POL00043744

Document Title:

Network Banking-Work Package 2 Report

Document Type: Report

Release: N/A

Abstract: This document reviews the work performed on Work Package 2 by ICL and others as part of the Network Banking Work Packages. It supplements the information provided in NB/PRP/001-Network Banking Work Package Review

Document Status: DRAFT

Originator & Dept: Martin Riddell

Contributors:
Tony Hayward
Simon Fawkes
Glenn Stephens
Peter Wiles
Richard Brunskill
James Stinchcombe
Allan Hodgkinson
Geoffrey Vane

Reviewed By:
Mike Stares
Tony Oppenheim
Mike Coombs
Peter Jeram
Liam Foley
Stephen Muchow

Comments By:

Comments To:

Distribution:
ICL Pathway Library,
Reviewers
Approvers

POL00043744

0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
0.1	29/1/01	Initial draft. Based upon NB/PRP/001. Incorporating revisions from authors	

0.2 Approval Authorities

Name	Position	Signature	Date
Mike Stares	Managing Director		
Liam Foley	New Business Director		

0.3 Associated Documents

No.	Reference	Ver.	Date	Title	Source
1.	CS/Rep/032	0.1	10/1/01	Network Banking WP2-HelpDesk options and requirements	ICL Pathway
2.					
3.					
4.					
5.					
6.					

0.4 Abbreviations/Definitions

Abbreviation	Definition

0.5 Changes in this Version

Version	Changes
0.1	Initial draft

0.6 Changes Expected

Changes

POL00043744

Review comments from issue 0.1

POL00043744

0.7 Contents

POL00043744

POL00043744

POL00043744

POL00043744

1 Introduction

1.1 Background

This document was commissioned by the Post Office to assist in the development of a Network Banking Business Requirements document.

NB/PRP/001 was produced to document the interim outputs of this work by ICL Pathway.

This document supplements the information provided in the above document.

1.2 Purpose and Scope of this Document

This paper documents the results of the investigations by ICL Pathway in each of the subject areas within Work Package 2, based upon initial requirement to date.

For each area it documents options, issues, areas requiring further investigations and, where appropriate, initial recommendations.

It will provide Post Office Boards with the necessary information to initiate and scope the NWB Programme.

POL00043744

2 Business Requirements and Technical Architecture

2.1 Service Boundaries

The following diagram illustrates the end-to-end architecture separated into the different domains of operational responsibility.

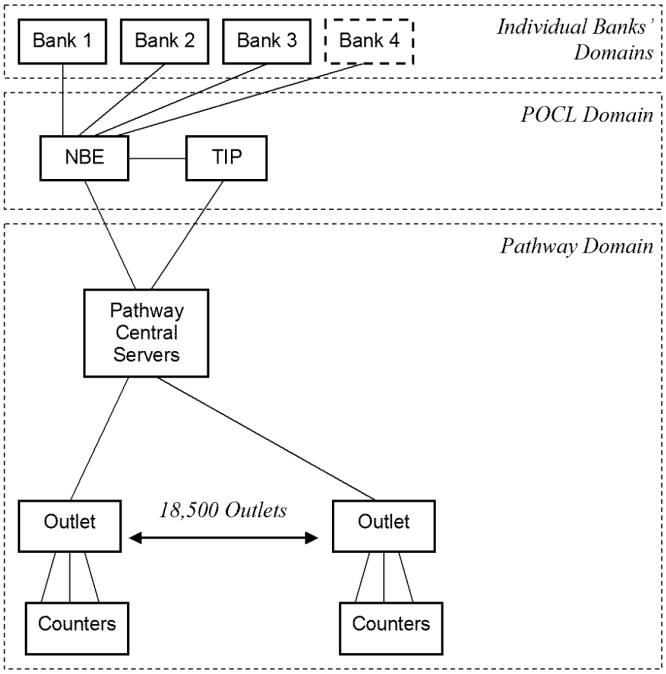


Figure 1 - Outline End to End Architecture

The system is intended to carry out the following card-based transactions:

- On-line cash deposit
- On-line cash withdrawal
- Balance enquiry

Later enhancements may include:

- Cheque encashment (this is already supported but not fully automated)
- Ordering a statement
- Printing a mini-statement
- Changing a PIN code
- Opening and closing an Account
- Setting up standing orders and direct debits

2.2 Web / XML Technology

2.2.1 Network Banking Context Diagram

The following diagram shows the context of Horizon Network Banking and its relationship to four external entities: the banks, the Network Banking Engine, the Post

POL00043744

Office and the retail customer. It is derived by interpretation from [ITT].

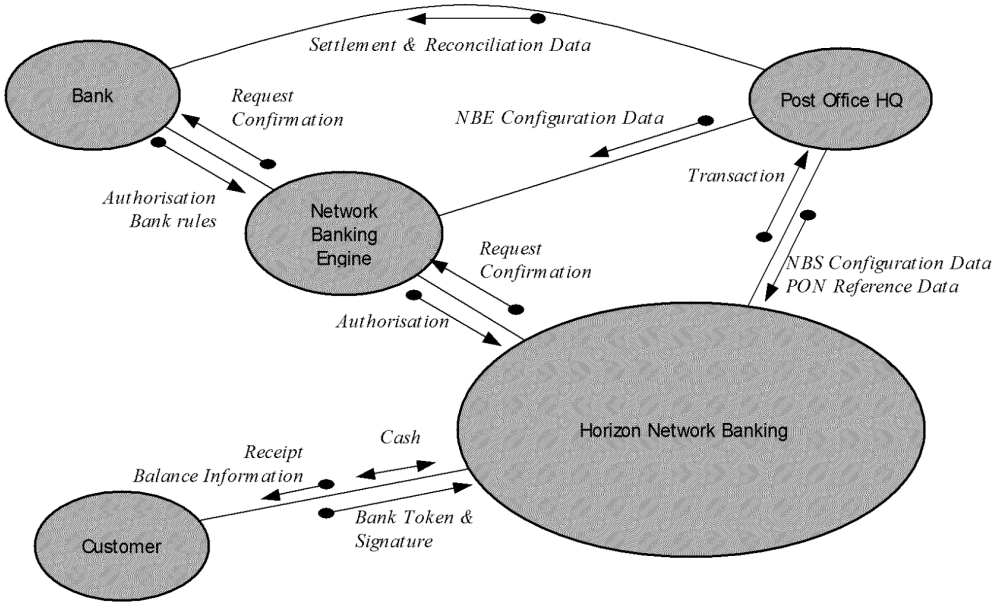


Figure 1 – Network Banking Context Diagram

2.2.1.1 External entities

The following entities are defined in the above diagram.

- *Bank* represents all the banks that are served by the Network Banking Engine
- The *Network Banking Engine* is to be supplied by IBM. The data flows that it supports are the subject of a separate Work Package, but are likely to be similar to those shown. It supports the interface between the Network Banking solution and all the banks that are served by the solution. It is the only interface to the Banks. It normalises all the different Banks' interfaces so that they appear the same throughout the rest of the solution.
- *Post Office HQ* represents the operational part of the Post Office organisation
- *Customer* represents the retail customer who is served by a Counter Clerk in a Post Office Outlet

2.2.1.2 Data Flows

This following logical data flows are shown in the above diagram. They are described in alphabetical order.

- *Authorisation* - the response from a bank to a Request. It will authorise or decline the transaction. It will include the Account ID, the Pathway Transaction Identifier, optionally an amount of money and a signal that authorises or refuses the transaction. It may also include some form of authorisation code provided by the bank.
- *Bank Rules* - data passed from the banks that defines various aspects of particular Bank Account Types that vary on a more frequent basis than the configuration data.

  There are no known requirements for this data at this time, but it is included for compatibility with the *Automated Payment System* (APS), which has a similar feed

POL00043744

for tariff data. It is important to separate this potential feed from the *NBS Configuration Data* to avoid that data being 'polluted' with inappropriate information in the future.

Any adoption of this feed requires agreement with the design of the NBS Client.

- *Bank Token & Signature* identifies the bank account against which the customer wishes the transaction to operate. The Bank Token includes the Bank ID and the Account ID. The "signature" is the means of authentication of the card, and is presented to the Counter Clerk. If necessary, the Counter Clerk may request additional proof of identity. No data is passed to the bank to represent the signature, though there may be an indication of the authentication method accepted by the Counter Clerk.
- *Cash* - money paid to the customer or being paid in by the customer
- *Confirmation* - the record of the actual transaction that occurs at the Outlet. It allows the bank and the Post Office to post the transaction within their central systems. It includes the Account ID, the amount and the transaction type (Deposit or Withdrawal). To avoid reconciliation problems it is important that the Transactions that flow to the banks and to the Post Office HQ use exactly the same demarcation. This will be reviewed following the outcome of the Work Package 1 and Work Package 5 work on Settlement and Reconciliation.

- *NBS Configuration Data* – data that configures the Network Banking Client Application to support particular banks and particular account types. It includes the rules or constraints that apply to the account types operated by each bank. Examples are: minimum and maximum deposit; floor limit for fallback working, etc.
- *NBE Configuration Data* - configuration information passed by the Post Office to the NBE. It has equivalent content to the NBS Configuration Data passed to Pathway
- *PON Reference Data* – as required by the existing Horizon applications. Of particular interest here is the additional products that represent the banking transactions to be accounted for. It includes product specification data and Cash Account mapping data
- *Receipt* – a printed slip of paper that records the transaction requested by the customer
- *Request* to a bank. The transaction may be one of: cash withdrawal, cash deposit or balance enquiry. The request will include the Account ID, the type of Request, the Horizon Transaction Identifier and, optionally, an amount of money
- *Settlement and Reconciliation Data* - represents the information flowing from the Post Office to each Bank to confirm the value of transactions executed within a given time period (probably a day). This has two purposes: to confirm that the Bank has received all the transactions and to trigger the transfer of funds between the two organisations. Note that there is some reconciliation data flowing between Pathway and TIP. There is limited reconciliation flow between Pathway and the NBE, and none between Pathway and the banks.

POL00043744

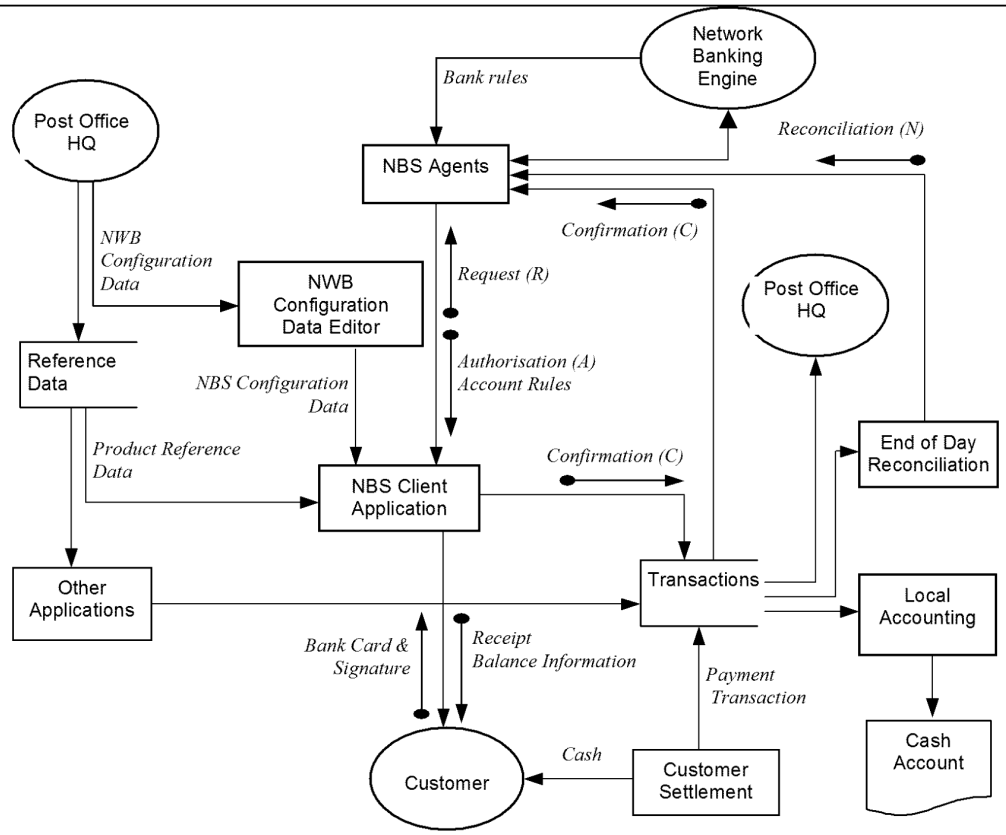


Figure 2 – Network Banking Data Flow Diagram

2.2.1.3 PON's Interest in Web Technology

PON believe that they need to be more responsive in terms of the applications and services provided within the Post Office Outlets, and that the appropriate way to do this is by use of Internet technology.

