FS		
CF_Serial_Number		CCYYMMDDXXX where X starts at 001 for first transfer.
FS		
Start_Signing_Date_Time		Earliest Signing_Date_Time from control file body records
FS		
End_Signing_Date_Time		Latest Signing_Date_Time from control file body records
FS		
Number_Records		Number of body records in the control file (may be zero)
FS		
Generation_Date_ and_ Time		Date and Time at which control file was generated
FS		
MAC _Record		A Base 64 encoded version of the MAC result of all the above fields including field separators.
EOL		

4.8.3.2 Control File Body

Message Element		***Notes***
Record_Type		Refer to section 7.8.
FS		
Signing_Date_Time		Signing Date and time of the segment file
FS		
File_Name		File name of segment file without path name or suffixes
FS		
File_Length		Length of segment file in bytes
FS		
MAC_File		A Base 64 encoded version of the MAC result of the segment file.

FUJ00001624

FS		
MAC_Record		A Base 64 encoded version of the MAC result of all the above fields including field separators.
EOL		

FUJ00001624

5 Security of Transmitted Data

5.1 Need to Know

Only the issuing financial institutions can verify PIN blocks for accounts they hold. The key under which PIN blocks are encrypted is translated at security zone boundaries. The content of the PIN block must not be exposed in clear in memory during the translation process.

5.2 Protected Data

Data is protected by encryption and message authentication codes, MACs.

PIN block data is encrypted at all times. The PIN block is never rendered in clear outside the hardware.

Sensitive data is encrypted while in transit.

The integrity of all messages will be protected by MACs.

5.3 Encryption and Decryption Methods

Encryption and decryption of NBE transaction data must use Triple DES with double length keys.

5.3.1 PIN Block Encryption

PIN Blocks are binary data and will be encoded in XML strings as base 64-encoded data

- PIN Block Format: Plain text PIN blocks shall be represented using Format 0 as defined in ANSI X9.8.
- Encryption Mode: The plain text shall be encrypted using a double-length DES key[1] using ECB mode as defined in Appendix 2 of FIPS Publication 46-3.

5.3.2 Sensitive Data Encryption

The binary result of sensitive data encryption will be encoded in strings in base 64-encoded XML strings.

- The plain text data shall be padded using the algorithm in ANSI X9.23 so that it is a whole multiple of 8 octets.
- Pad characters are binary zeros
- It is then encrypted using the TCBC mode of operation as defined in ANSI X9.52[2] using a 64-bit Initialisation Vector (IV)[3].

5.3.3 Message Authentication

MACs shall be computed using triple DES mode of operation specified in ANSI X9.19.

---

[1] According to FIPS46-3, TDEA keying option 2

[2] This is equivalent to the CBC mode in FIPS81 with the block cipher replaced by triple DES in ECB mode as defined in FIPS 46-3. FIPS81 has not been updated to cover triple DES.

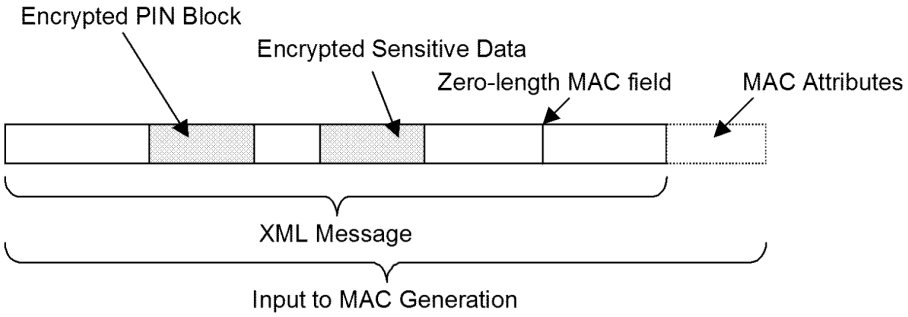
[3] The IV is required to protect against dictionary attacks on sensitive elements that have a limited number of values e.g. manually entered expiry date.

FUJ00001624

The MAC shall be computed on the complete XML message as ready for transmission, but with the MAC data, (but not its XML tag), replaced by a zero-length string. "R" messages and any future message, which includes encrypted PIN(s) and / or encrypted sensitive data, shall include the data in the form in which it will be transmitted. In other words,. any selective field encryption and Base64 translation shall be performed prior to MAC generation.

