FUJ00001902

EMV – Banking and Retail

NBX - POCA Technical Interface Specification (TIS)

ROLE	NAME	AREA OF RESPONSIBILITY	SIGNATURE	DATE
Authors	Mark JaroszKlaus Löffler on behalf of Post Office Ltd	**Business Architecture**		
		Product Deployment		
		Technical Architecture		
DA Sign-off (Peer Reviewer)	David Gray	**Design Authority**		
Programme Director	Beverley Dunn	**Project Delivery**		

FUJ00001902

Formatted: Font: 8 pt

1 Document Control

1.1 Document Information

Horizon Release No:	S750
Document Title:	EMV Banking and Retail: NBX – POCA Technical Interface Specification
Document Type:	Technical Interface Specification
Abstract:	This document defines the technical interface between the Horizon domain and Post Office Card Account
Document Status:	~~Draft~~Approved
Originator & Department:	David Gray Design Authority
Contributors:	
Post Office Distribution:	Design Authority – David Gray POL Document Control – Post Office Programme Office
Supplier Distribution:	EDS: Steve Leek Fujitsu Services: Klaus Löffler
Client Distribution:	N/A

Table 1: Document Information

1.2 Document History

Formatted Table

Version	Date	Reason for Issue	Associated WP / CT
0.1	10 Nov 2003	First working draft. Based on document produced by IBM entitled "Network Banking Engine: POCA Technical Interface Specification" (Version 2.0)	
0.2	26 Nov	Updates taking into account decisions reached at meetings between Post Office Ltd EDS, CitiCorp and Fujitsu Services,	
0.3	2nd Dec	Update following review on 27th Thursday between Post Office Ltd, EDS, CitiCorp and Fujitsu Services.	
0.4	6th Dec	Update following review on 5th December between Post Office Ltd, EDS, CitiCorp and Fujitsu Services.	
1.0	19TH Dec	Update following review on 17th December between Post Office Ltd, EDS, CitiCorp and Fujitsu Services.	
2.0	14th October 2004	Version for approval	

Formatted: Superscript

FUJ00001902

Formatted: Font: 8 pt

Table 2: Document History

1.3 Change Process

Any changes to this issued version of this document will be made, controlled and distributed by: -

Bob.Booth GRO

1.4 Review Details

Review Comments by :	
Review Comments to :	

Mandatory Review Authority	Name
Post Office Ltd	Beverley Dunn, David Gray, Post Office Ltd
Fujitsu Services Ltd	Tony Drahota
JP Morgan	Ed Koslow
EDS	Steve Leek
Optional Review / Issued for Information	
Post Office Ltd	Bob Booth, Keith Fowler, Jason Slatcher
JP Morgan	John Ibbitson
EDS	Gerrard Burras
Fujitsu Services Ltd	Mark Jarosz

1.5 Changes in this Version

Version	Changes
0.1	First working draft – based on IBM document "Network Banking Engine: POCA Technical Interface Specification" (version 2.0)
0.2	Second working draft with main changes being load balancing and active – active working across both NBX sites.

FUJ00001902

Formatted: Font: 8 pt

Version	Changes
0.3	Third working draft updated as a result of "page turning " review. Changes were made to the document during this review. Subsequent to the review the following main changes were made; 1. New section named Message Exchange patterns 2. Additional Text in section 4.2 Layers 1 and 2 – Physical and Link to cover interface assignment and use of BGP Routing protocol for selecting interfaces. 3. Completion of Appendix A and Appendix B There are 6 DN's in this version.
0.4	Third working draft updated as a result of "page turning " review on 5th December. Changes were agreed and made to the document during this review. Visio 2000 diagrams included as object within document.
1.0	Version for acceptance updated as a result of "page turning " review on 17th December. Changes were agreed and made to the document during this review. Vision diagrams included as pictures. Version 0.4, which included these as embedded objects, caused printing problems.
2.0	• Author changed to Mark Jarosz • Horizon release changed to S75 • Document Status changed to Approved • Header updated to include Horizon reference • Footer date changed to saved date

Formatted: Bullets and Numbering

Table 3: Changes in this Version

1.6 Key Contacts

Name	Position	Phone Number
Bob Booth	Solutions Architect	GRO

Table 4: Key Contacts

FUJ00001902

Formatted: Font: 8 pt

1.7 Associated Documents

	Reference	Version	Date	Title	Source
1.				CAPO Application Interface Specification (AIS)	Post Office
2.				OSI/ISO Reference Model	ISO
3.				Network Support: Operational Level Agreement between Post Office and EDS	Post Office
4.				RFC 896 Congestion Control in IP/TCP Internetworks	http://www.ietf.org/rfc.html
5.				NBX CAPO Rec & Sett AIS	

Table 5: Associated Documents

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

FUJ00001902

Formatted: Font: 8 pt

Table of Contents

1 DOCUMENT CONTROL 2

1.1 Document Information 2

1.2 Document History 2

1.3 Change Process 3

1.4 Review Details 3

1.5 Changes in this Version 3

1.6 Key Contacts 4

1.7 Associated Documents 5

2 INTRODUCTION 9

2.1 Purpose 9

2.2 Scope 9

2.3 Structure 9
2.3.1 Introduction 9
2.3.2 Environment 9
2.3.3 Medium of Transfer 10
2.3.4 Operational Considerations 10
2.3.5 Security 10
2.3.6 Recovery Facilities and Procedures 10

2.4 Terms and Abbreviations 10

3 ENVIRONMENT 11

3.1 Introduction 11

3.2 Context 11
3.2.1 Design Principles 11
3.2.2 Location of NBX – POCA Physical Interface 13

3.3 Components 14
3.3.1 Wide area Network Links 14
3.3.2 NBX Server's 14
3.3.3 NBX File Transfer Server 14
3.3.4 POCA Servers 15
3.3.5 Routers 15
3.3.6 Security Hardware 16

4 MEDIUM OF TRANSFER 17

4.1 Interface Overview 17

FUJ00001902

Formatted: Font: 8 pt

4.2 Layers 1 and 2 - Physical and Link 17

4.3 Layer 3 – Network 18
4.3.1 Control Plane 18
4.3.2 Data Plane 18
4.3.3 IP Address spaces 18

4.4 Layer 4 Transport 19
4.4.1 Transport Level interface 19
4.4.2 TCP Keep Alive 19
4.4.3 TCP Data Flow 20
4.4.4 Application EndPoints 21
4.4.5 Migration of IP Address to another Computer System 21
4.4.6 TCP Connection Management 21
4.4.7 Load Distribution 22

4.5 Layer 5 – Session Layer 24

4.6 Layer 6 – Presentation Layer 24

4.7 Layer 7 – Application Layer 24
4.7.1 Interface to Transport Layer 24
4.7.2 Reconciliation File Transfer 25
4.7.3 Communications Handling 26
4.7.4 Handshakes 26
4.7.5 Acquirer Working Key (AWK) Exchange 26
4.7.6 Delay ("Stand In") Processing 26
4.7.7 Message Exchange patterns 26

5 OPERATIONAL CONSIDERATIONS 28

5.1 Systems Management 28

5.2 Network Management 28

5.3 Restarts 28

5.4 Resilience and Fail Over 28

5.5 Performance 29
5.5.1 POCA and NBX Platforms 30
5.5.2 Wide Area Network 30

6 SECURITY 31

6.1 End-to-End Identification 31

6.2 Encryption and Decryption Methods 31
6.2.1 Network data privacy and authentication 31

6.3 Application Key Management 31

6.4 Protection 32

6.5 PIN Encryption 32

6.6 PIN Block Format 32

FUJ00001902

Formatted: Font: 8 pt

6.7 Key Changes 32
6.8 Key Ownership 33
6.9 Line Encryption 33
6.10 Firewalls 33
6.11 Network Infrastructure 33
6.12 POCA Authorised Engineering access to NBX locations 33