Current PON business initiatives (including NBS and, potentially, ERA) have highlighted the need for ICL Pathway to consider how to include new technologies in its service delivery capabilities to the Post Office.

PONB wish to make web-based technology applications available at the Horizon Counter by incorporating a web browser within the Counter architecture. They see this as enabling them to provide access to a wide range of existing and new applications, including the NBE host as described above, and web services provided by other Government Departments under the *Government General Practitioner* (GGP) initiative.

The challenge is to make the Horizon technical architecture more responsive to these needs, while protecting those aspects of the Counter stability, usability, performance and security that are required by any modified *Codified Agreement*.

Particular aspects that are determined by the present Codified Agreement include the following.

- *Usability* – the *Human-Computer Interface* (HCI) presented to the Counter Clerk has been developed to provide a highly usable, simple to learn and highly intuitive HCI that minimises the time taken by any customer at the Counter. Its features are

POL00043744

described in the Horizon Style Guide, [STYLE]. This standard needs to be maintained in the delivery of new applications regardless of the mechanisms by which they are implemented.

- *Performance* – the Codified Agreement lays down *Service Level Agreements* (SLAs) for a number of operational aspects of the Horizon system, including the time taken to carry out some designated tasks at the Counter, and deadlines by which information is available at the Counter or PON (depending on the direction of the data flow). While these SLAs stand, new applications cannot be permitted to disrupt ICL Pathway's ability to meet them.
- *Stability* – during Acceptance of the Horizon system, ICL Pathway accepted standards for the number of times that Counter Clerks are permitted to reboot the Counter PC, or on which it may "crash". To stay within these constraints, there is a need for ICL Pathway to prevalidate any software that is to be loaded onto the Horizon estate.
- *Security* – A number of security standards are laid down by the Codified Agreement, including the need for facilities to deter fraud and to prevent "hacking". The potential for fraud may have lessened with the removal of BES. However, the introduction of NBS will increase the scope for fraud, in particular if unauthorised users are able to obtain details of customers' bankcards. In addition, it is possible that the banks will insist on a range of security measures that are not currently employed by Horizon.

2.2.1.4 Escher's Strategic Directions and their Impacts

The technical direction of Escher Group, is highly significant. Their main technical strategies cover the following areas.

- A browser based desktop. Escher have developed a web based desktop framework (WebRiposte)
- XML data encoding for Riposte Message Server.
- Improved integration of the current messaging service with web services (page serving, HTTP tunnelling, etc)

PON has made a strategic decision that elements of Escher's WebRiposte technology will be used to support the Network Banking application. Some of the implications of that decision are discussed in this document.

2.2.1.4.1 WebRiposte

WebRiposte is a new product from Escher that "web enables" the Riposte Message Store. It includes FTP and HTTP servers. Its most significant difference from the Message Server used in M1 is that APIs are provided to store and read messages in XML as well as in the current Riposte Attribute Grammar format.

It introduces the concept of a "WebRiposte Object", which is similar to that of a traditional Persistent Object. It also supports remote lookups to obtain URLs from a Correspondence Server, if they cannot be satisfied within the Counter. However it can be configured to prevent it connecting to the remote Correspondence Server, and it will be necessary to enforce this constraint within Horizon.

2.2.1.4.2 WebRiposte Framework

POL00043744

This new product provides a run-time environment for Web based applications to use WebRiposte. It is focused primarily on Banking type applications. As well as Network Banking, Escher quote currency exchange.

2.2.1.4.3 WebRiposte Browser

The WebRiposte browser intercepts URL references and satisfies them by the content of WebRiposte Objects held within the Riposte Message Store. As indicated above, it would be necessary to ensure that this was restricted to the local (Counter) message store, thus ensuring that all executables and presentation objects must be predistributed to the Counters.

The web dialogue is generated by the client application, and uses an XML data stream. This is transmitted by Riposte over the communications link to the Campus. The connection to the NBE is made from the Horizon Agent layer. The task of the Agent software is to support the interface to the NBE, though it is likely that it will need to do some additional work as well.

2.2.1.4.4 WebRiposte Horizon Desktop

The current Horizon HCI is designed to be intuitive and easy to use by the Counter clerk. It uses a common touch-screen structure that is specifically tailored for use in a Retail environment. The intention is that unless absolutely necessary, the Counter Clerk should not have to type in any data on the Counter. Many transactions are initiated automatically by the Counter Clerk swiping a magnetic card or reading a bar code. (There is always a "fallback" facility for the Counter Clerk to enter these details manually if, for example, the bar card reader is out of action.)

Note that there is no mouse.

There is an explicit requirement in the Codified Agreement that any new application (such as Network Banking) should support this HCI, and link into the customer session, in a seamless manner.

The user interface makes use of "custom controls" provided as part of the Riposte Desktop system. These constrain the designer to work within a particular style, an example of which is shown here.

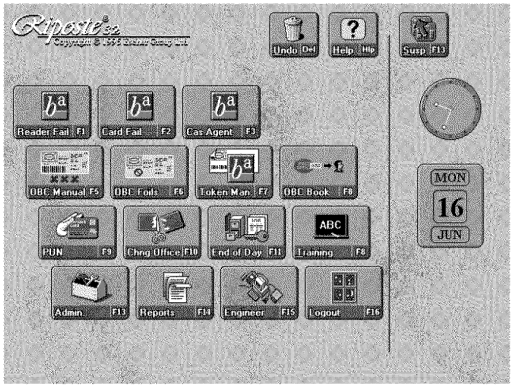


Figure 3 - Example of the Riposte Desktop

This style splits the screen into two parts. The left hand portion contains a number of menu Buttons that are valid in the context of the transaction (though some may be marked with a "stop sign" which indicates that they cannot be used in this particular transaction.) The right hand side of the screen is a "stack" showing, for example, the

POL00043744

purchases made by the customer so far. Various controls are used to support features of the interface, as shown here.

An application needs explicit knowledge of these controls, and of the Riposte APIs that underpin other aspects of the application's functionality. These APIs (or other controls; it is not yet clear) are defined by the WebRiposte Application Framework, and will need to be documented in [GENAPI] to conform to the requirements of the Codified Agreement.

A web-based server application such as the NBE could, in theory, specify the presentation style of the application using display objects that are passed to the Horizon Counter, for example using an agreed XML Style Sheet. However, to meet the requirement to retain the existing Horizon Counter HCI, Escher are developing Java based equivalents to the principal Riposte desktop controls, and have demonstrated some of these in the *Network Banking Browser - Proof of Concept* study carried out in mid-2000; see [PoC]. One impact of this is that there will be very strict constraints on what XML is considered valid, and in particular, all control over presentation will be removed from the XML data stream.

2.2.1.4.5 Reconciliation and Balancing

NBS transactions will have an impact on the amount of cash and number of cheques in the Counter Clerk's cash drawer, and hence on his Stock Unit balance. It is a fundamental requirement that Network Banking transactions are integrated within the standard customer session through the Riposte transaction stack. Further, all banking transactions need to be reported via the Horizon TPS process to PON's TIP systems in Chesterfield.

[ITT] further requires a three-way reconciliation between the NBE, TPS and Counter data flows.

The NBS Counter Application will use the WebRiposte Framework, which provides abstracted features to carry out specific tasks including capturing the values of particular types of variable from the Clerk, or writing particular message types to the Riposte Message Store.

Applications may use these APIs to read messages, and to generate messages for replication and transmission to a remote Host and to TIP. In addition, by generating messages that conform to the EPOSS data model, they can feed information into the Cash Accounting processes. The EPOSS data model is included in [GENAPI]. This data model requires that a valid Stock Unit ID is included within each transaction. The Stock Unit ID is available from an in-process API, and hence can be accessed by the Escher web browser. Again, this means that the web application would need to be tailored for use with the Horizon channel. In practice, Escher intend to provide an Application framework, tailored for use by Financial applications such as Network Banking, that understands and handles the interface to (for example) the EPOSS Transaction Data, and thus hides knowledge of this from the application itself.

By design, an application running outside the context of the desktop cannot place transactions on the transaction stack, as this stack is maintained in memory within the Desktop process. The Riposte APIs that manipulate the transaction stack are designed to be invoked in-process, i.e. within the desktop context.

Cash Account balancing takes place on the Counter. It scans through the messages in the message store and sorts them using information supplied via Reference Data. Thus, any introduction of a new banking application would need to be accompanied by new Reference Data that identified the Cash Account implications.

2.2.1.4.6 Communications Protocols to NBE

POL00043744

The protocol that passes between Pathway and the NBE is expected to be XML based, but for the reasons outlined above, the server application may need to develop its client component (or assumptions) specifically for the Horizon channel.

ICL Pathway expected that this XML data stream would be carried over HTTP. This is in line with the [ITT] expectation that the NBE would drive a number of other, web based channels, in addition to the Horizon network. However, it is noted that IBM's proposal for the NBE suggests the use of MQSeries messaging for this purpose and so further discussion in this area is necessary

2.1.1.1.7 Impact on Existing Infrastructure

The use of WebRiposte will require the Counter software set to be upgraded from Internet Explorer V4.01 to V5. Early versions of the WebRiposte documentation also indicate that the Counter infrastructure will need to be upgraded to NT Service Pack 5 or later. This will have a knock-on effect on the versions of other third party products running within Horizon.

If the Horizon infrastructure needs to be updated to Riposte Desktop Version 226, then there would also be a need to update the application run-time library environment from VB5 and C++5 (as at present) to Version 6 of both of these toolkits. This could require all Counter code to be recompiled with the later Run Time Libraries, and redistributed to all Counters, though this is not yet clear.

POL00043744

3 Co-Location

3.1 Summary

This section looks at the operational implications of the introduction of the Network Banking Service into the current managed environment.

The 2 principal options with regard to the placement of the NBE and associated infrastructure are whether to place them within Pathway's Data Centres or outside. It is ICL Pathways recommendation that the NBE infrastructure is placed within the Data Centres and within the managed service umbrella. This would take advantage of the current operational and management framework and simplify end-to-end boundary management.

In order to support the Network banking Service there will be an increase in the amount and type of network and data centre infrastructure. Although network planning work has yet to be completed, the current planning intention is that the existing network infrastructure will be retained for the existing pilot activities with a network upgrade at some future point . The upgrade and strategy will be completed following completion of the capacity planning and network design work activities.

One possible result of this exercise will be the possibility that there may be an extension to the current data centre estate required. This may result in a third data centre.

3.2 Managed Service Environment

3.2.1 General

The managed service environment comprises sophisticated and robust services and infrastructure which provide 24 hour management and support of the current Horizon Service. It includes schedule monitoring, hardware and application event monitoring, network management, integrated help-desk, change management, software distribution, security management and business continuity processes,

These have been developed to meet POCL's stringent contractual requirements and it is Pathways view that it would be beneficial to take advantage of this existing framework.

The addition of the NBE within the campus would be integrated into this framework to ensure complete monitoring of the end-to end service. Specific areas for which further work will be required are listed in this section.

3.2.2 Systems Operate Service

The Systems Operate Service is principally operated from Belfast with an on-site team within the Data Centres for on-site Network Management and peripheral Operations. All operations relating to monitoring of the operational schedule and management of alerts is carried out in Belfast in conformance to Security Access Policy.

The operation of the NBE would form an integral part of the Horizon system operation, and hence should be integrated into the Horizon operational environment. The Horizon platforms are managed and operated from geographically seperate but functionally integrated support centres.. It is relatively easy to provide management facilities for the IBM environment from a similar support centre specialising in management and support of IBM systems. This would be integrated into the overall operational environment.