The security sub-system will append the attributes associated with the MAC to the application message prior to calculation of the MAC. The attributes are defined as elements 1 to 3 in the Message Authentication Code Transport Fields, represented in their binary form. Please refer to 5.6.5 for further details.

The following figure illustrates the scope of the MAC calculation. It shows the various encrypted elements. The location of the elements within the message is for illustrative purposes only – the actual location is defined elsewhere in the AIS.



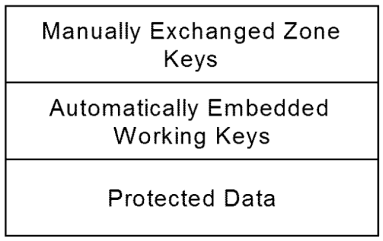
5.4 Session Establishment

Not applicable to this AIS.

5.5 Key Management

5.5.1 Key Hierarchy

The cryptographic interface operates at three levels identified in the following diagram:



The layers have the following functionality:

- The lowest layer provides cryptographic mechanisms that protect messages. There are three mechanisms each of which requires its own cryptographic key:
  - Message Authentication Codes (MACs) protects the integrity of messages in transit
  - PIN Encryption protects the confidentiality of card authentication data.

FUJ00001624

  - Data Encryption protects the confidentiality of any other sensitive data e.g. Track 2 Discretionary data.

- The middle layer manages the life cycle of the cryptographic keys used by the encryption and MACing services. Collectively these keys are known as Working Keys. An automatic Key Management Protocol is used to communicate the embedded working keys and their associated attributes across the interface.

- The upper layer is responsible for managing the lifecycle of cryptographic keys used to protect Working Keys. A Zone Master Key (ZMK) is used to protect the confidentiality of Working Keys in transit across the Horizon–NBE interface. Keys at this upper layer are established using manual procedures and are updated infrequently e.g. one every six months. Both the NBE and Horizon have a key similar to the ZMK that is used to protect keys in storage and/or transmission within their cryptographic sub-system. These keys are outside the scope of this document.

5.6 Key Types

The following keys are used across the Horizon / NBE Application Interface:

Key	Level	Expected Lifetime	Usage
ZMK	Zone Master Key	6 / 12 months	Protects working keys during distribution
NBPc	Working Key	1 Day	Protects the confidentiality of PINs in R messages
NBTDc	Working Key	1 Day	Protects the confidentiality of sensitive data in R messages
NBMCn	Working Key	1 Day	Generate & verify MACs on messages from NBE to Horizon.
NBMCc	Working Key	1 Day	Generate & verify MACs on messages from Horizon to NBE.

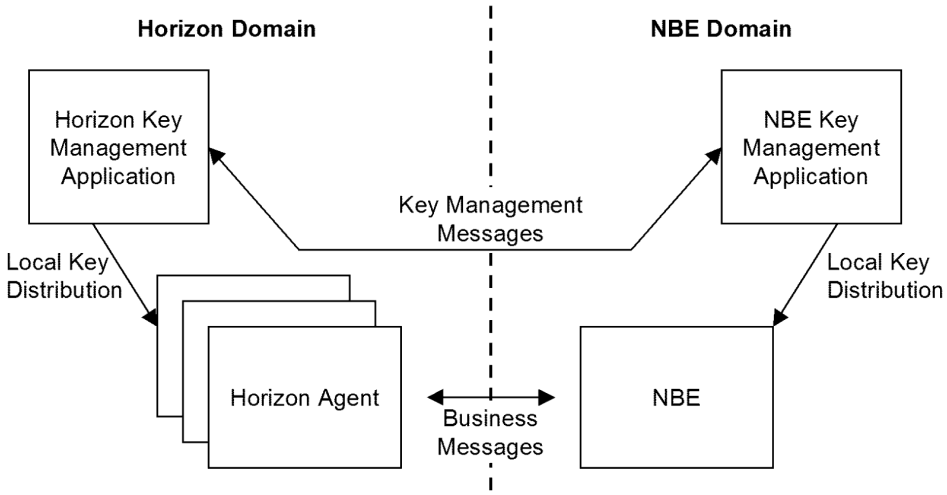
All keys are double length (112-bit) DES keys. The naming convention for Working keys is an extension of that currently in use by Horizon. “NB” indicates a protection domain applicable to Network Banking; P, TD and MC indicates the key usage as described above; “n” and “c” indicate the key owner / generator, “n” = Network Banking Engine and “c” = Horizon data **c**entre.