7 RECOVERY FACILITIES AND PROCEDURES 34

7.1 Fault Detection 34
7.2 Disaster Recovery Environment 34
7.3 Disaster Recovery Testing 34
7.4 Disaster Recovery Invocation 34
7.5 POCA Move to DR Processing 34
7.6 NBX Move to DR processing 34

APPENDIX A – DETAILED CONFIGURATION INFORMATION 35

APPENDIX B – TESTING 40

FUJ00001902

Formatted: Font: 8 pt

2 Introduction

2.1 Purpose

The purpose of this Technical Interface Specification (TIS) is:

- To specify the technical details of the interface between the Post Office Network Banking Switch (NBX) system and the host systems of Post Office Card Account (POCA) operated by EDS.
- To provide the Network Architects with sufficient detail to implement the NBX – POCA connection.
- To provide a consistent communications vehicle amongst the technical teams responsible for providing the various nodes and connections comprising the interface.
- Act as a base document against which project change control is assessed when implementing changes to the NBX – POCA connection.

2.2 Scope

This TIS describes an interface for exchange of information between NBX and POCA computer systems primarily for the online message components. Details about the CONNECT: Direct usage will be found in Ref 5

The interface is defined at two levels:

The Application level, concerned with the application data passed across the interface

The Technical level, concerned with the mechanisms by which the data is passed across the interface.

This document covers the specification of the technical mechanisms by which information is passed between the NBX and the POCA system.

This document does not cover the description of the information in terms of record/field structure and the meaning ascribed to information by either party. This aspect is addressed in the Application Interface Specification [Ref. 1]

This document does not describe internal interfaces within supplier domains (e.g. between production and DR instances).

This document is concerned only with the specification of information that is both computer-generated and computer-consumed. Specifically manual procedures, such as Master Key Exchange (for example), are excluded. Details of the procedure for Master Key Exchange are documented in Network Support: OLA between PO and EDS [Ref. 3].

2.3 Structure

2.3.1 Introduction

This section describes the structure of the remainder of this specification.

2.3.2 Environment

This section describes the context and major components of the NBX and POCA environment.

FUJ00001902

Formatted: Font: 8 pt

2.3.3 Medium of Transfer

This section describes the interface in terms of the various ISO OSI Reference Model layers [Ref. 2].

2.3.4 Operational Considerations

This section considers the operational impact and characteristics of the interface.

2.3.5 Security

This section covers the security aspects of the interface.

2.3.6 Recovery Facilities and Procedures

This section deals with disaster recovery design, facilities and procedures.

2.4 Terms and Abbreviations

Abbreviation	Explanation
AIS	Application Interface Specification
ARP	Address Resolution Protocol; this protocol determines which Ethernet Address corresponds to a given IP address
AWK	Acquirer Working Key
AZMK	Acquirer Zone Master Key
BGP	Border Gateway Protocol, a protocol used by Routers to determine which interface to use for forwarding IP Datagrams
DES	Data Encryption Standard
DKMS	IBM Distributed Key Management System
DR	Disaster Recovery
EBT	Electronic Benefits Transfer
HSRP	Cisco Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NBX	Network Banking Switch, part of Horizon and operated by Fujitsu Services on behalf of POL, that handles the interface between the PO counter systems and the Financial Institutions (FI). The NBX allows Post Office outlets to transact automated banking services.
OSI	Open Systems Interconnection
PI	Processor Interface. Interfaces to the module which handles the communications in order to obtain data from external systems.
POCA	Post Office Card Account
PVC	Permanent Virtual Circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP MSS	The TCP maximum segment size is the maximum number of TCP bytes that can be carried in a single IP datagram.
TIS	Technical Interface Specification
VIPA	Virtual IP addressing
VPN	Virtual Private Network
WAN	Wide Area Network
IPSEC	IP Security Protocol, provides crypto at the IP layer by encapsulating IP within IP.

FUJ00001902

Formatted: Font: 8 pt

3 Environment

3.1 Introduction

This section presents an overview of the context in which POCA and NBX operate and provides a lower level description of the components that are concerned directly with the operation of the Interface being described in this document. The approach taken to determine if a component is directly concerned with the interface operation is based on the following:

- The Transport protocol is TCP/IP and this can be visualized as a two-way pipe into which bytes are written and /or read. In general, this 'pipe' terminates on two different computer systems.
- The Components directly concerned with the Interface are taken to be both those that terminate the TCP 'pipe' and all other components through which the IP datagrams that implement the 'pipe' may flow. These may be Servers, Network links and /or Network devices such as Routers etc.

In the context of this document, unless specified otherwise, reference to POCA is the domain operated by EDS running the host systems of Post Office Card Account on behalf of Post Office.

3.2 Context

Figure 1 shows the context of the NBX and POCA systems excluding test systems.

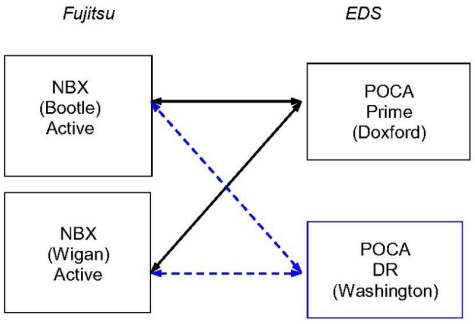


Figure 1 – NBX and POCA Context

Interfaces between POCA prime and disaster recovery sites are excluded from this specification. Only one POCA site will be running the production service at any time.

Functional testing capabilities will be provided by NBX Feltham and POCA DR location. It should be noted that the Test Environments have constraints, they are not identical replicas of the live system and as such testing will need to be calibrated to give representative results.

3.2.1 Design Principles

The following principles govern the design and implementation of the interface:

FUJ00001902

Formatted: Font: 8 pt

- No single failure[1] will impact the service offered to customers. In the event of a single failure, the full load will still be supported.
- Each physical communication line has a backup line. Following a failure of a component on one physical line the backup is capable of handling peak transaction volume on its own.
- Each physical communication line is routed via a different telco exchange, enters the building at a different point and approaches the building from a different direction.
- Hardware is selected and configured for fault tolerance and availability.
- The connection will be terminated with multiple boards, multiple ports and sockets.
- The Applications should be logically configured to use multiple threads so that loss of a thread does not impact the service to customers.

[1] A composite device such as a single server is acceptable as long as it is not itself susceptible to internal single points of failure. There are no known single points of failure relating to this interface.

FUJ00001902

Formatted: Font: 8 pt

3.2.2 Location of NBX – POCA Physical Interface

The interface is shown on the diagram, 'mid span' between the cables that connect the mutually facing Router pairs. EDS supply two routers at each NBX site, two routers at the EBT (Electronic Benefits Transfer) primary site and two routers at the EBT DR site. Fault Tolerant Firewalls will be provided at both EBT Primary and DR sites. There is one EBT server at each site; one Primary and the other DR. Encryption over the links will be provided using Cisco software encryption (IPSEC).