It also enables consistent management by the Horizon Maestro scheduling infrastructure, including management of failover. Maestro, as an IBM product, supports scheduling of

POL00043744

processes on a number of platforms including Sequent/Dynix, Windows NT and OS/3**90** ICL Pathway has developed sophisticated Maestro schedules that manage, monitor and control the processing of work on a wide variety of Sequent and NT platforms. The operation of the NBE will be intimately bound into the scheduling of these processes, for example in terms of end of day processing, reconciliation report generation and others, and hence it makes substantial sense to integrate the NBE into the Horizon scheduling environment

It will be necessary to produce a Service Description in this area defining all aspects of the operational service including interface management, archiving and recovery strategy etc.

3.2.3 Systems Management Centre

Based in Stevenage , with an alternate site in Manchester, this unit is responsible for event monitoring of the equipment within the data centre, software distribution and second-line support activities. It provides for consistent Event Management by the Horizon Systems management processes. The Horizon Event Management processes provide an unrivalled tool set to ICL Pathway's support staff, and already include sophisticated mechanisms to filter out unwanted events, amalgamate "event storms" into summary information, and make the impact of major Events clear so that remedial action can be taken. Because the NBE will comprise an integral part of the infrastructure needed to support Counter operations, it is sensible to include its Events within the same management facilities.

The development work involved in event management is covered in more detail in Section 8 of this report.

3.2.4 Horizon Systems Help Desk(HSH)

Based in Stevenage, Manchester and Wakefield this desk provides 2 main functions. It operates as the initial point of contact for the outlets for any system problem or advice and guidance. It also operates as the central call management service for all incident relating to the Data Centre infrastructure and operational schedule and as such is used by Pathway, Pathway suppliers such as Energis and also POCL Data Centres. This provides a single view of all incidents within the current end-to-end solution.

The current scope of this service will be expanded to include Network Banking Service. More detail of this is provided in CR/SPE/032 'Network Banking Help-desk Options and Requirements'

3.2.5 System Support Centre

This is the ICL Pathway unit responsible for software support. With the implementation of Network Banking Service it would be responsible for defining the support responsibilities and routes, in conjunction with HSH and relevant suppliers.

3.2.6 Business Support Unit

Based in Bracknell, this is the support unit responsible for managing and resolving any reconciliation-related incidents. They would work with POCL in defining any procedures necessary on this area.

3.2.7 Business Continuity

There are processes agreed between POCL and ICL Pathway for the management of Business Continuity incidents eg site failover. This includes definition and timing of Business Continuity testing, post-incident reviews etc. Work will be required to integrate NBS into this framework.

3.2.8 Reference Data Operation

POL00043744

Validation and release of reference data is managed by the Reference Data Team(RDT) in Bracknell. Working closely with POCL's RDT and OSG it is responsible for management of the validation and release of reference data into the live estate. Work will be required on any revisions to working processes resulting from the integration of NBS.

3.3 Technical Benefits of Co-location

3.3.1 Minimised NBE Response Times

The on-line response time to the Agent servers will be minimised. By connecting the NBE to the same Campus LAN as the Agent Servers, we can avoid the need to traverse Routers, Firewalls, encryption devices or any intervening E3 or ATM links, with the additional response time latency that these would give

3.3.2 Reuse of Horizon FTMS Services

The Campuses already provide established means (the *File Transfer Management Service,* FTMS) for transmitting batch files from RDS and to TIP, and these can be utilised by the NBE

3.3.3 Simplified Data Feeds for Reconciliation and Settlement

End-to-end reconciliation will be carried out within the Campuses, and again co-location of the NBE with the Campuses will simplify the task of making NBE reconciliation data available.

.

3.3.4 Enables Re-use of Horizon Audit Solution

It enables audit information generated by the NBE to be included in the Horizon audit trails. ICL Pathway has a contractual requirement to generate and secure Audit information at a number of points within the Horizon infrastructure, particularly in cases where data crosses organisation or contractual boundaries. These include Riposte data passing to and from the Counters (i.e. between the TMS and OPS) as well as data files passed to and from the Horizon Client estate. Facilities are provided to enable reasonable access to past audit information, for example for investigations. It is a relatively simple matter to integrate the NBE's audit data into these mechanisms so that it is both collected by and retrieved by the same processes.

3.3.5 Re-use of Data Warehouse Facilities for SLA Monitoring

It provides for consistent input of SLA-related data to the Horizon Data Warehouse, and hence simplifies the calculation of SLA conformance figures for both the ICL Pathway and NBE domains. [ITT] indicates that POCL will seek to agree SLAs with both ICL Pathway and the NBE supplier for the response times and availability of NBS transactions. In the Data Warehouse, ICL Pathway already has a sophisticated mechanism to collect the data needed to calculate the adherence to such SLAs, and these are used on a regular basis to generate reports for POCL. It is sensible to extend these facilities to include both SLA calculations for ICL Pathway, and to calculate the

POL00043744

impact on these of SLAs that depend on the responsiveness of either the NBE or the banks. This is considerably simplified if the NBE is collocated with the Data Warehouse.

3.3.6 Minimised Communications Costs

It avoids the need for expensive communications links between the Campuses and a separate NBE location. ICL Pathway estimates that any such links would need a capacity of at least 34 Mbps, and these have a significant installation and running cost.

If the NBE is *not* co-located with the Horizon Campuses, then at a minimum it will be necessary to install and support the communications links between the two (pairs of) sites. it can be assumed that an ATM service is required, as the NBE sites are unlikely to be close enough to be accessed by Fast Ethernet.

3.3.7 Simplified Release Migration

By co-locating it with the Campuses, the NBE can be included in and co-ordinated with the overall planning and migration activities for future Horizon releases.

3.4 Third Data Centre

The current Data Centre Infrastructure is contained within the Bootle and Wigan Campuses. It is likely there will a requirement for an increase in the amount of equipment required to be housed in the data Centres to support NBS, particularly with regard to network infrastructure.

The current planning assumption is that there need be no increase in network infrastructure until require ie the initial pilot is carried out on existing infrastructure. This planning assumption will be validated by a Network Study.

Following this, again depending upon the results of the network study, there will be an upgrade to network infrastructure. It is possible at this stage that there will be insufficient room at the existing campuses to hold the additional equipment and a move to a third data centre will be required.

There will be additional benefits in this approach

- The spreading of routers across 3 campuses will provide additional availability and therefore less risk to the service.
- In the event of a data centre loss, there will be an facility to replicate the lost data centre, including the NBE, in a timely manner. This is an extension to the current contractual obligation with regard to the provision of an additional TMS layer.

This is discussed in more detail in sections 3 and 4.

POL00043744

4 Availability and Reliability

4.1 Summary

ICL Pathway expects that there will be additional stringent resilience requirements, over and above those to which the Horizon network is currently liable, caused by the need to support a substantial amount of real-time on-line traffic for Network Banking. The current ISDN network is sufficient to satisfy the low call rate required by the current solution, but further investigation is required to define the network enhancements necessary to meet these additional requirements

It is recommended that a study is initiated to establish the specific requirements with regard to outlet availability and to specify enhancement options.

In addition, the availability and resilience required to support on-line service such as Network Banking could be met by spreading the infrastructure necessary to support Network Banking across 3 Data Centres thus reducing the amount of equipment required in each data centre and reducing the effect of any campus disaster.

Specific key points are as follows

- Instability and risk of new software can be mitigated by plan to pilot
- There will be an upgrade required to the network. This will be defined following a Network Study.
- Upgrades will be required in Data Centre Infrastructure.
- A new availability model needs to be defined and possibility of third data centre examined
- An upgrade to service Pack 4 is required

4.2 Definitions

Resilience is the general term used to describe the measures taken to maximise the *Availability* of an IT system. Availability is a measure of whether the system is able to be used when the users need it. Availability is achieved through a combination of factors.

- *Reliable components*, both hardware and software
- *Detectable failures*, so that a failed component is immediately detected and notified to the support organisation
- *Resilience*, so that major components are replicated or include retries and error processing to minimise the impact of failure.
- *Recovery and repair processes* that can restore a failed component or system to normal operation speedily
- *Distribution, installation and activation processes* that can be used to install and configure components remotely to fix an identified problem, or to minimise the disruption when a key component is out of service
- *Measurement techniques* that may be used to determine the overall availability of the services provided by the information system and whether these conform to agreed service levels.
- *Diagnosability* is the ability to determine the reason for a function failing to deliver the expected output. That includes both the ability of the user to diagnose misuse of facilities and the ability to determine the cause of a product's non- conformance to its specification
- *Supportability* is the ability to provide solutions to problems, and to correct errors, experienced by user.

POL00043744

- *Maintainability* is the ability to prevent failures by correcting faults in a released product

A substantial amount of resilience is provided by the existing Horizon infrastructure. Specific areas where we need to address the resilience of NBS transactions include the following.

- the integrity of transactions authorised by the NBE
- to the delivery of the Confirmation records for transactions.
- problems occurring in the end-to-end NBS system are correctly traced to their cause

4.3 Introduction of Third party software

Third party bespoke software (written specifically for the Network Banking application), and off the shelf products, are expected to be introduced into a number of Horizon platforms. This is based on a set of assumptions derived from the following sources.

- The decision by POCL to specify the use of WebRiposte Framework for the Counter
- The Network banking engine ITT:
  - The network banking engine itself
  - Client side Counter code that will interact with the network banking engine
- IBM note entitled – Network Banking Engine Solution Issues
  - Communication protocols to the Network Banking engine – preferred option MQ series.
  - System management software – Tivoli and BMC Patrol

4.3.1 Counter

4.3.1.1 Application Reliability and SLA issues

The introduction of WebRiposte and software produced by the NBE supplier or other third parties could have a significant impact on currently functioning Counter software, for which ICL Pathway has stringent SLAs, in terms of both performance and reliability. Note that a badly behaved Counter application could impair use of the system,

4.3.1.2 Counter Memory

The WebRiposte Framework product set consumes more memory than the Riposte software used at M1. Current figures show this to be an extra 40 Mbytes By implication, this can introduce memory contention with other software running on the Counter. It may be necessary to upgrade the memory of each counter PC.

4.3.1.3 Rapid Application Deployment

A stated aim of the use of WebRiposte is to speed up the introduction of new applications. However, it should be noted that a significant part of the current "time to market" for new applications is in their testing to ensure that there is no degradation of the behaviour of other applications, and that while SLAs exist, ICL Pathway must continue to provide this regression testing regardless of the source or technology of the new software.

4.3.1.4 Mitigation of Risks

POL00043744

To mitigate the risk associated with introducing third party software onto the Counter, a strict regime of software proving is suggested, including:

- Design reviews
- Code inspections (therefore access to the source)
- Strict Acceptance criteria as defined by [GENAPI} which will ensure that the third party code is non intrusive for existing business applications and works to the defined interfaces
- Thorough testing, concentrating on performance and reliability testing.
- Limited initial rollout (say 100 Counters) with a bedding in period when Counter performance and reliability SLAs will not apply. This will allow ICL Pathway to derive an application footprint, for example in terms of event usage in a live environment.

The level of proving necessary to protect ICL Pathway's current SLAs and to maintain the current Counter reliability levels will be bound to have a significant impact on the speed of functionality rollout.

It is recommended that all third party software introduced to the Counter should be simple to disable (say by Reference Data), in the event that its failure affects other applications. In addition, diagnostics must be included to assist in determining where any exceptions to the desired operation are occuring

Memory management has been improved in later versions of the NT Service Pack. As there is a declared WebRiposte dependency on Service Pack 5, this may reduce some of the risks associated with memory contention.

4.3.2 Correspondence Servers

New Web Riposte software will be required on the Correspondence Servers...

4.3.3 Agent Servers and Applications

4.3.3.1 MQSeries Software Introduction

IBM is proposing the use of MQSeries messaging as the application-level protocol between the Agents and the NBE. While ICL Pathway has not yet investigated the full implications of this, or considered any other options, it is possible to make the following points.