5.6.1 Key Management Application

Both Horizon and NBE will have their own Key Management Application. The Horizon Key Management Application will be an updated version of the existing Horizon Key Management System. The NBE Key Management Application will be based on the ICSF cryptographic sub-system and the IBM Distributed Key Management Server, DKMS.

The relationship between the key management applications is shown below:

FUJ00001624



Each Key Management Application will be responsible for:

- Storing keys securely for its own domain.
- Secure communication within its domain of keys to the business processes that require them.
- Participating in the manual and automatic key management protocols that establishes keys across the interface between Horizon Agents and the NBE.

It is a **design objective** to ensure that the local distribution of keys within a domain is transparent to the other domain.

Messages flowing from Horizon to NBE are secured at the outbound Horizon Agent. Securing consists of an outbound PIN Translate (R messages only), selective encryption of sensitive data (R messages only) and a MAC Generate (all messages). The security processing is performed as soon as practical after the signature is verified on the message inbound from elsewhere in the Horizon Campus. The complimentary processes are performed at NBE on the received message. In the opposite direction, the NBE performs a MAC generate which is verified by the receiving Horizon Agent. There is no requirement for selective encryption or PIN processing in this direction.

5.6.2 Key Management Principles

The following principles are agreed:

- NBE will generate all Zone Master Keys (ZMK). Each party must generate Working Keys that it uses to protect its outbound messages.
- The generator of a key (referred to as the “owner” of the key) is responsible for communicating it to those who need it. Please refer to 6.3 for procedures.
- The key transport mechanism of Zone Master Keys shall include a Key Check Value (KCV) to enable correct reception of a key to be verified by the recipient.
- The key owner will allocate each Zone Master Key a unique identity, its Key Tag. The Key Tag will be communicated with the key and stored with it so that both parties can use the Key Tag as a reference to the key during its lifetime.
- The key owner initiates routine replacement of the key.

FUJ00001624

- The recipient of a key can request replacement of it at any time. It is then the responsibility of the key owner to generate and distribute a new one.

- ZMKs will be transported manually in key component form and be authenticated and verified using manual procedures.

- Correct installation of a new ZMK will be confirmed by the electronic exchange of key management messages that:

  - act as a service level boundary by signalling that the sender is ready to accept traffic protected by the new ZMK, and

  - trigger the deletion of ZMKs that are no longer required. See Section 5.7.3 for fuller details of the ZMK life cycle.

- Each electronically transmitted key management message will be MACed using a key carried with the message and protected by the appropriate ZMK.

- Each business message will be MACed using a working key carried with the message and protected by the appropriate ZMK. Similarly, a message containing an encrypted PIN and encrypted sensitive data will carry the working keys required to translate the PIN and decrypt the data respectively.

- Any message carrying a Working Key will also contain the Key Tag of the ZMK used to protect the Working Key so that the recipient can identify the correct ZMK to use.

- The recipient of a Working Key does not store it. Working keys may be unique to a message but will, in any event, be changed at least daily. Where the owner stores Working Keys, the owner shall ensure that the key is securely deleted on replacement.

- NBE will generate two ZMKs for future use and transport their components to Horizon for safe storage.

  NOTE: It is proposed that two "spare" sets of ZMK components be held at Horizon in case of emergency. This allows faster response in the event that a live ZMK is suspected of compromise. It can be achieved by initially creating two sets and putting one of them live. The above procedure then creates the second spare once the first key is put live and ensures that, subsequently, as soon as any first spare is put live a new second spare is created. Assuming the regular replacement of ZMKs at six-monthly intervals, any ZMK will have a total life span of four successive six-month periods i.e. two years (one as second spare, one as first spare, one in use, one as reserve on the receiver's key ring). To assist the recognition of ZMKs, it is recommended that not more than one ZMK be generated on any particular day.

- NBE and Horizon will be responsible for deleting working keys after use.