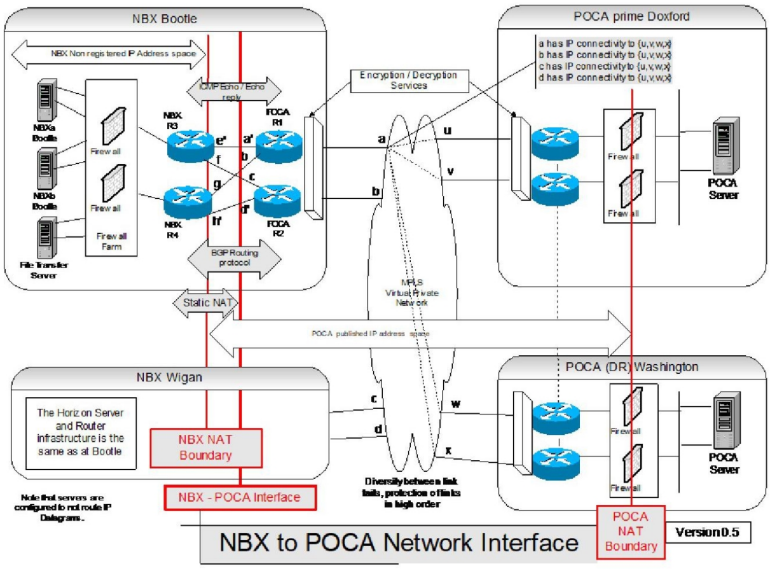


Figure 2 – NBX – POCA Physical Interface

Specific characteristics of the Interface are documented in the following table.

Boundary	Overview
Component	EDS will provide and manage all components to the right of the line labelled NBX - POCA interface in Figure 2. NBX supplies the cables for the connections between the POCA Routers and the NBX Routers. Within the NBX locations, rack space* will be made available for the POCA Routers. These Routers will have connections to: The WAN circuits from the telecommunications provider The NBX Routers * Separate racks and power supplies within each NBX Data Centre.

FUJ00001902

Formatted: Font: 8 pt

Network Management	The POCA Routers are fully within the POCA Network Management domain. The NBX Routers are fully within the NBX Network Management domain. The Connections between the POCA Routers and the NBX Routers fall into both the POCA and NBX Network Management domains as far as monitoring is concerned. This is possible since the POCA Routers will respond to ICMP Ping requests received from the NBX Routers and similarly the NBX Routers will respond to ICMP Requests received from the POCA Routers.
Operational	The POCA Routers located at the NBX location are operated remotely. Once these Routers have been commissioned, occasional and infrequent physical access may be required, for example to replace a faulty component. The Connections between the POCA Routers and the NBX Routers are placed within the same Operational domain as the NBX Routers. Changes will only be made to the Connections under agreed procedures. Performing these procedures will require agreement from both Network management domains.
Environmental	Since the POCA Routers are physically located near the NBX, then responsibility for providing a suitable environment for these falls to the NBX provider.

Table 6 Interface Characteristics

3.3 Components

3.3.1 Wide area Network Links

There is an IP Select MPLS VPN cloud between the two POCA locations and the two NBX locations. All links into NBX locations are diverse. Similarly all the links into both the POCA locations are kept diverse in order to provide resilience to the failure of one link. The term diverse is used to denote physical separation and termination of the 'tail circuits' from the Telecommunications provider. Encryption is provided using Cisco Router encryption

3.3.2 NBX Server's

There are two separate Computer Systems (NBXa and NBXb) that contain the interface endpoints on the Horizon side.

(Each of these Computer systems consist of two computer platforms in an active / standby arrangement).

Hardware	Fujitsu Server
Software	Windows 2000
	NBX Agent Application
Security Hardware	Integral HSM).

3.3.3 NBX File Transfer Server

Hardware	Fujitsu Server
Software	Windows 2000
	CONNECT: Direct

FUJ00001902

Formatted: Font: 8 pt

3.3.4 POCA Servers

POCA will be running one fault tolerant HP Non-Stop Server at each of the primary and disaster recovery locations. The Server will consist of multiple CPUs and communication cards providing the capability of supporting multiple physical and logical connections to the NBXsystem. This also provides the needed redundancy to mitigate against single points of failure from hardware/network/software failures.

Normally the POCA processes will run at the primary location, with Computer Systems at the disaster recovery location providing "hot standby" of data.

3.3.5 Routers

Cisco routers are used for Fujitsu Services provided routers.

Cisco routers are used for POCA provided routers.

FUJ00001902

Formatted: Font: 8 pt

3.3.6 Security Hardware

The NBX and POCA configurations include firewalls and routers to implement security policy for enabled ports and addresses. The network infrastructure also includes Triple DES cryptographic capability although this is implemented within the routers.

The application key management software is part of the NBX and is used to store the zone master key received from POCA.

The NBX and POCA configurations include hardware cryptographic features to conform to the requirement for PIN block Encryption. PIN blocks are Triple DES encrypted.

FUJ00001902

Formatted: Font: 8 pt

4 Medium of Transfer

4.1 Interface Overview

The Interface between NBX and POCA is a telecommunications link. All data passes on this link except the three Zone Master Key components which are passed in securely printed envelopes at intervals between six and twelve months. This Key transfer and its associated procedures are outside the scope of this document.

The online interface between POCA and NBX will support a set of messages as described in the AIS [Ref. 1].

The OSI Reference model is used as a convenience to structure the documentation of interface components, starting at the Physical level.

4.2 Layers 1 and 2 - Physical and Link

At Bootle and Wigan, a resilient pair of POCA Routers connects directly (using cross over cables) to the pair of high performance NBX Routers. The Router Interfaces are Fast Ethernet and to avoid any issues of interoperability, Cisco data Routers are used to satisfy agreed service levels.

To keep things simple and avoid issue with Asymmetry in data flow the following Router Interface assignment is proposed on the POCA Router pair and Mirrored on the NBX Router pair. This will have the effect of ensuring that in non-failure scenarios, the same physical connection is used for all IP datagrams. This facilitates diagnosis of problems and ensures that 'out of order' packets do not impact performance.

Router	Interface
POCA Router 1 – Primary	Interface a Primary Interface Interface b Secondary Interface
POCA Router 2 - Secondary	Interface c Secondary Interface Interface d Primary Interface
NBX Router 4 – Primary	Interface e Primary Interface Interface f Secondary Interface
NBX Router 5 – Secondary	Interface g Secondary Interface Interface h Primary Interface

Please refer to Figure 2 – NBX – POCA Physical Interface for details of Router and Interface labelling. So for example in the no failure scenario, all IP Datagrams will flow between 'Interface a' and 'Interface e'. Note the interface labels are unique across all four Routers. Note that in practice the above specification will be exceeded in the sense that asymmetric routing will be avoided in most failure scenarios, for example by weighting of all interfaces and use of BGP to select the "best interface".

The above interface assignment applies at both Wigan and Bootle locations.

Level 2 traffic will consist of ARP and Link Quality monitoring as well as Level 3 payload.

EDS will provide Internet Protocol (IP) connectivity between the NBX and POCA.

IP Select is used to provide a virtual private network dedicated to this service. As well as the MPLS backbone network, the service includes all PVCs, routers and tail circuits together with their maintenance and management. Utilisation and performance of the circuits and PVCs and router-to-router availability is constantly measured and reported.

Network links also provide backup routes, which enter the locations at a different point and follow a different route to a second local exchange. These provisions are dependent on physical structures, wayleaves and local exchange location. The physical separation is large enough so that redundancy is not compromised by single points of failure affecting both halves of a redundant pair.