New Agents will be required to connect to the NBE. The IBM solution issues document specifies a preference for MQSeries as the communication (messaging) protocol. ICL Pathway understands that this will require a third party off the shelf product (MQSeries Adapter for NT), which would need to integrate into the Agent. This supports an XML based application protocol.

Conventionally, Agent processes have been developed to connect to an Oracle or SQL Server database running on a Host Server located within the Campus. There are significant implications in developing a new style of Agent that connects to an MQSeries repository. There is the obvious assumption that the MQSeries software will not adversely affect other software running on the Agent servers. MQSeries Adapter software, as a third party off-the-shelf product, can be handled by ICL Pathway's normal validation program.

ICL Pathway understands that MQSeries is widely used within The Post Office, and understands the relevance of this technology to the Network Banking service. However, it has further implications in terms of the infrastructure within the

POL00043744

Campuses. The IBM Web Site implies that the Agent Servers will need to be upgraded to NT Service Pack 5 or later to run the Adapter software.

4.4 Impact of Traffic Levels

4.4.1 General

The introduction of Network Banking will significantly increase the level of real time traffic from Outlets to the Campuses.

This increased traffic will generate more work for many of the components and platforms within the Horizon system. As the utilisation level of these components increases towards their system limits, the reliability, and therefore availability will decrease. This can be addressed in a number of ways.

- By upgrading individual platforms
- By increasing the number of platforms carrying out the function and load balancing across them
- By improving the overall reliability of software on the platform by upgrading to newer software versions. Specifically, a move to later versions of the NT service pack.
- By enhancing the diagnosability and supprtability of the software

4.4.2 Counter

A disconnected Counter will be inhibited from carrying out Network banking transactions. Disconnected Counters occur for two reasons.

- Counter LAN failure
- ISDN connection failure

LAN failures will be reported to the Counter Clerk, and hence these Clerks will be aware that they are inhibited from carrying out banking transactions.

4.4.3 ISDN Network to the Campus

[

4.4.3.1 Network Service Levels

There will be a need to significantly increase the network capacity to ensure that a reliable authorisation service can be offered. There will be higher visibility of any network problems due to the real-time nature of the service.

It will be necessary to define and agree the network availability targets that are required to achieve the necessary increase in on-line traffic.

This will be included as part of a proposed network study.

4.4.3.2 Current network reliability

4.4.3.2.1 General

[PoC] envisage that enhancements would be necessary to the ISDN Network to support the increased traffic levels (particularly real-time traffic) generated by Network Banking. Investigations of the current service have shown some evidence of network congestion with this technology in the Energis network in certain areas at certain times. One effect of this congestion is to cause Outlets to fail to connect to the Campus. As an increase in real-time traffic can significantly exacerbate this

POL00043744

congestion, it is believed to be necessary to re-evaluate the network technology currently being used.

4.4.3.1.2 Analysis of ISDN Network Resilience

An ISDN switched network (approximately one ISDN call per business transaction) is not suitable for supporting a Network Banking type workload. This conclusion is based on a combination of the following factors.

- Conjecture, based on observation, that the achievable availability (as measured by a sequence of call attempt sequences) of an ISDN switched network is no better than 99% and for practical purposes is in the range [94%-98%]
- The assumed on-line nature of the Network Banking Service workload, that is WAN connectivity necessary for providing a Network Banking service to a Customer
- The assumption that the service availability requirement of Network Banking Service transactions may exceed 99.5%. Specifically, no more than 1 in 200 customer transactions should observe "first choice dialogue path failure", to prevent adverse impact on customers of the Network Banking Service

The conclusion that flows from this is that a study should be undertaken to arrive at a cost optimum way of migrating from the switched ISDN network to one that will achieve defined levels of Availability for Network Banking transactions.

4.4.3.1.3 ISDN availability challenges

The factors that limit the service availability provided by ISDN include the following.

- *Call set-up failures due to congestion*. For a call-set-up attempt to succeed requires that resources exist in the BT and Energis networks. These service providers are likely to run their networks at relatively high utilization levels, for cost reasons, especially as steps are approached in their capacity plans. In addition, the likely increased use of non-metered Internet access delivered over both voice and data networks is likely to add to the variability and magnitude of congestion levels
- *Failure detection for long-term outages*. One of the problems with a switched ISDN network is that the service availability cannot be easily monitored proactively. Instead, in a predominantly online transaction based environment, it is the attempt at a WAN connection on behalf of a customer transaction that detects a failure in ISDN Service. This is contrasted with a fixed network (one where a data path is always expected to be available); in this case, a Network Management function can be used to detect a lack of network service (and initiate repair)

Call set-up failure due to Transient problems and handling these failures. For an ISDN call-set up to result in a usable data path requires that a number of layered services succeed in this endeavour (SS7 signalling, Q931 call management, PPP authentication and network path, IP flow, Exception Routing, etc.). The failure in any of these components is likely to result in the failure of the application interaction. The probability of success is increased by use of Managed Router (like) capability at the Outlet,

4.4.3.1.4 Approaches for achieving required availability

There are a number of other approaches that can be investigated (as a Work Study) in order to arrive at recommendations for a cost optimum network change to support of Network Banking

POL00043744

4.4.4 VPN layer

The current resilience model employed shows that the VPN layer is believed to be adequate for current projections. Obviously, if the amount of traffic increases to the point where the system limits of individual servers are being reached, then more VPN servers per cluster may be required.

4.4.5 Campus Network

The increase in real-time and general network traffic (could bring the Campuses closer to the limits of the Campus LAN, which in turn would decrease the system performance and reliability of the network. The resilience model requires that the Horizon system retains the ability to run the complete workload, including Network Banking, even after the loss of a single Campus (or critical Campus platform) or of the inter-Campus network.

4.4.6 Correspondence server

4.4.6.1 NT Reliability

The increased level of traffic will lead to scaleability, memory and reliability issues which can be mitigated by a move to a later NT Service Pack.

It is important that a single Correspondence Server is still able to service all Outlets within the cluster. This may require an upgrade to the hardware platform currently used for the Correspondence Servers.

4.4.7 Agent server

Should the current servers be unable to sustain the load generated by the new Agent processes then new Agent Servers will be required.

As discussed elsewhere, ICL Pathway will need to develop an alternative resilience model for Interactive Agents, for example using a pool of "hot-standby" Agents.. Any changes to achieve a quicker response may need changes to the Systems Management technology.

The Agent Servers are also likely to handle the reconciliation service needed to support the data flows to and from POCL and the NBE. There are not expected to be any significant resilience issues associated with this. The assumption at this time, is that reconciliation is carried out in the Host Central Server, using data feeds supplied by the Agents and by the NBE and TPS Host application. It is also assumed that reconciliation is not a "real time" application, and that it will be handled in a similar way to TPS in that SLAs will be required for the delivery of reconciliation data at TIP but instantaneous delivery is not required.

4.4.8 Network banking engine

The NBE is a new system and it is assumed it will be sized appropriately. It is also assumed that a single NBE server will be able to handle the entire workload generated by the Outlet community, with the other acting as a standby system.

4.5 Solution Availability and Failover

4.5.1 General

POL00043744

The stated NBE availability requirements are 99.999 % between 08:00 and 18:00, with a 3-minute site fail-over.

4.5.1.1 Service Availability Model

It is not clear whether this availability figure applies to other components within the solution, for example Agents, Correspondence Server and the ISDN Router network. It should be noted that availability of Network Banking functionality at the Outlet will equate to the availability level achieved by the weakest single component in the route to the NBE. It is clear that an availability model needs to be defined for the complete Network Banking solution. The model will define the availability of various components, both hardware and software.

4.5.1.2 Availability following a site disaster

POCL need to consider reduced availability figures in the event of prolonged Campus failure. Currently, ICL Pathway is contracted to provide a plan that provides for an off-site copy of the TMS layer within five days from such a site outage. This plan does not include any Host systems or other servers such as the NBE. A third Campus would help mitigate these issues. It would also mean that it would not be necessary for a single Campus to be able to process the whole Horizon workload, as there would always be two other Campuses available. The third Campus and its implications are discussed later.

4.5.2 Counter

No specific availability figures are specified for the Counters. It is assumed that the requirement for 99.999% availability does not apply at this level

4.5.3 ISDN Network to the Campuses

Again, no availability requirements have been specified, but it is assumed that the 99.999% availability level is not required. As discussed elsewhere, there is a need for POCL and ICL Pathway to discuss and agree the availability requirements for the ISDN network given a significant increase in the amount of real-time traffic.

4.5.4 Three Minute Failover

The Network Banking Agents will be affected by the three-minute site fail-over requirement of the NBE. How this is achieved will depend to a great deal on how IBM implements the NBE. Host Server

It is assumed that the 99.999% and three-minute figures are not applicable to the Host system. In addition to their normal use of transmitting TPS data to TIP, the only new use for these servers is to handle the Network Banking reconciliation processes, and these are not as critical as the real-time requirements of the Counter applications.

4.5.5 Network Banking Engine and Links to the Banks

The target of 99.999% availability of the NBE must be measured at the Agent Layer. Thus, the NBE must be accessed via network communications that are resilient to the same degree within the Horizon Campus environment.

All links from the NBE to the banks must be resilient to single points of failure. This includes failure of the banks own systems. It is assumed the banks will provide multiple sites through which they can offer connection by the NBE. It is understood that most banks host their inter-bank systems on Tandem or Stratus Non-Stop technology.

POL00043744

4.5.5.1 NBE Fail-over

Assuming that ICL Pathway operate the NBE it is important that consideration is given to the acceptance process

- ICL Pathway must be provided with the necessary materials and information necessary to understand the technology being used and be satisfied that the design will meet the PON defined requirements
- IBM must develop and prove to ICL Pathway a detailed validation activity for the NBE and prove this prior to systems integration testing. It will be used to test and rehearse operational procedures that must be supplied by IBM to cater for all failure scenarios
- A number of new business continuity tests will be required, including one that proves the three-minute fail-over.

4.6 Software Infrastructure

A number of issues arising from the nature of the Network Banking application components and their supporting middleware will have an impact on the software infrastructure supported by ICL Pathway. In particular, it will be necessary to update both the Counter workstations and Campus servers from NT 4.0 Service Pack 3 to Service Pack 5 or later to support WebRiposte.

Moving to a later Service Pack is a positive move in resilience and availability terms The latest currently available version is SP6a. This is believed to be stable and reliable, but not all of the Horizon commodity software products are yet proven on it, and it is likely that the next major upgrade will be to SP5. However, ICL Pathway has not yet investigated whether it is possible to move from SP3 to SP5 in one step, and in practice, it may be necessary to proceed in a number of less dramatic increments.

There are obvious issues with the rollout of a new Service Pack across the estate. Some of these are not directly relevant to resilience and availability but are included here for completeness.

- There may be issues with effective rollback on failure and should be investigated and rehearsed from the outset
- The NT failsafe operating system partition, installed as a “get out of jail” regression capability on all Counters, will need to be updated at the same time. This is especially important as Service Pack 5 updates the NTFS file system
- Certain third party software product versions in use are supported on SP3 but not SP5. In addition, the latest upgrade to these products may be supported on SP5 but not SP3. It is important to carry out any necessary upgrades in a ‘safe’ order..

4.7 Service Level Monitoring

4.7.1 General

Service levels need to be defined and monitored across the Outlet estate . In addition, any Outlet that exceeds the failure criteria by more than agreed tolerance should be separately identified and the reasons for such poor performance understood and rectified.

It will be necessary to develop data capture mechanisms on various platforms (including Counters), additional data feeds into the Data Warehouse, and additional SLA processing code within the MIS.

POL00043744

4.7.2 Counters

This requirement introduces the need to monitor the Outlet and Counter position availability more closely than is the case at present. It will be necessary to provide metrics for the following.

- Number of application failures
- Number of failed calls to the Campus, with the ability to identify the cause of the failure
- Number of timed out and failed connections to the NBE. This would exclude line faults but would identify those calls that reached Pathway and not the NBE as well as calls that reached the NBE but not the bank.