- NBE and Horizon should ensure superseded keys are not enabled for use (set to Horizon's "dead" key status) after one key replacement cycle.

5.6.3 PIN Block Encryption Key Transport Fields

The XML field value for each of the <PIN1> and <PIN2> fields contains the content of the PIN Block Encryption Key Transport Fields in the table below which are represented in Base64 encoded form in the XML structure.

Element		Size	Content
1.	Type	1 Octet	Value = 1 (binary)
2.	ZMK Tag	8 Octets	Key tag (identity) associated with the ZMK used to encrypt the PIN Encryption Key.

FUJ00001624

3.	Key value	16 Octets	The PIN encryption Triple DES double length key encrypted under the sender's current ZMK as identified in element 2.
4.	PIN Block	8 Octets	The encrypted PIN block. See Section 5.3.1

5.6.4 Sensitive Data Encryption Key Transport Fields

The <Encrypt> field in the <Sec> structure in 4.3.2.1 is a single encrypted field, the source of which is the Sensitive Data Encryption Transport Fields in the table below represented in Base64 encoded form.

Element		Size	Content
1.	Type	1 Octet	Value = 2 (binary)
2.	ZMK Tag	8 Octets	Key tag (identity) associated with the ZMK used to encrypt the sensitive data Working Key.
3.	Key value	16 Octets	The sensitive data Working Key encrypted under the sender's current ZMK as identified in element 2.
4.	IV	8 Octets	A 64-bit random or pseudo-random value.
5.	Encrypted Data	N+1 to N+8Octets	The encrypted sensitive data of length N. This will be up to 8 octets longer than the plain text as a result of the padding. The last octet contains the number of pad characters. Eight octets are added when N is an exact multiple of eight.

Element 5 "Encrypted Data" in this table of Sensitive Data Encryption Transport Fields is the cipher text, which results from encrypting the data present in the XML structure <EncData>. <EncData> will contain either <T2>, where the card Track 2 image is read, (or <ExpDte>, and optionally <IssNum> and <EfctDte>), where the data is entered manually. The structure is encrypted as described in 5.3.2. Please refer to 4.3.1 for the XML structure.

5.6.5 Message Authentication Code Key Transport Fields

The XML <MAC> field will contain the content of Message Authentication Code Key Transport Fields represented in Base64 encoded form. The MAC field within the Transport fields will be a zero length field before the MAC is calculated. See 5.3.3. The Base 64 representation of the MAC blob will be inserted into the XML structure MAC field after it has been computed across the complete <NBAMsg> Element.

Element		Size	Content
1.	Type	1 Octet	Value = 3 (binary)
5.	ZMK Tag	8 Octets	Key tag (identity) associated with the ZMK used to encrypt the MAC Key.
6.	Key value	16 Octets	The MAC working key encrypted under the sender's current ZMK as identified in element 2.
7.	MAC	4 Octets	The MAC computed over the message and the above "attributes" (elements 1 to 3 inclusive).

5.6.6 Key Encryption

All the Network Banking Working Keys are Double length DES keys. Working Keys shall be encrypted as specified in ANSI X9.17 / ISO 8732. Each working key shall be represented as a 128-bit string with odd parity prior to encryption. The ZMK used to encrypt the Working Key will be modified by a variant as defined in Section 5.7.5 prior to use.

FUJ00001624

5.7 Zone Key Agreement

5.7.1 ZMK Distribution

ZMKs for this interface will be generated at the NBE. Each ZMK will be allocated a Tag by which it can subsequently be identified. See Section 5.7.5.1 for a definition of the tags.

ZMKs will be distributed as two separate components:

- Each component will be the same length as the key
- Components will be represented in hexadecimal format.
- Hexadecimal digits shall be grouped for ease of readability. Each group of 16 hex digits shall be further sub-divided into groups of four digits e.g.

  ```
  0123 4567 89AB CDEF

  0246 8ACE 1357 9BDF
  ```

- Each component will be adjusted to have odd parity prior to representing it in hex form (as per ANSI X9.24 Appendix C)
- The ZMK will be formed by exclusive-ORing the binary representation of the components. The resulting key may be adjusted for odd parity as required.
- A Component Check Value (CCV) will be calculated for each component. The CCV will consist of the leftmost four hexadecimal digits from the ciphertext produced by encrypting a 64-bit binary zero value with the subject component.