FUJ00001902

Formatted: Font: 8 pt

Two or more circuits will terminate at each data centre. The number of circuits may increase or decrease in accordance with the volume requirements of the service.

POCA ensures the onward routing of the connection between its production and contingency (DR) sites.

NBX ensures the routing from the POCA routers to relevant NBX sites.

Both of the physical NBX locations will operate a production service. Testing is supported from a separate location (refer to Appendix B – Testing).

POCA testing is provided from the POCA DR site.

4.3 Layer 3 – Network

This section is concerned with the interface description at layer 3 that is IP. For purposes of description this section is split into 3 subsections:

- Control plane, concerned with Routing and ICMP
- Data plane, concerned with actual flow of IP datagrams
- Virtual IP Addressing
- IP Address spaces, concerned with enumeration of IP address space and translation schemes

4.3.1 Control Plane

4.3.1.1 IP Routing

At Bootle and Wigan, in order to provide a fully resilient link between the pair of POCA Routers and the pair of NBX Routers, the BGP Routing protocol is used. This approach requires a cooperative approach between the POCA and NBX domains. It provides a good technical solution to maintaining resilience that is simpler than alternative level 2 schemes. The *Border Gateway Protocol (BGP)* is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies.

Access lists are used in the POCA routers to limit the Routes that can be learnt from the NBX Routers and to avoid redistribution of these further back into POCA. Similar restrictions on accepting Routes will be applied on NBX Routers.

4.3.1.2 ICMP

In order for the POCA Network management team to confirm that all Interfaces on the POCA Router pair are functioning, ICMP Ping traffic is allowed to the directly connected interfaces on the NBX Router pair. Similarly, the POCA Router pair are configured to accept ICMP Echo Requests and respond on the interface that they have directly connected to the NBX Router pair. The source IP address of these interfaces is documented in the IP Address space section.

ICMP Ping is only permitted between known hosts as specified in Appendix A – Detailed Configuration Information. Other source and destination addresses are blocked.

4.3.2 Data Plane

All traffic over the interface at level 3 is IPv4.

4.3.3 IP Address spaces

The purpose of this sub section is to:

FUJ00001902

Formatted: Font: 8 pt

- Provide an overview of the various IP address spaces from which components associated with the interface are allocated IP addresses. Note that the criteria for associating a component with the interface are stated in section 3.1.
- State the points at which Network address translation (NAT) is performed and the type of NAT.
- Enumerate the usage of IP addresses in all components associated with the interface.

4.3.3.1 Address Space Overview

There are three separate IP Address domains, NBX Non Registered, POCA Published and POCA Non Published. These are illustrated in Figure 2 – NBX – POCA Physical Interface. The Boundary between the NBX Non Registered domain and the POCA Published domain is labelled NBX NAT Boundary. Similarly the boundary between the POCA Non Published domain and the POCA Published domain is labelled POCA NAT boundary.

The NAT Boundary represents the location within the Network that Network address translation is implemented.

Note that EDS provide the POCA Published IP address space.

4.3.3.2 Network Address Translation

Network Address Translation (static with no port overloading) is performed as shown in Figure 2 – NBX – POCA Physical Interface.

4.3.3.3 IP Address usage

The IP addresses used across the interface are documented in Appendix A – Detailed Configuration Information.

4.4 Layer 4 Transport

The only Transport protocol used across the interface is TCP/IP. The mode of use is peer to peer.

4.4.1 Transport Level interface

At this level, there is no single location for the POCA NBX Interface. This is because TCP/IP is essentially a cooperative protocol between two endpoints. For example, a TCP connection exists between a component (POCA Process) located on the POCA Server and a component on the NBX. If the flow of bytes from the POCA Server to the NBX is slow then this can be caused by either the NBX reading too slowly, or the POCA process writing too slowly. Whilst these behaviours can be distinguished by observing the TCP communication, they cannot simply be differentiated at the Application interface into TCP (socket level). The consequences of this is that any measurement of service levels at the transport layer and above need to take account of this TCP connection behaviour.

4.4.2 TCP Keep Alive

The purpose of TCP Keep Alives is to detect disappearing endpoints and inform applications that a connection is broken. For example, in a client server environment, if a client fails then a listening server will not necessarily detect this. Over a period of time 100s of such stale connections may result in the server running out of resource and having to be reloaded. TCP Keep Alives are only sent when the connection has been idle for a defined time interval and thus pose very little overhead.

TCP Keep Alives are configured on Hosts either side of the Interface with values specified in the following table.

FUJ00001902

Formatted: Font: 8 pt

Refer also to section 4.7.4, which covers used of Application level 0800 echo test messages.

TCP Property	Overview	NBX	POCA
Keep Alive Idle	Seconds between each TCP keepalive segment if no data has been sent on the connection.	30	45
Keep Alive Interval	Seconds between successive retransmissions of the keepalive segment when a response to an initial keepalive is not received.	30	45
Keep Alive Retry Count	After sending (Keep Alive Retry Count) retransmissions the connection is abandoned.	5	8

4.4.3 TCP Data Flow

This section documents configuration options for TCP Data Flow behaviour and their settings.

TCP Property	Overview	NBX	POCA
Delayed Acknowledgements	When a TCP peer receives a segment, the acknowledgement of the segment is not sent immediately.	Enabled (Delay Ack Time) 5 milliseconds	Enabled 200 milliseconds
Nagle Algorithm	Please refer to RFC 896 [Ref. 4] for further details.	Enabled	Enabled
MSS Adjustment	Cisco Routers provide the functionality to adjust the MSS on a TCP connection to avoid IP datagrams that are too large to pass through the network without fragmentation and / or discard.	It is not necessary for the POCA facing Routers to adjust the MSS of all TCP connections. This is because it is not necessary as Fragmentation is avoided by Design of the WAN.	Not applicable

FUJ00001902

Formatted: Font: 8 pt

4.4.4 Application EndPoints

This section provides an illustration of Application Endpoints concerned with the NBX - POCA ISO 8583 Interface.

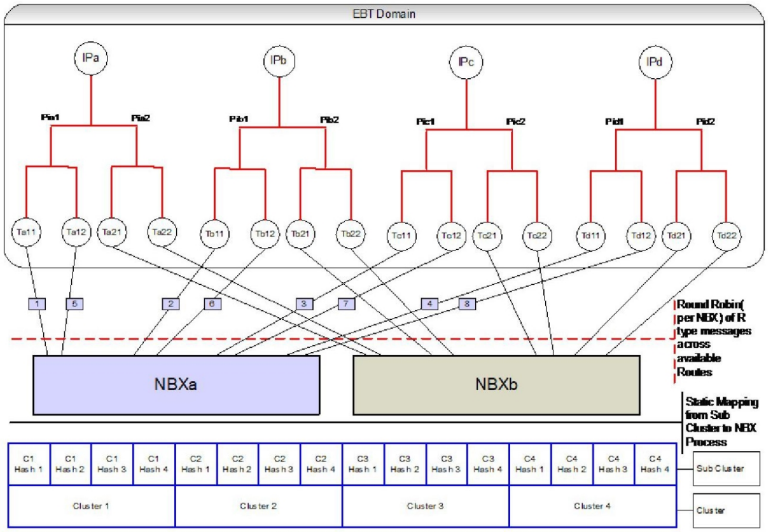


Figure 3 – Application Endpoints

4.4.5 Migration of IP Address to another Computer System

After DR invocation, the published (as visible to NBX) POCA IP addresses and ports at the DR site are identical to those in live. Fail over to the DR site will be achieved by making these IP addresses active in the sense of accepting incoming connections and ensuring that the Routing in the POCA domain is reconfigured to converge on the DR site. This is a manual process undertaken by POCA.