4.7.3 Disaster recovery

PON need to define the availability requirements for the Network Banking Service in the event of a site disaster. Network Banking introduces a substantial real time service (the NBE) that, if not available, will result in all Outlets being denied access to the service. Because the stated long-term aim is that the Network Banking Service will replace the Order Book Control Service (OBCS), this could result in benefit claimants being turned away, with considerable political ramifications. In the event of a site disaster, a further failure of the NBE will result in complete loss of service, and that situation would remain until ICL Pathway rebuild the lost Campus. The present contractual requirement is to be able to do this within 180 days with the provision of an additional TMS layer being available within days of the failure.. This timescale could be considerably reduced by the introduction of a Third Campus. This need not contain all aspects of the Horizon solution, but would provide an environment within which a full service could be reintroduced in a considerably shorter timescale than 180 days.

The overall strategy would be to set up a third Campus that operates in a similar manner to Wigan in terms of TMS functionality. Sufficient infrastructure would be installed to allow the site to be upgraded to a full Campus within a short timescale. The third Campus would thus, from the outset, contain the following platforms.

4.7.4 Agent Servers

These would be fully Maestro and Tivoli managed, and able to communicate with all Hosts, including the Sequent host, KMA, OMDB and NBE.

4.7.5 Correspondence Servers

The current “wing” Correspondence Servers, and their associated Compaq disk arrays, would be relocated to the third Campus. This would comprise one server per cluster. However, these servers would not handle communications from Outlets. This move removes the need for the Compaq Recovery option, and associated standby servers, at Wigan and Bootle. These spare servers will be redistributed to ensure that the most powerful processors are located in Wigan and Bootle, where the Audit services will continue to run.

The Correspondence Servers at both Bootle and Wigan will be reconfigured with neighbour relationships to the wing servers at the third Campus.

4.7.6 VPN servers

As the third Campus ISDN Routers will be in full communication with Outlets a full compliment of VPN servers will be required.

(Check with Peter wiles-believe this is contradictory to current thinking)

POL00043744

4.7.7 ISDN routers

ISDN routers will be distributed evenly between the three Campuses, with enough Routers and PRI circuits to support 50% of the Counter load at each Campus. The Outlets need to be spread out such that all three Campuses have 1/3 of the Outlets for the primary and 1/3 for their secondary. This can be achieved by changing the mappings of the existing phone numbers across all three Campuses. In the event of a site disaster, it is then possible to change the mappings in a matter of a day or so to ensure that every Outlet still has two sites to call.

Note that if we move to an Energis Data network, it will only be possible to have a primary and a standby number. There will be no option to specify a third choice.

4.7.8 Infrastructure Services

Each Campus will be linked to the other two by 155 Mbps links in a triangular configuration, thus allowing two routes between any two Campuses. One link will be direct and one via the other Campus. Enough infrastructure and space will be available to allow the third Campus to be upgraded to full operation, including a NBE, within a matter of weeks.

4.8 Settlement and Reconciliation

It is assumed that reconciliation between the NBE (and therefore the banks), TIP and the Outlets will be carried out by a separate application. It is further assumed that this new application will be hosted on the Sequent Host Servers, and that it will take feeds from TPS, the NBE and the Riposte Message Store. This new application will follow the design guidelines set out in [HADDIS].

The Network Banking reconciliation application database will have similar resilience characteristics to other Host applications namely:

- All data files will reside on SRDF-mirrored EMC disks. Note that the capacity of the EMC disk arrays will need to be extended.
- Harvesting will be controlled in a resilient manner by the Maestro scheduler, utilising the existing generic dynamic scheduling capabilities.
- Data re-harvest must be possible. It is unclear whether this will be possible using the current mechanisms, as these is dependant on the EoD markers generated at the Counter. If reconciliation is required to operate to some other timescale than the Outlet EoD, then a different mechanism will be required. Note that some Interactive Harvesters are already unconstrained by the EoD markers.
- Cold backups of the Network Banking Reconciliation Host database will be taken after each nights processing is complete
- Files will be sent to PON via an FTMS gateway. It is unclear at present whether this will follow the same route as the files currently sent to TIP, or indeed whether this data feed will be integrated into TIP.

4.9 Audit and Fraud Management

There are a number of possible implications on the Horizon Audit solution.

- Is there a need for the Audit Server to harvest and store information from the NBE? If so, then the NBE will need to support either NFS or NT file shares
- Audit Server sizing will need to be examined. There will be a significant increase in the data that needs to be audited.

POL00043744

- Will there be an increase in the number of requests to retrieve audit information? The current Audit solution is designed to service a limited number of requests (a maximum of 50 per year). Any dramatic increase in requests will require the current solution design to be re-examined
- A Fraud Management system was developed for the PAS/BES system, but removed from the Horizon solution when these applications were dropped. It is necessary to consider whether there will be a requirement for fraud investigations and control with Network Banking. Although the current Audit solution will hold the data that may form the basis for detailed fraud investigations, it is not designed for, nor can it cope with, an on-going fraud management approach based upon statistical analysis of transaction patterns over a wide variety of Outlets.

POL00043744

5 Performance & Capacity

5.1 Summary

Introducing support of banking transactions will have a major impact on the profile of Counter transactions and the message load that they impose on the Horizon infrastructure.

The major reason for this is that banking transactions will require an immediate authorisation from the issuing bank, and hence the Outlet must make an immediate call to the Campus. At present, a call is made every 30 minutes, or occasionally sooner if a priority message is generated (for example in response to an OBCS Foreign Encashment). Moving to a largely real-time call profile will have a significant impact on the equipment needed to support calls to the Campuses, in particular on the instantaneous peak rate that must be supported.

The impact of this will require widespread changes in the Outlet-to-Campus network.

The Network Banking application and its supporting infrastructure (WebRiposte) will operate alongside the existing Horizon Counter applications, and may impact on the existing application behaviour and response times. Prior to the development of NBS, it is necessary to develop capacity management tools to ensure that sufficient resources are put in place to handle the expected workload. Once development is complete, it is expected that performance studies (including video benchmarking) will be needed to ensure that there is no untoward impact on existing applications, and that the requirements on the NBS itself are met.

In case any such significant impact is observed, it is necessary to introduce widespread response time monitoring hooks within the overall Horizon infrastructure (and in some cases into the applications themselves) to ensure that any problems can be quickly identified, and the problem resolved by the appropriate supplier.

In addition, these measuring points will feed data into the Data Warehouse. Enhancements to the Management Information System (MIS) will be needed to provide evidence of adherence to any new SLAs that may be negotiated as part of the Contract discussions prior to the implementation of the NBS.

5.2 Performance Requirements

5.2.1 Data Volumes

One of the key determinates of performance will be the volume of on-line NBS transactions. PON's best estimates, given in [ITT], are:

- Message volumes reach a peak in 2004 (40.95M cash withdrawals, 51.70M cash deposits, 41.22M balance enquiries giving a total of around 133M transactions per annum out of a total of 2,500M)
- The NBE (and hence the link to it from Horizon) should be sized for a "burst" peak of 15,000 transactions a minute, or 250 per second
- The Horizon network must hence support the same peak number of incoming calls from Outlets. Note that, if each call lasts 20 seconds (including set-up) then the number of ISDN lines required would be 250x20, or 5,000

To put these into perspective, one transaction per Outlet per day equates to approximately six million transactions per annum, so the estimates given above would correspond to an average of around 22 NBS transactions per Outlet per day.

POL00043744

Each of these messages is likely to cause an ISDN connection to be made, and thus the peak call rate (the major factor in determining the number of ISDN Routers) will also be around 250 per second. Our standard sizing assumption is that, to cater for disaster situations, each Campus must be able to carry the entire Outlet workload. This workload would thus require 50 Routers per Campus, at a maximum call rate of five calls per second per Router.

There is a major need for further analysis of the likely banking transaction load, and for detailed modelling of the impact of banking transactions on the ISDN call rate.

5.2.2 Counter

5.2.2.1 Interaction with Horizon application

The NB Counter Applications will operate alongside the existing Horizon Counter Applications and will share the resources of the Counter PC.

New Counter Applications must be able to co-exist with existing Counter Applications on the same NT Counter platform, and must run on the current Counter platform without impacting the performance of Horizon applications.

New applications must be able to work within the counter platform else an upgrade would be required.

The counter platform comprises

- CPU (400Mhz PII)
- Memory (128Mb)
- Disc (13Gb)

Note that, given the nature of the Windows NT operating system that controls the Counter terminals, it is not easy to partition applications within a constrained set of resources, or to identify any "spare" capacity that may exist in the current Counters. There is thus no easy way to ascertain whether there will be any identifiable problems with running NBCA and its associated infrastructure alongside the existing Horizon Counter applications, other than by a detailed validation including performance and capacity evaluation and stress testing, with joint action to identify and resolve any issues that arise.

5.2.2.2 Acceptance

All Counter Applications require a performance acceptance process. The Horizon counter transactions were benchmarked as part of the acceptance process at CSR and CSR+.

Because of the extent and complexity of the Release necessary to introduce Network Banking, it is thus expected that all transactions (Horizon & NB) should be re-benchmarked against the response times defined in the updated Contract schedules as part of the acceptance process for the NB Release. This process should include:

- Counter benchmarking by video
- Load/stress testing (similar to 20-Counter benchmark)

5.2.2.3 Model of Counter Transaction Dialogues

5.2.3 The Counter dialogue for revised Horizon transactions and for NBS transactions should be modelled using using current Horizon Benchmarking procedures.**Applications (including Counter Applications)**

5.2.3.1 Response Time Monitoring

POL00043744

The NBS applications differ from the existing Horizon applications in that they require on-line access to the Horizon Campus, to the NBE and the banks. Managing response times in this complex network environment will require the system to collect response time data to support:

- Service management
- SLA management
- Performance investigations

Other data may need to be added to the message, for example to assist in fraud investigations. Note that this will increase the message sizes, and will have a knock-on effect on network utilisation and data storage. The infrastructure that is designed to support all the requirements described above will have to be well thought through to ensure that it does not impose an unacceptable load on the system.

Time stamping of messages should take place at all major application interfaces including:

- Counter NB application <-> Horizon application interface
- Counter application <-> Riposte interface
- Riposte <-> WAN network interface
- Horizon <-> NBE
- NBE <-> Banks

However, note that time stamping as such may not be sufficient for a number of reasons, including the following.

- Clock synchronisation is not perfect
- Clocks can change as a result of Riposte synchronisation
- Normal timestamps are in seconds and this may be too coarse for detailed SLA calculations

A better mechanism may be for each component to time (using tick counts, say) the time it believes another application has taken, and also the time it has taken itself. The difference between the Counter times for a request to the Campus, and the Agent time for handling the same request, is the time lost in replication and communications.

Data that has been captured can either be stored in file on the Counter and harvested later e.g. overnight, or stored as part of the message. The later method has advantages in that it will be continuously available and can be automatically fed to the Data Warehouse. The data will be processed by the MIS and a set of reports generated. Ad-hoc reports will also be required to support performance investigations.

5.2.3.2 Reporting and Logging of Failures

As discussed extensively elsewhere, the current Horizon system has a very small on-line component, and therefore the network infrastructure has been optimised to support the periodic replication generated by Riposte. The introduction of the NBS will change the workload profile significantly and new features will be required to manage the resulting SLAs. For example, the management of incidents where the outlet has failed to contact the Campus need to be pro-actively managed if NBS service levels are to be retained.

Thus, some level of automatic reporting of failures will be required. Where appropriate, data about the failure (e.g. network response code) should be added to the message that failed to make contact with the Campus.

To support this infrastructure, the Counter Application that generates the failure message will need access to data stored in the network adaptor in the Counter PC.

POL00043744

Note that a NBS Confirmation message is expected to be generated, even where the transaction fails, to enable matching with the Request and enable full reporting.

The same reporting mechanism should be used to record all of the following failure types:

- Failure of outlet to contact Campus
- Failure of Horizon Agent to contact NBE
- Failure of NBE to connect bank

This data will be used by the DW to *adjust* the calculations of SLA achievement, where necessary.

5.2.4 Service Level Agreements

5.2.4.1 Response Time SLAs

The response time requirements for the NBS transactions should be defined in the Contract Schedules for these transactions. If more than one supplier is involved, then the response times should be defined at each contractual SLA boundary. SLA boundaries must be defined at an interface that is measurable.