Components will be transported on paper using secure mailers that do not reveal the value of the component or its CCV until opened. Manual procedures will ensure that the components are kept separate at all times.

Each key mailer containing a component and its CCV will also contain the following data:

- the relevant key Tag that identifies the ZMK of which it is a part,
- the component number (e.g. Component 1 of 2), and
- the date of generation of the corresponding ZMK with the month in letters (e.g. 5 APR 2002).

These elements will be visible without revealing the value of the component.

A Key Check Value (KCV) will be calculated for each ZMK. The KCV will consist of the leftmost four hexadecimal digits from the ciphertext produced by encrypting a 64-bit binary zero value with the subject key.

Horizon key holders will enter the key components without verifying the component check values. The Key Manager will combine the components to construct the key and verify the key check value.

The KCV for the complete key shall be provided on a separate mailer. Each key mailer containing a KCV will also contain the following data:

- the relevant key Tag that identifies the corresponding ZMK,
- an indication that the mailer contains a KCV, and

FUJ00001624

- the date of generation of the corresponding ZMK with the month in letters (e.g. 5 APR 2002).

These elements will be visible without revealing the value of the component.

5.7.2 Key Stores

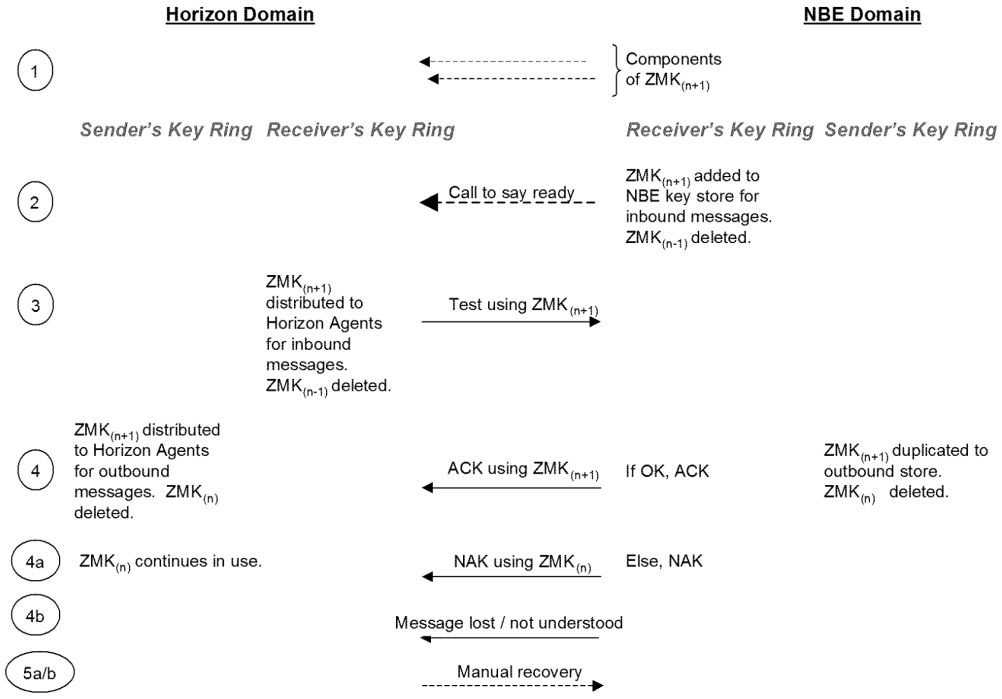
Conceptually, each party keeps two key stores (or key rings):

- The Sender's Key Ring has keys used to protect outbound messages. It will contain a single ZMK used to encrypt the Working Keys that protect outbound messages. It may also contain the corresponding Working Keys if the originator chooses to regenerate them once per day. The identity of a ZMK that is selected is included in the outbound message.

- The Receiver's Key Ring contains keys used to process inbound messages. It will contain up to two ZMKs required to decrypt Working Keys used to protect inbound messages. No Working Keys are stored since Working Keys are always carried with the message. The message receiver does not have the concept of a 'Current' key. The message that is received will contain the identity of the ZMK that he is required to use, and the receiver can thus pick this key off its receiver's key ring.