TCP/IP connections will fail during a machine swap over. In order to remake these connections the components will:

- For POCA - Enter into a listening state, ready to accept connections from NBX
- For NBX - Attempt to initiate connection setup by retry (after a delay of at least one second) until the connection is made.

4.4.6 TCP Connection Management

In production separate POCA threads will maintain a TCP/IP socket connection down each Ethernet Port at POCA. This configuration allows for the failure of a circuit while still maintaining full production service between POCA and NBX.

As and when required, additional TCP/IP socket connections will be established to facilitate the CONNECT: Direct transfer of the Reconciliation file.

FUJ00001902

Formatted: Font: 8 pt

At the TCP/IP communications level, connection establishment and re-establishment will be managed from the NBX end of the interface for all TCP/IP socket connections. The NBX end will use dynamic ports as detailed in Appendix A – Detailed Configuration Information

If NBX fails to establish a connection, or a connection fails it will retry connection establishment (after a delay of at least one second) until the connection is made.

Either end can terminate TCP Connections.

The above environment is replicated in the POCA Disaster Recovery site with the Test environments scaled appropriately. When testing connections are required, additional TCP/IP socket connections will be made to the TCP/IP addresses and ports nominated by POCA for their test systems. These additional testing and CONNECT:Direct sockets will be established over the existing communications infrastructure.

4.4.7 Load Distribution

NBX is responsible for the balancing of transaction volumes as explained below.

The objectives of this load balancing are twofold:

- To ensure that the POCA software processes are balanced in terms of transaction volumes and hence CPU utilisation on the POCA switch.
- To ensure that the TCP/IP processes are balanced across the PIs.

If the entire system is well balanced at the communications infrastructure and PI level then the response times across the POCA switch and communications queue times between POCA and NBX will be reduced, resulting in better overall transaction response times.

4.4.7.1 Interface Flow during Normal operation

Step	Overview
R origination	An R (Auth Request) message originates at a Post Office Counter. There are approximately 40,000 Post Office Counters and these are partitioned using a two level scheme into Clusters and sub clusters. All Counters at a Post Office Outlet belong to the same partition. 1. A Post Office is statically mapped to a Cluster using a scheme that results in 30:30:20:20 average workload profile. 2. The Sub Cluster for a Post Office Counter is determined by applying a Hash function to the Post Office FAD code (static for Post Office). The Hash Function has 4 output values. 3. The total number of Partitions (called sub clusters) is 16 (4 Clusters * 4 Hash values).

FUJ00001902

Formatted: Font: 8 pt

Step	Overview
R to NBX instance	There are two separate Computer Systems (NBXa and NBXb) that contain the interface endpoints on the Horizon side. (Each of these Computer systems consist of two computer platforms in an active / standby arrangement). The mapping from the R message to the NBX computer system will be achieved by mapping the 16 sub clusters (*) to the 2 NBX instances in a scheme, which provides for approximate load balancing. Mechanisms will be in place, which would allow the mapping to be altered during guaranteed "quiet time", specifically no Transactions can be performed. The granularity of change will be at the sub cluster level. * Note that the R message and Reversal are associated with the same sub cluster . Any alteration to the mapping will take account of late reversals.
NBX instance to Thread	The interface endpoints on the EBT side of the interface are Threads. Each Thread is associated with a particular IP address and TCP port. On this IP address and Port a TCP server is listening for incoming connections (*). There are 16 Threads and these will be partitioned by NBX into two endpoint collections {C1, C2} such that each collection has Threads associated with 4 PI's and all 4 IP addresses. The set of PI's covered by C1 will be disjoint from the set of PI's covered by C2. NBXa will be associated with C1 and NBXb with C2. Each NBX instance will attempt to maintain a TCP connection to each Thread in its associated Collection. The NBX instance will consider the TCP connection usable if no errors have been reported for the connection from the Sockets API and the backlog of outstanding (*) R messages is less than an agreed threshold (as set in configuration parameters). The NBX instance will map incoming messages as follows; 1. An R message will be scheduled to usable TCP connections (hence EBT thread) in the following manner. Consecutive attempts are targeted at the next entry in the list of PI's for this NBX instance. This is shown in Figure 3 – Application Endpoints for the case of NBXa. This is termed "Round Robin" scheduling. 2. A reversal will be scheduled to the same EBT IP address and Port as the original R message. Please refer to Message Exchange patterns section 4.7.7 for further details. *(Awaiting A or timeout)*

FUJ00001902

Formatted: Font: 8 pt

4.4.7.2 Interface Flow in failure situations

Step	Overview
NBX instance fail over	Fujitsu have two data Centres, located at Wigan and Bootle. Each NBX instance will be mapped to two computer platforms, one at each Data centre. For example NBXa will be "Active" on a Computer platform at the Wigan Data Centre and in "Standby" on a Computer platform in the Bootle Data Centre. The "Active" and "Standby" roles are agreed and maintained using a protocol between the Two Computer Platforms. 1. The "Active" instance of NBXa (and similarly NBXb) will maintain TCP connections with EBT Threads as already mentioned earlier in this document. 2. When a "Standby" instance takes over as "Active", a TCP connect followed by an application level logon will be performed on relevant PI's.

4.5 Layer 5 – Session Layer

Only NBX initiates sessions using sign on messages.

Only NBX will send log off messages.

Sign on messages are followed by transmission of an acquirer working key, AWK, from NBX to POCA. Where multiple systems or PIs are employed, a separate sign on and AWK is required for each one.

Sign on, log off and key management exchanges flow as ISO 8583 Network Management 0800 messages according to a protocol described in the AIS [Ref. 1].

4.6 Layer 6 – Presentation Layer

This is covered in the AIS [Ref. 1].

4.7 Layer 7 – Application Layer

Information regarding transmission of financial transactions and key exchanges at this layer shall be presented in the corresponding AIS.

Transfer of reconciliation information will be performed using CONNECT: Direct.

4.7.1 Interface to Transport Layer

The NBX - POCA interface is comprised of the following two major interface types:

FUJ00001902

Formatted: Font: 8 pt

- The NBX - POCA ISO 8583 Interface. This is the default Interface, used for all messages defined in the AIS [Ref.1].
- The Data Reconciliation Interface. This interface is only used for the batch file transfer (per day) of data to the Reconciliation service.

Figure 3 – Application Endpoints illustrates the relationship between the POCA processes and threads in the POCA Servers and the NBX Systems. Only some of the interface elements are shown in order to provide clarity. This is based on the following key features of the POCA Server design and how this is to be interfaced most effectively with the NBX software.

- There is one POCA HP Non-Stop server at each of the main and DR sites. There are eight POCA server processes per POCA server. NBX is responsible for load balancing as described in 4.4.7.
- The connection relationship must be maintained for certain messages (0100/0200 and the associated 0420/0421 reversal). Specifically the reversal must be delivered to the same EBT Thread as the original transaction. [Refer to the AIS [Ref.1] for the details of message relationships.]
- Each POCA server process will have two threads.
- An NBX will connect to POCA processes and threads as described in 4.4.7.
- The number and designations of TCP/IP connections is documented in Appendix A – Detailed Configuration Information. Under normal operational conditions there will be no connections made between the NBX Servers and the POCA DR site. In the event of a DR scenario then all connections will be between the NBX Servers and the POCA DR site.