If the NBS applications require changes to be made to the existing Horizon application environment e.g. menu hierarchies, then this will have a knock-on effect on the dialogue required to process an existing Horizon transaction. Any such changes will require the current SLAs for Horizon counter transactions (as defined in the Contract Schedules) to be updated to bring them in-line with the new dialogue model.

The Horizon system has SLAs for complete transactions as seen by the Counter. The NBS system will run a mixture of Horizon and NB transactions with the NBS transactions potentially coming from a number of separate suppliers. In these circumstances, the definition of SLAs should reflect the multi-supplier state.

Note that, as a result of investigations called for by **Error! Reference source not found.**, different Outlets may well use different network technologies. For example, some Outlets may move to permanently connected circuits, while those where the volume of NBS transactions cannot cost justify permanently connected lines will stay on dial-up lines. The SLA calculations should reflect this, with different SLAs for different outlets or sets of outlets.

The SLAs should reflect the varied demands that will be placed on the services in different time periods. The system should have sufficient capacity to meet the SLAs at the times when the system is under peak stress. However, the greatest level of stress on the system may occur on only a few days a year and for a few hours within that day. The current Horizon system is sized to meet the highest peak loads on the busiest days of the year. This can be justified where the ISDN call rate at the Campuses is essentially static. With Network Banking, however, it is worth considering whether it is reasonable to relax the SLAs during these periods as this could result in a considerable saving in the cost of the platform and infrastructure required to support these peak-on-peak loads. This would need to be traded-off against longer queues in the outlets during these periods.

SLAs should be defined in terms of:

- End-to-end SLAs and
- SLAs of each component measured at a contractual boundary.

The SLA boundaries should be clearly defined. (The Horizon Contract defines logical boundaries and these have been difficult to police. Putting third party code into the Counters could make this significantly more difficult.). They must also be measurable.

POL00043744

Timestamps can only be taken within a platform, but there is likely to be a component of the elapsed time to perform a function e.g. platform to network, that is logically part of the SLA for that component but may fall outside the capture window. This must be reflected in the definition of the SLAs

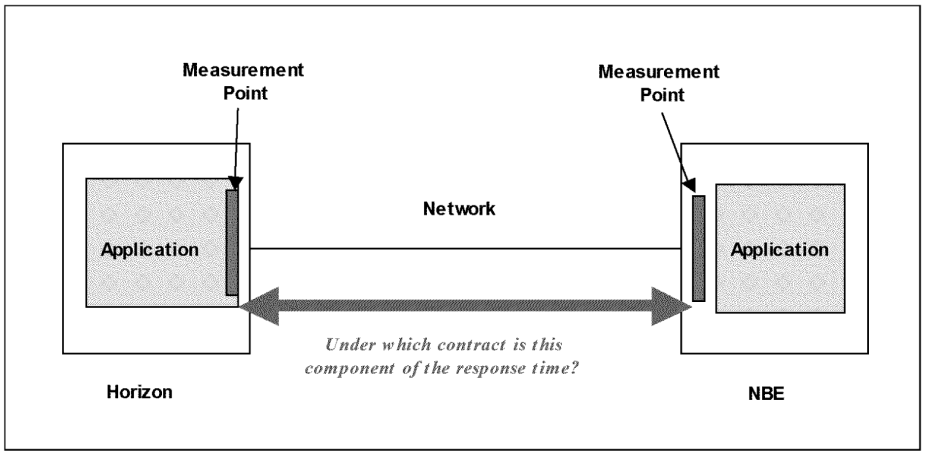


Figure 4 – SLA Measurements

The data to be collected at the SLA boundary should be defined as part of the interface description.

5.2.4.2 Workload Definition - Transactions .v. Messages

The units in which SLAs are defined should be measurable. A transaction is a logical measure whilst a message is a physical measure.

If one part of the system changes, e.g. by the addition of a message to a transaction, this may result in a significant increase in the workload processed by some parts of the system which could result in additional capacity being required.

5.2.4.3 SLA Calculations

SLAs will be calculated in the Data Warehouse

5.2.5 Capacity & Scalability

5.2.5.1 System Capacity Plan

The system capacity plan will co-ordinate and report on all capacity issues relating to all components of the system.

Workload modelling is the essential first step in determining the capacity required to support the NBS workload. The workload should accurately document the profile of work (on-line transactions, overnight batch, support tasks, etc) that the system must be able to process and the time window in which it must be processed.

The accurate definition of the workload components will enable the capacity of the system to be determined more accurately. This will have the benefit of:

- Reducing the need for additional contingency
- Enable the risk to be accurately assessed and the effect of change during the design & development process to be accurately assessed

The capacity must be flexible enough to process the peak daily, weekly and monthly cycles of POCL business and to utilise the assets as efficiently as possible.

POL00043744

The modelling will represent the growth in capacity needed as NBS volumes increase. This approach will allow the phasing in of enhancements to the infrastructure to ensure capacity remains ahead of demand.

5.2.5.1.1 Business Workload Model

The business workload model will define the business workload that the system is to support. Pathway will manage the development of the business workload model and will review the model and report on the updated model to POCL every 3 months.

The business workload model should include:

- Accurate workload projections for 6 months, 12 months and 18 months into the future
- Theoretical projections for 24 months or longer.

To construct the projections the model must include data on:

- Peak on peak volumes
- Distribution of workload by time
- Workload profile
- SLAs
- Batch schedules
- External file deliveries
- Growth over time from the date of service introduction
- Resilience requirements Response time requirements
- Data delivery to external systems
- Systems management inc. roll-out and software distribution
- Data change e.g. Reference Data
- Data retention/archiving
- Audit

The business workload model should include both:

- The Horizon workload (OBCS, APS, EPOSS, LFS)
- The NB workload.

The business workload model will capture the SLAs that define e.g. data delivery times.

The first iteration of the business workload model will be created by NB WP3a.

5.2.5.1.2 System Workload Model

The system workload model will map the business volumes onto the volumes of messages:

- Transmitted
- Processed and
- Stored

by the system during different time periods to determine the peak workload that the system has to support in each major time window.

5.2.5.1.3 System Capacity Model

The system capacity model defines the capacity required to support the volumes system. The first iteration of the system capacity model will be created by NB WP3b.

The system capacity model will determine the size of platforms, including storage and network requirements, needed to support the workload in a defined time window.

POL00043744

The capacity required to support the Horizon system is based on the requirement for a single Campus to support the full workload with no degradation in service. This is based on a 100% redundancy model across two Campuses.

Because of the enhanced resilience requirements of an on-line service, one option is to reduce the total capacity required and to reduce the time to recover (to a fully operational two site model) following a site disaster. ICL Pathway is proposing a Third Campus as part of the steps necessary to meet the resilience requirements of Network Banking. With this, each Campus would need to be able to support only 50% of the total workload capacity, and therefore only 50% redundancy is required. Not all components need be present in all Campuses, as long as there is a plan to rapidly upgrade the remaining Campus up to full capacity e.g. a second NBE, within 30 days of the disaster.

There are a number of strategy decisions to be made regarding the capacity planning and management; for example

- How are planned changes to the workload included in the capacity plan
- How should the capacity plan be reviewed and approved

Further discussions are required with POCL in this area. Questions which need to be resolved include

- Who manages and reports on the end-to end performance and capacity of the system?
- How are planned changes to the workload to be included in the capacity plan.?
- How should the capacity plan be reviewed and agreed?

5.2.5.1.4 System Scalability

The major architectural principle in the Horizon system is to allow scalability by "sideways expansion" in most cases. That is, where a platform is provided to carry out a certain function, an increasing demand for this function is normally catered for by providing additional similar platform instances sharing the workload. As well as providing for scalability, this provides a degree of resilience, especially where the additional platforms are geographically separate, for example in different Campuses. Performance modelling is used to verify that scalability is feasible, and to identify any discontinuities that may arise.

Where this is not possible, scalability is provided by the potential to increase the size of the particular platform.

Both these approaches are used, as shown here.

POL00043744

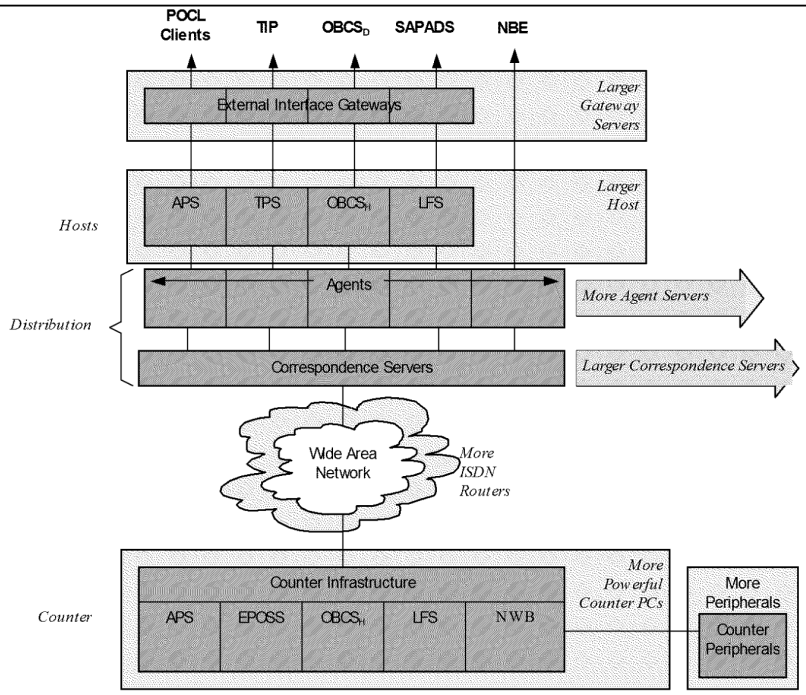


Figure 5 – Scalability

It is unlikely that the hardware required to support full rollout will be deployed from day 1. The hardware deployed at all times must be capable of supporting the projected workload with planned spare capacity:

- How is the planned scale-up hardware of the hardware managed?
- What headroom is acceptable at each major step in the rollout?

A scalability plan should be maintained for all major components of the system. These will be developed in an appropriate time-scale to meet the performance requirements of the solution, and will then be maintained over time to reflect the findings of performance monitoring/capacity planning activities which may take place, and in particular to reflect observations made in the live service. They will detail the planning information required to safely and successfully manage and control the deployment of the necessary scaling options for the necessary components within the necessary time-scales.

The Horizon system is designed to support the peak on peak workload within the SLA and response time requirements. The Horizon workload is very peaky, with the peak workload only being supported for a small number of hours per week and the peak on peak workload a small number of hours per year.

The system must support the workload defined by the current Contract plus the network banking workload.

To support higher workloads requires either:

- More capacity to be delivered than is required or
- Some of the headroom to be used to support the increasing workload therefore reducing headroom and increasing risk

Two work packages have been defined to evaluate and define the capacity characteristics of the system:

POL00043744

- NB WP3a – Workload Model
- NB WP3b – System Capacity Model

The models will have to consider all options including:

- Implementation options e.g. different network models may be used for different sizes of outlet – a large outlet may be permanently connected to the Campus and a small outlet may continue to utilise ISDN dial-up.
- Disconnects in the scalability of a particular component or layer requiring a change of component or architecture to support higher volumes

5.2.5.2 Demonstrating Scalability

Some major components of the system are so complex that it is not possible to model the solution with any degree of certainty. It is therefore necessary to determine the performance characteristics of these components in the laboratory, to determine their:

- Scalability curve
- Limits
- Bottlenecks

5.2.5.3 Component Scalability Plans

A component scalability plan is required for each key component of the solution, i.e.

- Counter
- Outlet to Campus Network including the ISDN Router layer
- Campus LAN
- VPN layer
- Correspondence Servers
- Agents Servers
- Host Central Server (Reconciliation Engine)
- Data Warehouse
- Horizon/TIP network connections
- Horizon/NBE network connections
- NBE
- NBE to Banks network connections

These plans will document the workload and capacity models for each component of the system, and will determine how additional capacity could be delivered over and above the requirements in the business workload model if:

- The workload were to grow at a much faster rate than expected or
- A component or layer of the system cannot support the planned workload

5.2.5.4 Data Distribution

The overnight schedule is driven by the SLAs for data distribution from Horizon to POCL & POCL Clients or from the Campuses to the Counters.