5.7.3 Zone Master Key, ZMK, Life Cycle

The ZMK Key Life Cycle and key change process is illustrated in the following figure:



The following explains the steps illustrated:

1. A new set of components are generated at NBE and communicated to Horizon using secure procedures.

2. On a date agreed between the key management officers at the two sites, the components are entered into the NBE.

FUJ00001624

- The components are combined to form the "new" ZMK which is added to the NBE's Receiving Key Ring.

- Any existing previous ZMK[4](superseded before the current cycle) is deleted.

- In the event of errors in components or key check values, the process is halted whilst the error is resolved.

- On completion, the NBE key management officer advises the Horizon key management officer that the new key has been successfully installed.

3. Horizon installs the new ZMK to its receiving key rings (one per Agent). When all Agents have installed the new ZMK, each Agent sends one or more Key Test Messages to NBE. The first test message is Horizon's commitment that all its Agents are ready to receive business traffic protected under the new ZMK. The test message has a MAC, which is generated using a Working Key protected by the new ZMK.

4. On receipt NBE will validate the MAC and retrieve the Key Tag that identifies the ZMK. If successful, NBE copies the ZMK to its sending key ring, replacing any other ZMK that is there[5]. Any subsequent outbound messages from NBE will contain a Working Key encrypted under this ZMK.

   NBE sends a Key Acknowledgement Message to Horizon advising the success (or failure) of the process[6]. The message has a MAC, which is generated using a Working Key protected by the now current ZMK. It will contain the Tag that identifies the key. A positive acknowledgement is NBE's commitment that it is ready to receive business traffic protected under the new ZMK. [KA] key acknowledgement messages should be returned on the same connection.

   4a. If the MAC fails or the NBE cannot locate the identified ZMK, no key updates are performed. A negative acknowledgement is sent with a MAC and a MAC key protected by the current ZMK (n).

   4b. If no response is received by Horizon, manual processing is required.

   After sending a positive acknowledgement to a [KT] message for a new Acquirer ZMK, the NBE will use that ZMK for all outgoing messages. Incoming messages from other queues may contain working keys, protected by this new ZMK(n+1) or the previous key ZMK(n).

5. Horizon validates the MAC on the Key Acknowledgement Message:

   5a. If the acknowledgement is positive, the new ZMK is securely copied to all Agents for protecting the Working Keys associated with all subsequent outbound messages. The previous ZMK is deleted from the sending key ring.

   5b. If the Key Acknowledgement Message is either an error indication (NAK) or it fails authentication, manual recovery is required.

On satisfactory completion of setting the new ZMK current, a replacement set of components is generated and distributed as per step (1). This ensures that there is a contingency ZMK that can be set live quickly in the event of an emergency. If that emergency involves the suspected compromise of a ZMK, the update process will need to be performed twice to ensure all compromised keys are flushed out of the system and are not retained as previous.

5.7.4 Zone Master Key Management Messages

The Security Key Test (KT) and Security Key Acknowledge (KA) messages are defined in Section 3.2.

[4] i.e. one which has been positively confirmed at step 4.

[5] No update is required if the message is a duplicate i.e. the Tag identifies that the key is already on the key ring. However a positive acknowledgement should still be sent.

[6] In exceptional cases where the NBE has no current ZMK (e.g. a failure during the first-ever key exchange), no MAC can be created and thus the failure is communicated using manual procedures.

FUJ00001624

5.7.5 ZMK Variants

Messages from the NBE to Horizon will be MACed, with a key that is transported with the message under the protection of the defined variant of the ZMK, as required by the Atalla card . Messages from Horizon to NBE will not use the variant and will thus have one or more Working Keys under the protection of the unmodified ZMK.

The defined variant is: hex (98000000 00000000 98000000 00000000)

5.7.5.1 Key Tags

Each key has a unique tag or identity allocated by the party that generates it. It is a security requirement that the identity does not reveal anything about the value of the key. The tag:

- Allows the recipient of a message that does not contain a key to work out whether or not they have the right key and which key should be used.
- Assists in the correct identification of ZMK components prior to loading them.
- Assists the Key Management Officers to diagnose failures.