4.7.1.1 Message delineation

As the messages defined in the AIS are (or can be) of variable length, a mechanism is required for the applications on either side of the interface to recognise when a complete messages has been read from the socket.

The mechanism used is for a length field to precede each message defined in the AIS. This is a 2-byte binary Big Endian[2] field.

An Application may close a TCP connection if it detects a fundamental inconsistency in the data being received which may not ultimately be recoverable by any other method (for example an invalid message length field).

4.7.2 Reconciliation File Transfer

The Reconciliation is transferred from the NBX system to the POCA system using CONNECT: Direct file transfer software from Sterling Commerce, over a TCP/IP socket connection.

The CONNECT: Direct file transfer is made between any NBX data centre and the POCA Production service. NBX is always the initiator of any File Transfer. In the event of a prolonged CONNECT: Direct file transfer failure it is assumed that WAN service can be resumed, the file transferred and the data processed at POCA all within 24 hours of link failure. Therefore there is no need for a magnetic tape standby process. Note that there is a pair of resilient links into each NBX Data centre and it is sufficient for just one link to be working in order to provide WAN connectivity for File Transfer. For this reason no standby process has been specified.

Refer to Ref 5 for details of File Naming / Paths and CONNECT:Direct Attributes.

[2] The most significant digits are in the lower memory locations, just as it would be written on paper.

FUJ00001902

Formatted: Font: 8 pt

4.7.3 Communications Handling

Application level communications handling (i.e. sign on, log off and echo testing) will be handled using 0800/0810 network management messages, as specified in the AIS [Ref. 1].

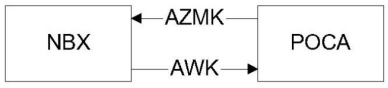
4.7.4 Handshakes

"Handshaking" (echo testing) is implemented, with a maximum interval of 3 minutes between exchanges of 0800 echo test messages in the absence of real traffic. NBX initiates these handshakes based on its own timer.

After 3 consecutive non-responses,

1. NBX will invoke Application Logon
2. Should the Application Logon not succeed, NBX will terminate the TCP connection and then try to establish another TCP connection.
3. Once the TCP Connection is established, NBX will invoke Application Logon.

4.7.5 Acquirer Working Key (AWK) Exchange



POCA generates the Acquirer ZMK (AZMK) that applies to the acquirer zone.

The Acquirer Working Key (AWK) is generated by NBX and sent to POCA in a 0800 network management message. POCA should respond to NBX with a 0810 message once the new AWK has been decrypted and applied to POCA successfully.

NBX may generate a new Acquirer Working Key at any time, and will generate and issue a new AWK upon the **sixth** failed transaction (due to PIN sanity error) for a particular PI and AWK. POCA works with two generations of AWK at all times (except PIN change transactions) to ensure the successful decryption of messages in flight at the time of key exchange.

4.7.6 Delay ("Stand In") Processing

The connection between NBX and POCA will be NBX acquiring only. Stand-In processing by the NBX is therefore not applicable to this connection. The design principles state that the service to customers not be affected by single failures, and the sizing and topology of interface components needs to reflect that. However, there may still be situations (in multiple failure scenarios) where POCA could be considered by NBX to be "in delay". In this case the NBX times out the transaction. Only repeat reversals will be queued if the connection is considered to be "in delay" In general, the reversal queue will be cleared first before any new transactions will be allowed.

4.7.7 Message Exchange patterns

This section documents associations between Application level messages and TCP Connections, PI's and Ports. It should be noted that Messages may be interleaved and there are no restrictions on the number of outstanding requests without a response.

4.7.7.1 Reversal Matching

NBX must send Reversals on the same IP and Port as the original. This is so that Reversals can be matched. Note that there is no significant difference in processing between matched or unmatched reversals. For

FUJ00001902

Formatted: Font: 8 pt

settlement however in the event of disputed transactions, it is always easier for POCA back-office operations team to research transaction sequences when there was a match.

4.7.7.2 Reversal Initiation from NBX

NBX should send Reversals only when a response has been received from EBT. If EBT never responds to a transaction, then NBX should never send an associated Reversal. This eliminates the possibility of false credits, which can be very problematic for accounts that cannot overdraw and regularly have zero balance.

4.7.7.3 Response from POCA

POCA will send responses from the same IP address and Port that the associated "Requesting" message was received on.

In the event of a TCP Connection not being available for delivery of the response message, the transaction response will be queued by POCA (up to a configurable buffer size) and forwarded as a late or unsolicited message when the TCP Connection becomes available.

4.7.7.4 Reversals in Error conditions

If the application determines it is not possible to establish or use a TCP connection after a configurable period (initially set to 5 seconds, range [0..600]) to the same IP and Port as original, then a Reversal can be sent to another IP address and Port. It will be treated as an unmatched Reversal.

4.7.7.5 Application Logon

The Application logon message exchange pattern (MEP) causes side effects at the PI level. Specifically each such MEP results in a new working key per PI. Note that there will be no sharing of AWK between NBX instances or platforms.

FUJ00001902

Formatted: Font: 8 pt

5 Operational Considerations

5.1 Systems Management

There is no Systems Management operating across the NBX - POCA Interface.

5.2 Network Management

All network components and links in the POCA Domain (that is to the right of the line labelled NBX to POCA) in Figure 2 fall fully within the scope of POCA Network Management.

In addition, the POCA-facing Interfaces in the NBX Routers in Figure 2 will have these interfaces tested for reach ability using ICMP Echo Request / Reply otherwise known as Ping.

In a reciprocal arrangement, the POCA Routers will respond to ICMP Echo Requests directed on the NBX facing Interfaces maintaining high performance and service resilience.

5.3 Restarts

The NBX and POCA exchange handshake messages at a regular configurable time interval. In the event that the party sending a handshake does not receive a response to a handshake message, business rules define the process for restart of the connection. (See AIS.)

Utilisation and performance of the circuits and PVCs and router-to-router availability are constantly measured by POCA. A joint document detailing the phone contact numbers of the various operational groups involved in the interface will be agreed, exchanged and appended to the Operational Procedures documents of each organisation. This document will be kept up to date and will only be changed by mutual consent. The diagnosis and correction of operational problems relating to the interface will be coordinated by phone contact.

5.4 Resilience and Fail Over

The following table provides a summary of the resilience mechanism for the components concerned with the POCA – NBX Interface. (The criteria for inclusion of components was stated in section 3.1).

Resilience covers:

- Detecting that a particular component is not providing service.
- Selecting an alternative component that is providing service (termed fail over in the following table).
- Periodic probing of any standby components.