Some components of this overnight batch workload have proved to be very peaky, in particular Reference Data distribution. Significant steps have been made to smooth the load on the Horizon estate due to the processing and distribution of Reference Data.

The data distribution processes required to support NBS must ensure that the data delivered to Horizon will not demand the deployment of large amounts of capacity to support infrequent demand.

5.2.5.5 Schedule

POL00043744

Interaction between the current batch schedule and the schedule required to support new applications may impact the delivery times of current tasks which may have a knock-on effect on SLA delivery times. Where possible, current tasks and new tasks should not be scheduled concurrently unless there is demonstrably sufficient capacity to support the two sets of tasks running within the same time window.

As the workload is migrated to the new applications, the workload processed by *some of* the current tasks will reduce. This will reduce the load on some resources within the system. Any planning of the schedule must take into consideration the changes in workload volumes during the transition from the current workload model to the new workload model. Modelling of the schedule should include all key changes to the schedule that will take place during the transition.

Issues identified can be resolved by either:

- Increasing the resource level to support both sets tasks of tasks concurrently (e.g by increased platform capacity)
- Re-scheduling existing tasks (and re-defining the associated SLAs) to free up capacity to support new tasks

5.2.6 Service Performance and Capacity Management

5.2.6.1 Service Management

The end-to-end performance and capacity of the system should be managed through a single interface even if each of the suppliers is responsible for the performance and capacity of the service within their service boundaries.

Planned changes to the workload and/or the capacity required to support the workload will be documented in the capacity plan that will be reviewed by all service providers and approved by POCL. Pathway will manage the master workload capacity plan on behalf of POCL.

5.2.6.1.1 Performance Problem Management

When/if performance problems occur how are they managed and resolved?

- Who manages the resolution of the problem? If there is more than one supplier what are the obligations of the supplier
- Boundaries between components of the system should support monitoring that will enable performance problems to be isolated to a particular component of the system
- How is the specification and delivery of additional monitoring that may be required to identify and resolve performance problems managed?

Further discussion is required with Post Office to address the above questions.

5.2.6.1.2 Performance Monitoring Tools

The tools used to measure and evaluate performance should be able to produce consistent output across all the platforms in the solution.

The tools used to monitor performance should record

- Platform and disc subsystem resource usage statistics
- Application statistics
- Data & database statistics
- Network statistics

ICL Pathway is currently deploying Metron's Athene product to performance and capacity manage the platforms in the live estate.

POL00043744

5.1.1.1.3 Service Workload Management

The workload should be continuously monitored and the following measures should be assessed against the workload model for the system:

- Daily volumes and response times
- Hourly peak volumes and response times
- Instantaneous peak volumes and response times
- Peak on peak cases e.g. Bank Holidays or Christmas

Reports should be regularly produced detailing the workload volumes and response times

5.1.1.1.4 Service Capacity Management

The capacity of the service should be regularly reviewed against:

- Workload growth projections from the live service
- Workload growth projections from the business model
- Resource growth projections to support the workload growth projections

This will ensure that any capacity upgrades can be made to the system in a timely way.

Projections should be maintained for six, twelve and 18 month forward windows

POL00043744

6 Security

6.1 Summary

The introduction of Network Banking into the Horizon system will significantly increase the complexity of the interacting security domains within the system. It also raises issues to do with the external security constraints applied to banking transactions, arising (for example) from the Data Protection Act.

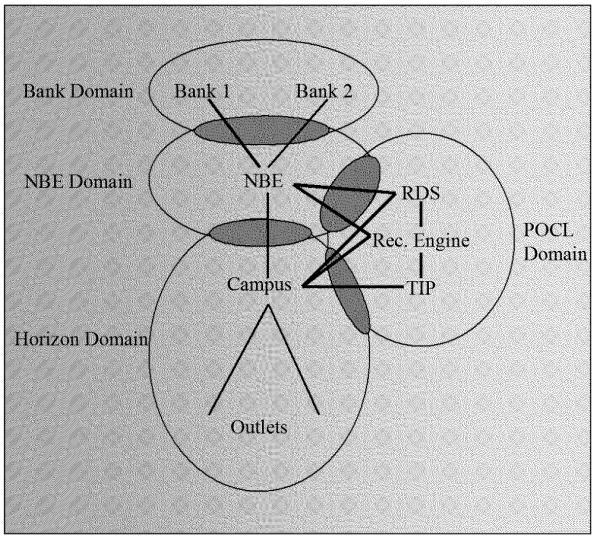
The system will be responsible for disbursing large amounts of money to Post Office customers, and it is important that this money is properly accounted for and that any potential for fraud is removed. This requires clear boundaries between the responsibilities and liabilities of the various parties to the overall solution.

A number of issues of liability are not properly clarified in [ITT] or in discussions following on from that. These include:

- Acceptance that the banks will be satisfied with authentication provided solely by signature
- Specification of any points within the end-to-end solution where encryption of data is required
- Responsibility for prevention of "hacking" or software failure in an environment that includes bespoke code provided by a number of suppliers while maintaining the supportability of the system components

6.2 General

The NBS environment is considered from the perspective of Domains and their inter-connections - see Figure 6. Notwithstanding the on-going discussions on the co-location of the NBE, the key determinants of the Domain boundaries are Ownership and Responsibility. The approach adopted is not to exhaustively examine all possible security criteria, for example to encompass the security relevant functions identified within the Codified Agreement, [SFS] and [ACP]. Rather this paper focuses on the end-to-end security issues and options pertinent to Network Banking, with the express purpose of allowing POCL to derive the overall security requirements of the Network Banking environment.



POL00043744

Figure 6 – NBS Security Domains

It is not possible to define the over-arching security philosophy of the NBS environment, shown in Figure 6, at this stage. At either end of the spectrum of possibilities, the two approaches are:

- *Trusted Domains*, whereby each Domain is trusted to be "well-behaved" in its internal operations and interactions with the other Domains. As a consequence, minimal protection mechanisms are placed on the inter-connections between the Domains
- *Self-Protecting Domains* whereby each Domain takes no cognisance of and places no trust in, the security posture of the other Domains. Thus, each Domain takes all appropriate measures to protect itself on any and all inter-connections with the other Domains.

In practice, the approach adopted will differ for each connection based upon a consideration of the following factors:

- Security Assertions for each Domain
- Evidence provided to support the Assertion.
- The 'strength' by which the Assertion is implemented
- The Residual Risk within each Domain
- Liabilities 'carried' by each Domain
- The nature of any connection between the Domains (both in terms of application and technical features, facilities and capabilities)
- The Risks (technical, application etc.) associated with the interconnection
- The requirement to support and maintain the application software

Examples of the security assertions for each domain are included in Appendix A

Within the remainder of this Chapter, the security issues of the NBS environment are described in the following areas:

- Exclusions & Unknowns.
- Assumptions.
-
- .
- Consideration of security issues and options

6.3 Exclusions & Unknowns

- The Legal and Regulatory requirements as they may apply to NBS have not been identified and have not been addressed within this Report.
- The provisions of the Banking Code as they may or may not be applicable to NBS have also not been identified and have not been addressed.
- Audit and Reconciliation issues are not specifically considered
- Physical and procedural security requirements are not considered
- Security requirements that may be imposed by the bank(s), either collectively or individually, have not been identified and are not considered

6.4 Assumptions

POL00043744

6.4.1 Arising from the Data Protection Act 1998 (DPA)

- Some of the information contained within NBS transactions will fall within the context of personal data, as defined within the DPA
- Each Bank will be the Data Controller of the NBS information relating to its own clients
- POCL, ICL Pathway (and IBM?) will operate as Data Processors on behalf of the Bank(s) as regards the NBS information

  Note the seventh principle of the DPA requires that the Data Controller "Shall take all appropriate technical and organisational measures against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

It is presumed that the banks will:

- Require the Post Office (Data Processor) to enter into a Contract that ensures that the PO will only act on instructions from the Bank (Data Controller).
- Require POCL to comply with the provisions of the seventh principle of the DPA
- Seek an indemnity from POCL for any breaches arising from any default by POCL

It is the responsibility of the Bank(s) to obtain all necessary agreements and consents from their customers that allow Post Office Counter staff to access their account information on-line

6.4.2 Verification

Post Office clerks will verify NBS transactions using (manual) procedures and checks that have been agreed and approved by the Bank(s)

6.4.3 Authorisation Risks

The Bank(s) accept all authorisation risks associated with NBS transactions.

6.4.4 Validation and System Acceptance

Validation and acceptance of the end-to-end NBS environment is the responsibility of the Post Office.

6.5 Consideration of security Issues and Options

6.5.1 Security Definition and Control of Interconnections

A mechanism is required by which the security aspects of a connection between any two (or more) systems can be documented and managed in terms of the connection, operational management, risk management and responsibilities of all involved parties.

The proposed vehicle to solve this issue is the provision of an Inter-connection Security Policy (ISP) for *each and every* connection between systems that crosses a Domain Boundary.

The *Interconnection Security Policy* (ISP) is a formal Document that is to be agreed by all of the involved, parties and is subject to periodic review and confirmation.

- In relation to Figure 6, there would be a separate ISP for the following connections:

POL00043744

- Horizon and POCL
- Horizon and NBE
- NBE and POCL

- Between the NBE and the Bank(s) there would need to be a separate ISP for each NBE/Bank (n) connection

In broad terms, an ISP will contain the following information about the interconnection:

- Description of the Interconnection – identifies the systems involved and their function, connection technology, functions, operation etc.
- Assertions of security posture of the respective systems
- Assertions of security posture for the inter-connection
- Security measures applicable for the inter-connection, cross-referenced to the applicable security assertions
- The security functions, measures, operations to be performed by each party (outside of the inter-connection), cross-referenced to the applicable security assertions
- The Residual Risk for the inter-connection, identifying assertions that are not, or only partially, met
- The agreed mechanisms, procedures and processes (for each party) for the continued operation of the connection (e.g. responsibility for Crypto key changes and frequency, application of 'hot' fixes to meet discovered vulnerabilities)
- Agreed mechanisms, procedures and processes in the event of an actual or potential breach of the security posture. This should particularly address the security criteria for disconnection, e.g. detection of an actual or potential Denial of Service attack
- Procedures on the notification of a change or event in one of the (connected) systems that may affect or impact the security posture/risk of the interconnection. Examples include 'hacking' or virus incidents.

6.5.2 Securing the NBE to the Banks)

6.5.2.1 Securing the Bearer Network and communications entry/exit points

It is presumed that the NBE will connect to each of the participating Banks via a dedicated leased line (2Mb). Under this scenario, the preferred mechanism to secure the connection is to use Hardware encryption devices, using this technology provides multiple benefits:

- The communications line and communications ingress/egress points (at both sites) are secured against external attack.
- Confidentiality of the exchanges (over the bearer network) is ensured.
- Integrity of the exchanges (over the bearer network) is ensured.
- There is an implicit identification and authentication of both the Originating and Receiving sites.

Since the information exchanged relates to financial information it is assumed that commercial grade crypto hardware and algorithm(s) would provide a sufficient level of protection.

A software based encryption mechanism would provide equivalent levels of protection, but must be accompanied by two caveats:

- There would be a performance 'hit' using software encryption.
- Software encryption will be more 'intrusive' into the Bank(s) system and thus may encounter some resistance.

POL00043744

As with all crypto based solutions there is the need to provide accompanying Crypto and Key management functions. Thus in order to avoid a fractured and complex environment consideration should be given to forming a single crypto authority and common solution covering all of the NBE to Bank(s) connections. Note there would be some advantages in extending this scope to also include the cryptographic management of other exchanges within the NBS environment (i.e. NBE/POCL, NBE/Horizon, Horizon/POCL).

If a crypto based solution is not deployed for the NBE-Bank(s) connection then depending upon the identified risk a more complex Architectural/technical/application environment may be necessary to provide equivalent levels of functionality/protection; for example, a DMZ with proxy agents for the NBE.