A key tag has 4 numeric fields separated by a period character: 1.2.3.4 where field is a number in the range 0 to 65535 (i.e. 16 bits). The form is similar to that of an IP address.

The following convention is used for the field contents:

1. is a country code –always 44 - i.e. it is not used, but has to be there.
2. is used to identify the 'type' of key (e.g. MAC, PIN encryption or Sensitive Data encryption) (ICLP also call this a protection domain). This is not the algorithm used (like DES or RSA), but the purpose to which the key is being put. Value 03242 identifies Zone Master Keys (ZMK).
3. is used to identify the owner of a key (e.g. the Horizon KMA). Note this concept is not very useful in NWB, but becomes necessary where Horizon has 20,000 keys of a given type. Value 60116 has been allocated to keys owned by NBE.
4. is split into 3 sub-fields:
   a) The most significant digit identifies an algorithm (e.g. MAC or DES). Value "3" – (triple) DES.
   b) The next digit identifies test keys (set to zero for production keys and 9 for test keys)
   c) The remaining 3 digits are a sequence no. (which can cycle back to 1 if 999 is reached).

The Tags identified for this interface are:

Key type	Field 1	Field 2	Field 3	Field 4
ZMK	00044	03242	60116	30xxx

Where a key tag is represented in a human-readable form (e.g. on key mailers), it is represented as four sets of five decimal digits separated by a period (.). Where the Tag is represented in a blob (see Section 5.6.3 onwards), it will be represented as four 16-bit unsigned binary integers, each of which is big-endian i.e. 8 bytes. When transmitted in [KT] and [PR] messages it will also be represented as four 16-bit unsigned binary integers, each of which is big-endian i.e. 8 bytes, then padded with an additional byte '=' and Base64 encoded to become 12 bytes.

FUJ00001624

6 Operational Procedures

6.1 Processing Cycles

This interface relates to online message exchange to support real time financial transactions.

Stale messages are discarded before transmission or on receipt, as appropriate. Please refer to section 6.4for details of which message types can be discarded (i.e. non "Must deliver" messages).

The timeout associated with each message type is addressed in the NBE Operational Level Agreement, Reference [6].

6.2 Transfer Initiation

All transfers defined in this AIS are automatic.

6.3 Security Procedures

Manual Procedures are required to support the above key management protocol, as described in Section 5 above. They will need to be agreed between the Horizon operator and the NBE operator for inclusion / reference in the Operational Level Agreement (OLA) between them.

1. Generating and despatching a new set of ZMK components at NBE.
2. Receipt and installation of a new set of ZMK components at Horizon.
3. Putting a new ZMK live at NBE and Horizon.
4. Requesting a new set of ZMK components from NBE.
5. In addition, internal procedures will be required at NBE and Horizon to handle:
6. The secure storage and retrieval of ZMK components between the time that they are received and the time that they are put live.
7. Distribution, storage and retrieval of components to back-up / disaster recovery sites.
8. The secure destruction of the paper mailers used to exchange and store components.
9. The handling of Storage Master Keys (or their equivalent) used to protect local key stores.

6.4 Fallback Procedures

Fallback procedures are not addressed in this AIS.

Restoration of the interface and the disposal of stale messages (other than "must deliver" messages) is expected to be automatic. [R], [A], [KT], [KA], [PS] and [PR] messages awaiting transmission at the time of failure can safely be discarded, as the integrity of the transaction is protected by timeouts.

In general, if a process on either side of the interface can process the data passed to it, it will do so even if it does not fully conform to the rules defined in this AIS. However should a MAC be found to be invalid the message will not be processed. Any message that cannot be processed will be logged by the receiving system and manual processes will be required to resolve any consequent issues.

FUJ00001624

Should the systems at either end of the interface (or the infrastructure that makes up the interface) fail, then any outstanding Transient messages (ie [R], [A], [KT], [KA], [PS] or [PR] messages) will be discarded. The design of the end-end application message flow and business logic permits such discards without impact on the overall operational integrity of the Network Banking service. In particular failure of [R] or [A] messages requires the Horizon system to decline the attempted transaction and the NBE to undertake any subsequent required adjustment to the bank financial position as a result of such declined transactions. .