FUJ00001902

Formatted: Font: 8 pt

ISO Layers	Components	Resilience Mechanisms
1,2 and 3	**POCA domain and Interface Span** Network devices and links from POCA Server (Interfaces facing towards NBX) to Routers 4, 5, 6 in NBX domain.	• No Single point of failure. • Failure detection and fail over takes place mainly at level 3 using Routing protocols. • Some use of Level 2 Failure detection and fail over return mechanisms. • POCA Server recovery. This covers failure of the platform, and associated POCA services. Note that a POCA Service can be deemed to have failed if onward connections to other POCA components have failed.
1,2 and 3	**NBX Domain** NBX Routers to NBX	• Failure detection and service return takes place mainly at level 3 using Routing protocols. • NBX comprises two systems NBXa and NBXb Each such system consist of two computer platforms (one at Wigan and one at Bootle) in an Active / Standby arrangement. In the event of the loss of one such computer platform the other can take over within minutes.
4	All Components	• Most classes of component failure are 'almost transparent' at the TCP level. However, it is important to note that because TCP treats IP datagram loss as congestion, then the TCP connections are likely to shrink their Transmit / Receive Windows. A robust TCP stack is required which will correctly expand its window, especially if the number of TCP connections is low resulting in each connection having to do more work.
5 and above	Application Connection retries.	• When a network outage occurs, whether planned or unplanned the NBX will automatically detect this (usually as a result of an error code following a send or receive) and go into a "Retry" state. This means at a specified interval an attempt is made to re-establish the session. The interval will be no more frequent than 10 seconds. • The AIS [Ref. 1] describes an application level echo test. If a timeout of this heartbeat is detected then the application software can close the connection (if appropriate) in order to reset the current session.

5.5 Performance

This section states the Performance targets for components concerned with the Interface.

FUJ00001902

Formatted: Font: 8 pt

5.5.1 POCA and NBX Platforms

The NBX Platform will be configured with 8 PIs and two threads per PI. The Card Account EBT Platform will also be configured with 8 PIs and two threads per PI and this results in 16 ports, with 4 Ethernet cards carrying this traffic.

The performance requirements are drawn from figures supplied by POL on the expected hourly transaction rates over the working week for each year of service. The expected number of transactions for the peak hour is 488,159.

The working assumption is that the system be sized for an instantaneous peak of +25% of the peak hourly average volume of transactions i.e. 168 tps. For the purposes of the contractual performance guarantee a higher figure, 180 tps, is used and the further assumption is made that each of these will result in one transaction passing over the NBX- CAPO Interface and back again. Moreover, it is required that this transaction rate can be sustained with the loss of 1 IP address (ethernet card) and therefore 4 ports on EBT. This gives a design point of 15 counter transactions per second per EBT thread (180 tps divided by 12 remaining ports).

Note, however, that NBX is delivered from two separate 'instances' each configured with 4 PIs and 8 threads. And that the configuration shown in section (Figure 3 – Application Endpoints) ensures that the loss of an EBT IP address results in the loss of only 2 threads per NBX instance. Therefore, assuming round robin thread usage, EBT can sustain 6 x 15 = 90 tps from each NBX in a failure scenario. Without any failures 120 tps per NBX can be sustained.

5.5.2 Wide Area Network

The required capacity of the links from the Live NBX locations to the POCA locations (2M bits /sec), has been determined as follows. Sizing for wide area networks for this kind of application traditionally employs a peak-to-average ratio of 2:1 on the volume of traffic. The average message sizes for the up and down flow rates as defined above are combined and the resulting peak link traffic indicates a requirement for 2M bits/sec lines.. The design calls for duplicated links and this provides a cost optimum approach to providing sufficient capacity even in the event of failure of a single link.

FUJ00001902

Formatted: Font: 8 pt

6 Security

This section provides a very brief overview of the security aspects of this Interface. It applies to Live, DR and Test environments.

This is a financial application. IP addresses and ports will not be published to the public. Knowledge of Security Key components is restricted to nominated key component holders.

6.1 End-to-End Identification

Messages will be sent to or received from known IP addresses. A message from an unrecognised address should be rejected. Working keys exchanged daily under the AZMK provide positive authentication of the other party.

6.2 Encryption and Decryption Methods

This section concerns NBX encryption only.

The Triple DES encryption process follows the ANSI standard X9.52 (1998).

When data is Triple DES encrypted, the first half of the encrypting key will be used to encrypt, the second half to decrypt, and the first half to re-encrypt. This is the Encrypt-Decrypt-Encrypt (EDE2) method. To decrypt data the process is inverted; Decrypt-Encrypt-Decrypt.

Please refer to AIS [Ref. 1] for details of encryption / decryption applied to the contents of messages. PIN block fields are encrypted. Other fields are not encrypted.

It has been agreed that a Triple DES MAC will not be used to protect each message.

6.2.1 Network data privacy and authentication

The protection described here is in addition to application-level authentication and encryption, which is described elsewhere.

Encryption (IPSEC tunnel mode, Triple DES) applied within the routers provided by POCA assure privacy of data in transit across the virtual private network.

6.3 Application Key Management

Procedures for distribution and management of Master Keys are documented in OLA [Ref 3]. Working keys are used to provide integrity of transmitted data and to encrypt certain fields within the application messages.

The Acquirer Working Keys used for PIN block encryption are transmitted under the protection of a shared key encryption key the Acquirer Zone Master Key, AZMK. The AZMK is exchanged at an agreed interval. This period is normally between six and twelve months. The Acquirer Working Keys, AWKs, for PIN block encryption translation, are changed daily and exchanged under the protection of the AZMK.

The AZMK is exchanged in component form. Three components will be securely printed by POCA and sent to nominated key holders in NBX. These AZMK components are entered separately and securely into the NBX and verified.

FUJ00001902

Formatted: Font: 8 pt

6.4 Protection

Defensive coding practices are employed to check for parameters that are out of specified range, fields or records that exceed expected lengths, and unexpected message sequences.

Operating System builds follow secure build practices.

6.5 PIN Encryption

The security requirements with respect to PIN concealment and message confidentiality between NBX and POCA follow Banking industry standards. PINS are translated in hardware and are encrypted at all times, and must not be stored in network nodes. Dynamic key management is adopted, with keys being exchanged and verified at least once every 24 hours.

6.6 PIN Block Format

The PIN information is held in a 16-digit HEX string PIN block.

RACAL/ZAXUS Format 01 is used. This is the format adopted by the American National Standards Institute (ANSI X9.8) and is one also known by the International Standards Organisation (ISO 95641 – format 0).

This format combines the customer PIN and account number as follows:

- A 16-digit block is made from the digit 0, the length of the PIN, the PIN and a pad character (hexadecimal F).
- Another 16-digit block is made from four zeroes and the 12 right most digits of the account number, excluding the check digit.

The 2 blocks are then exclusive-OR added giving the final PIN block, which is then encrypted.

6.7 Key Changes

Acquirer Zone Master Key (AZMK) changes take place every 6 months.

The same AZMK is used for all PIs. NBX will transmit Triple DES Acquirer Working Keys (AWK) to POCA systems encrypted under the AZMK using an 0800 message.

All encryption keys used between NBX and POCA systems are double length keys, 32 HEX Characters. The PIN block is encrypted using Triple DES encrypt-decrypt-encrypt (EDE2) techniques.

NBX may initiate a new AWK, key change at their discretion.

POCA will not initiate a key change in the event of a bad de-block but will rely on the problem being detected in the NBX.

Please refer to AIS [Ref. 1] for more information) on application key changes.

6.7.1.1 Acquirer Working Keys (AWK)

These keys apply at the POCA process level, i.e. there will a unique Acquirer Working Key (AWK) for each of the PI's.

FUJ00001902

Formatted: Font: 8 pt

6.8 Key Ownership

POCA own the AZMK to be used between NBX and POCA.

POCA generates and distributes the 3 AZMK components to NBX in a secure manner.

The 3 components are combined and securely stored in the NBX . No person should ever be allowed to see all 3 clear components of the AZMK.

6.9 Line Encryption

POCA provides Encryption (IPSEC tunnels) to protect the data being transported over the circuits in place between NBX and POCA.

Cisco router encryption (IPSEC) is used.

All management and monitoring of the routers containing line encryption is the responsibility of POCA.

6.10 Firewalls

POCA has installed a firewall security system in front of each of the Ethernet ports on the POCA systems.

NBX systems are also protected by the use of firewalls and dedicated ports are provided for use of this interface.

6.11 Network Infrastructure

All network infrastructure from the dedicated NBX firewall ports towards the POCA domain is solely used in provision of the POCA service and this shall be managed through these same ports.

6.12 POCA Authorised Engineering access to NBX locations

In the event of a POCA equipment failure at one of the NBX locations, POCA will arrange for an authorised engineer to attend the NBX site to diagnose and repair or replace the equipment.

NBX will provide POCA with procedures to follow when access is required for POCA authorised engineers to NBX locations.

FUJ00001902

Formatted: Font: 8 pt

7 Recovery Facilities and Procedures

7.1 Fault Detection

One Live network management centre will manage the network with a DR facility available.

7.2 Disaster Recovery Environment

NBX does not provide a DR capability, since both Data Centres are active.

POCA will create a DR capability at their contingency location, a replica of the production environment.

In the event of total failure of the primary POCA systems, DR will be invoked and production service restored to NBX.

7.3 Disaster Recovery Testing

The POCA contingency systems will be tested (details are provided in the POCA DR Test Plan). Should the entire processing environment be transferred from the production environment to the contingency environment for testing purposes, notice must be provided to NBX at least thirty days in advance.

7.4 Disaster Recovery Invocation

The decision to invoke the move to the contingency system from production by POCA may be taken by persons in the positions listed in the POCA DR Plan, to be produced as a separate document under a different contract schedule.

This decision will be taken following an incident of sufficient severity to justify the invocation.

The decision may also be taken as a safeguard measure to reduce the impact of an impending systems or environmental failure.

The steps to be taken and the approximate timings will be contained within the DR Plans to be produced by POL, Fujitsu and EDS.

7.5 POCA Move to DR Processing

The move by POCA between Live and DR will not require NBX to change their systems in any way.

Under normal operational conditions there will be no connections made between the NBX Servers and the POCA DR site. In the event of a DR scenario then all connections will be between the NBX Servers and the POCA DR site.

If POCA invokes DR the NBX Operations department must be contacted by POCA Operations and informed of the switch to DR processing.

7.6 NBX Move to DR processing

NBX does not move to DR processing.

FUJ00001902

Formatted: Font: 8 pt

Appendix A – Detailed Configuration Information

Production / DR System Sockets

The following tables define the TCP/IP sockets used between NBX production system and POCA production system for message exchange. If DR is invoked at POCA the socket definitions remain unchanged. Note that all IP addresses documented in this section are in the Peering Address domain.

All published NBX IP addresses as defined below, including the Network Management IP addresses will be allowed to ICMP Ping all POCA Published IP addresses and vice versa.

Note that the PI labelling is shown in Figure 3 – Application Endpoints.

NBX			POCA			
System	**IP**	**Port**	**PI**	**IP**	**Port**	**Thread**
NBXa	IRRELEVANT					
NBXa						
NBXb						
NBXb						
NBXa						
NBXa						
NBXb						
NBXb						
NBXa						
NBXa						
NBXb						
NBXb						
NBXa						
NBXa						
NBXb						
NBXb						

FUJ00001902

Formatted: Font: 8 pt

NBX		
Name	**IP**	**Ports**
NBXa Bootle	IRRELEVANT	
NBXb Bootle		
NBXa Wigan		
NBXb Wigan		
Network Management Server Wigan		
Network Management Server Bootle		

FUJ00001902

Formatted: Font: 8 pt

Inter Router LAN'S	
IP Subnet	Name
IRRELEVANT	Bootle LAN0
	Bootle LAN1
	Bootle LAN2
	Bootle LAN3
	Wigan LAN0
	Wigan LAN1
	Wigan LAN2
	Wigan LAN3

The following table defines the TCP/IP socket used between NBX production system and POCA production system for file transfer using CONNECT: Direct. If DR is invoked on the POCA side the socket definitions remain unchanged.

File Transfer	NBX IP& Port	POCA IP & Port
NBX ➔ POCA	Wigan: Bootle:	IRRELEVANT

FUJ00001902

Formatted: Font: 8 pt

Test System Sockets

The following table defines the TCP/IP sockets used between NBX test system and POCA test system for message exchange. The intention is that sockets 6001/6002 are reserved for use by simulators (typically single-threaded), 6004/6005 are used for multi-thread testing and augmented by additional sockets chosen from the list below as required by the prevailing tests. All ports are defined at the NBX end but remain dormant unless they are used. The usual change control procedures apply to requesting activation of additional ports.

All published NBX IP addresses as defined below, including the Network Management IP addresses will be allowed to ICMP Ping all POCA Published IP addresses and vice versa.

NBXTest			POCA Test			
System	**IP**	**Port**	**PI**	**IP**	**Port**	**Thread**
NBXTest	IRRELEVANT					
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						
NBXTest						

NBX Test		
Name	**IP**	**Ports**
NBXTestx Feltham	IRRELEVANT	

FUJ00001902

Formatted: Font: 8 pt

NBXTesty Feltham	IRRELEVANT

The following table defines the TCP/IP socket used between NBX test system and POCA test system for file transfer using CONNECT: Direct.

File Transfer	NBX IP& Port	POCA IP & Port
NBX ➔ POCA	IRRELEVANT	

Inter Router LAN'S	
IP Subnet	Name
IRRELEVANT	Feltham LAN

FUJ00001902

Formatted: Font: 8 pt

Appendix B – Testing

The following diagram illustrates the Testing Environment. The Test IP address assignments are documented in Appendix A – Detailed Configuration Information.

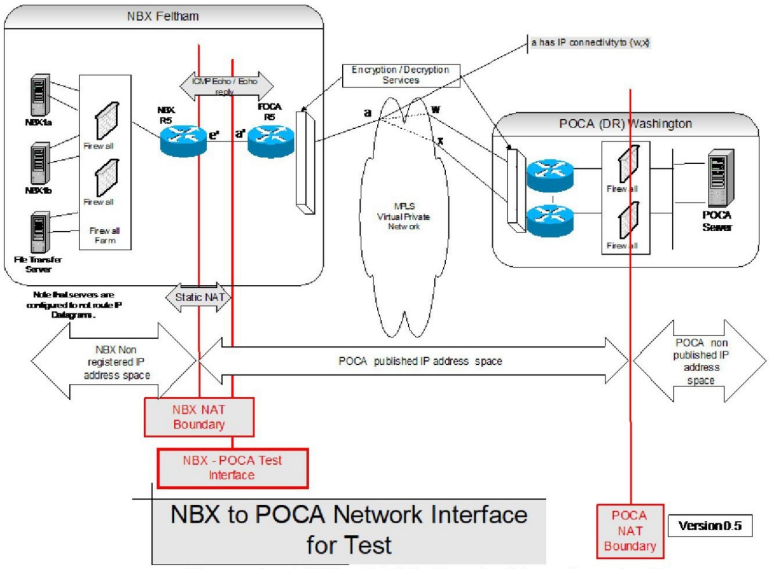


Figure 4 – NBX – POCA Physical Interface for Test

Table 6 Interface Characteristics, with suitable scaling for one Router each side of the interface, applies to the Test Interface as well.

End of Document