Failures which impact transient messages do not require recovery actions to ensure their eventual delivery. In the case of non-transient data from Horizon to the NBE, Horizon will retain such messages and they will be resent once a connection is found to be re-established (by means of periodic echo tests). In the case of messages from the NBE to Horizon, the NBE will continue to retain messages and Horizon will resume the fetching of such messages as soon as connections are re-established.

Please note that there may be manual operational re-alignment required should messages that were thought to have been delivered turn out to have been lost.

6.5 Control

The interface must be resilient to duplicate messages, which may occur after recovery of any element in the system, but are not otherwise expected to occur.

Lost or discarded messages are handled by timeout processing at every stage of the “RA” message sequence, to ensure that incomplete transactions are declined if unauthorised or reversed if authorised.

FUJ00001624

7 Appendix A

7.1 Transaction Type Enumerators

The following table shows the values for Horizon message element Txn_type. For example, a value of 14 means a Withdrawal with balance transaction with Signature Verification; a value of 22 means a Deposit with No Verification.

Transaction Type	Code for PIN Verification	Code for Signature Verification	Code for No Verification
Balance enquiry	01	11	N/A
Deposit	N/A	N/A	22
Withdrawal	03	13	N/A
Withdrawal with balance	04	14	N/A
Withdraw Limit	05	15	N/A
Change PIN	06	N/A	N/A

7.2 Discrepancy Reason Codes

The following reasons will be provided with Reconciliation Exception [D] messages sent by the NBE to Horizon

Discrepancy Reason Code	***Discrepancy Reason***	***Discrepancy Value***
01	Late [C2] Decline for [A1] Approve	Approved Amount
02	Unmatched [C2] after X days	Zero
03	Stand Alone Reversal	Zero

7.3 Response Codes

This is the code, included in the [A2] message, indicating the Bank's view of the transaction. The following meanings have been identified:

- 01 = Authorised OK
- 02 = Declined – Impound Card
- 03 = Declined – Incorrect PIN
- 04 = Declined – Insufficient Funds
- 05 = Declined – Usage Violation (frequency)
- 06 = Declined – Usage Violation (amount)
- 07 = Declined – Transaction not supported

FUJ00001624

- 08 = Declined – Other
- 2n = Failed by NBE
- 3n = Failed by Agent
- 4n = Failed by Counter

Please note:

Values between 20 and 29 are reserved for "Failed by NBE"

Values between 30 and 39 are reserved for "Failed by Agent"

Values between 40 and 49 are reserved for "Failed by Counter".

7.4 Transaction Result Code

- 01 = Transaction Completed OK
- 02 = Transaction Abandoned by Clerk
- 03 = Customer Signature Fail
- 04 = Fee Customer Declined
- 05 = Card Check Failed
- 06 = Decline Confirmed
- 07 = Transaction Failed

7.5 Balance Type

- 00 = Unknown;
- 01 = Account ledger balance;
- 02 = Account available balance;
- 03 = Amount owning;
- 04 = Amount due;
- 05 = Account available credit;
- 16 = Credit line;
- 20 = Amount remaining this cycle;
- 40 = Amount cash;
- 56 = Hold amount;
- 57 = Pre-authorised amount;
- 58 = Authorised amount
- 90-99 = Reserved for future use

7.6 Network Management Response Codes

- 00 = Positive acknowledgement, Use in PR and KA from 1st Horizon Agent promoting the NBE ZMK n+1;

FUJ00001624

- 01 = Positive acknowledgement, Used in KA from subsequent Horizon Agent where ZMK Tag is current NBE ZMK Tag;
- 12 = Negative acknowledgement, ZMK Tag unrecognised;
- 13 = Negative acknowledgement, ZMK Tag inactive (superseded).
- 21 = MAC is invalid.

7.7 Message Type Enumerators

- R2 – Authorisation/Financial Transaction Request
- A2 - Authorisation/Financial Transaction Request Response
- C2 - Confirmation
- C4 - Confirmation
- D – Reconciliation Exception
- KA – Security Key Acknowledge
- KT – Security Key Test
- PS – Echo Test
- PR – Echo Test Response

7.8 Record Type Enumerators

- CH = Control File Header
- CF = Control File Record
- SH = Segment File Header
- ST = Segment File Trailer

Segment File Records are in native XML.

End of Document