6.5.2.2 Protecting the NBE from Network intrusions

It is necessary to consider how the NBE is to be protected from Network intrusions originating from either the Banking systems or external sources (where there is no protection of the connecting network). To a large extent the necessary protections will be dependent upon the assertions that can be made (and demonstrated) by the Banks and the Liability that is to be carried at the NBE. At a minimum checks should be instantiated to only allow authorised and approved services and protocols into the NBE environment eg using a filtering router. At higher levels of Risk, consideration would need to be given to validating the content and 'pattern' of packets as they are received. From a technology perspective consideration this would give rise to a possible combination of screening router, firewall and intrusion detection software.

6.5.2.3 Authentication, Integrity and Non-repudiation of Information Exchanges

The issues/measures described above are solely concerned with protecting the communications layer. They do not, in themselves, guarantee the validity and correctness etc. of any information exchange. Whilst these later factors are partially dependent upon the assertions that can be demonstrated for the NBE and the Bank systems, it is essential that the adopted mechanism of exchange have positive measures that satisfy these requirements. Critically, the issue of non-repudiation needs to be considered in conjunction with the issue of Liability and how is this to be apportioned/decided in the event of any disagreement.

Care should be taken as to what measures are agreed with the Banks to address these requirements. If individual solutions are provided for each Bank then the NBE interface becomes extremely complex.

On a technology note, digitally signing each transaction/information exchanging would address the needs of authentication, integrity and non-repudiation.

6.5.3 Securing the NBE to Horizon Connection (not Co-located)

6.5.3.1 Securing the Bearer Network and communications entry/exit points

These are the same issues as covered in the Inter-connection between the NBE and the Banks, but in this case they are to be applied to the NBE/Horizon inter-connection. The critical difference is that there is NO identified (to-date) hardware encryption device that will meet the necessary performance characteristics required of this connection. This would lead us either into the area of software encryption (with the associated performance 'hit') or the use of alternative (weaker) mechanisms (e.g. IP/MAC address filtering) combined with more complex architectural models (e.g. introduction of DMZ's/Proxies).

6.5.3.2 Protecting the NBE/Horizon from Network intrusions

POL00043744

These are the same issues as covered in the Inter-connection between the NBE and the Banks, but in this case they are to be applied to the NBE/Horizon inter-connection.

Note: if a Firewall is required to mediate this connection, then careful consideration needs to be given to the Firewall configuration because of the performance characteristics of this connection.

6.5.4 Securing the NBE to Horizon Connection (Co-located)

6.5.4.1 Securing the Bearer Network and communications entry/exit points

In a co-location scenario this is not applicable since there is a common secure physical environment that protects both systems.

6.5.4.2 Protecting the NBE/Horizon from Network intrusions

There is no need to provide protection against 'external' network threats, since this has already been applied at the Bank(s)-NBE boundary. However, since the NBE boundary protection is also being used to protect Horizon then there must be joint POCL/Pathway agreement and approval of this boundary protection layer.

Co-location of the NBE and Horizon, as recommended above, will result in higher levels of trust between the two systems. However, because the differing ownership and responsibilities for each system, it is important to establish the liabilities of each party in order to determine the appropriate measures to be implemented. At a minimum mechanisms, that only allow authorised and approved communications protocols and services between the systems should be put into place (e.g. screening router).

Note: the initial presentations from IBM have proposed that the operational environment will include a test environment with direct connections to second line Application support. Any operational NBE solution that includes a test and development environment will significantly increase the Risk and Threat to Horizon and result in rigorous and stringent requirements to protect the Horizon system. It should be noted that the Horizon Campus environments do not provide test capabilities; all testing is carried out on test rigs in a different location. Further, the possibility of adding other channels, for financial transactions, into the NBE has been stated. This will affect the risk profile associated with the NBE and correspondingly impact on the measures to needed to protect the connections NBE-Banks and NBE-Horizon. It is strongly recommended that a separate test platform is provided by IBM for NBE testing outside the live environment.

6.5.4.3 Authentication, Integrity and Non-repudiation of Information Exchanges

These are the same issues as covered in the Inter-connection between the NBE and the Banks. Irrespective of the issue of the co-location of the NBE, the differing ownership and responsibilities of the respective systems together with the liabilities carried by Pathway ensure that Authentication, Integrity and Non-repudiation will be MANDATORY requirements for all exchanges between the NBE and Horizon. As noted previously Digital signatures would be one mechanism to satisfy all of these requirements.

It should be noted that there is a scenario whereby TWO digital signatures will be required for all NBE-Horizon exchanges.

6.5.5 Securing the NBE/Horizon to POCL Connection

6.5.5.1 Securing the Bearer Network and Communications Entry & Exit Points

POL00043744

These are the same issues as covered in the Inter-connection between the NBE and the Banks, but in this case, they are to be applied to the NBE/Horizon to POCL inter-connection. Again, a hardware crypto device is the recommended solution

6.5.5.2 Protecting the NBE/Horizon from Network intrusions

It is presumed that the principle function of these inter-connections is to execute a (nightly) file transfer to POCL of Reconciliation data; it is further assumed that there is a level of trust between the NBE/Horizon and POCL system. Provided the assumptions are correct then minimal protections measures are required for this interconnection (e.g. screening router).

6.5.5.3 Authentication, Integrity and Non-repudiation of Information Exchanges

These are the same issues as covered in the Inter-connection between the NBE and the Banks. If the assumption that the inter-connection is for the transfer of Reconciliation files were valid then digitally signing the files would provide sufficient guarantees for these requirements.

6.6 Securing the NBS Transactions across Horizon

In essence, for the NBS environment, the purpose of the Horizon system is to securely execute the end-to-end processing and transfer of NBS transactions between the NBS counter application and the NBE. From a business perspective, the fundamental 'driver' for this requirement are the inherent contractual liabilities carried by Pathway that will undoubtedly be extended by NBS.

The inherent architecture of Horizon is such that it is possible to assert that Horizon contains sufficient security measures that preclude any significant risk of external penetration; hence, the principle risk to be address is to ensure that there is no accidental or deliberate cross-pollution between the NBS context and other Horizon activities.

In an ideal scenario the enforced separation of NBS and other Horizon transaction would be achieved by establishing a secure compartment/pipe that extends from the counter (includes the NBS application), across the Horizon infrastructure and ends at the boundary with the NBE. Whilst desirable, retrospectively trying to impose this architecture onto the extant Horizon would equate to a fundamental redesign of the whole system and is thus neither practical nor feasible. The alternative is to apply security measures/principles that will, in practice, achieve that same effect within an acceptable level of residual risk.

6.7 Transiting the Horizon Infrastructure

6.7.1 Integrity

The essential need is to preserve the integrity of NBS transactions across the Horizon infrastructure. The simplest mechanism for ensuring integrity is to digitally sign each and every transaction. The following criteria would then arise from the adoption of digital signatures:

Each transaction would be Signed 'on entry' into the Horizon Domain:

- At the desktop – the signature would need to be applied at the point when the transaction was written into the message store.
- From the NBE – the signature would need to be applied at the point of entry into the Horizon Domain.

POL00043744

Signatures would be verified 'on exit' from the Horizon Domain:

- At the desktop - on 'delivery' to the NBS Counter application.
- To the NBE - whilst in principle this should be the boundary with the NBE there may be some value in requiring the NBE to validate the signature.

Since the requirement is to preserve the integrity of the transaction across the Horizon infrastructure, the digital application of the digital signature would be a Pathway responsibility.

Digitally signing transactions will impact four areas of the Horizon environment:

- *WebRiposte* – discussed later.
- *Agent Servers* – It is presumed that the agent will NOT transform or translate the NBS message before it is passed to the NBE, otherwise there is no guarantee of integrity. If a translation or transformation is necessary then it will be necessary to log the modified message, as sent to the NBE, in addition to the message from the Counter. The latter is already held in the Message Store.
- *Agents (Signing)* – Transactions received from the NBE will need to be signed before they are entered into the Correspondence Server, again if there is any transformation/translation then there will be a REQUIRED (?) audit record containing the original message and amended message sent to the Correspondence Server.
- *Crypto & Key management* – a new crypto Domain would be formed for the NBS signing.

6.7.2 Confidentiality

There is no identified need for confidentiality of NBS transaction. If required, this can be achieved by (software) encryption. The key issues/decisions are:

- To identify where does the responsibility lie (i.e. within the NBS desktop application or as a part of the Horizon Infrastructure) and specifically who has the liability.
- What data is to be encrypted?
- Impacts for Audit & Reconciliation (dependent upon data to be encrypted)
- Crypto & Key management impacts.

6.8 NBS Application at the Counter

In considering the security environment for NBS at the counter, the decision as to whether Pathway or a third party provides the NBS counter application has a significant impact on what security measures are to be applied, essentially because of the differing responsibilities and liabilities that result. Indications of some of the potential impacts are provided below and in the sections following.

6.8.1 Authentication Integrity and Non-repudiation

As identified previously there is a need to ensure that any NBS transaction/information - came from an authorised source has not been amended and cannot be repudiated. It has also been suggested that digital signatures can satisfy this requirement. This scenario is complicated when a third party provides the NBS application i.e. what reliance/trust can be placed in the third party application digital signature (correctly applied, what algorithm, strength etc.) and what liabilities arise in the event of any failure (note there is an attendant issue of how to identify and allocate fault).

If there is no reduction in the Pathway liabilities then a separate signing process must be applied by Pathway *(note similar arguments apply to NBE transactions sent to the NBS application)*. The end effect could be that TWO digital signatures are required for all NBS transactions with Pathway.

POL00043744

As noted previously the implementation of cryptography will be greatly simplified if there is a common signing mechanism used by all parties and a single crypto authority and key management regime is adopted.

6.8.2 Securing the NBS application

See discussion under WebRiposte.

6.9 WebRiposte

WebRiposte is an Escher provided product that "extends and enhance the functionality and scalability of the existing Riposte message server and is fully web-enabled". The product allows the execution of web-based applications, through Riposte, and claims "built-in support for secure, highly scaleable Web based transaction processing".

So far it has not been possible to validate or confirm the claim for secure operation since the product information provided to-date has not included any explicit or detailed description of the security architecture, security features/measures. Notwithstanding this lack of information initial investigations have identified a number of issues related to the product itself and its use within Horizon and are further described below:

6.9.1 Proxy Server, FTP Server and Web-based Administration and Configuration

These services are *not* required for NBS and introduce security risk into the Horizon system. They must be removed from the version deployed within Horizon.

6.9.2 HTTP Server

To establish secure operation of this component, further information is required on what capabilities/facilities have been implemented, the required/desired configuration settings for operational use and the available security settings. Of particular concern is that the HTTP server will 'open' the HTTP port on each Counter, this needs to be secured for an operational deployment.

6.9.3 SOAP Server

SOAP is a protocol within HTTP that allows language independent execution of objects. Within the provided documentation it is stated that the SOAP server will only support Riposte APIs, this needs to be confirmed by Escher. Any additional capabilities/functions will need to be documented and described. Within the Horizon environment it would be desirable to be able to constrain the objects that can be invoked by any particular browser application – to ensure that no application can invoke services outside of its boundary.

6.9.4 Using the Message Store as a Program Repository

As discussed extensively elsewhere, Escher is currently proposing that a number of program objects (e.g. Java Objects, XML transaction definitions, Framework DTDs) are held within the Riposte Message Store, as opposed to within the Counter filestore. It is further proposed that each of these objects is signed and the signature will be checked prior to execution.

Apart from the possible effect on Systems Management (discussed below), there is a fundamental concern about bypassing the inherent capabilities of the underlying NT operating system. NT has strong, well-known, well-understood and documented file level security that is allied to detailed auditing capabilities. These facilities and capabilities have passed a formal evaluation and thus have a high level of assurance in terms of their correct operation. Any alternative mechanism would, initially at least, be

POL00043744

viewed as a weakening of the security posture. There is a need to show that any alternative proposal provides equivalent levels of security to that provided by NT.

Considering the particular merits of the proposed approach, the following observations can be made:

- These objects are not auditable as other programs objects – this is of particular concern with regard to the DTDs', which can be viewed as having a security enforcing function.
- Digital signatures do not provide access control they only provide a validation and integrity check. Any process that has access to the Message Store can read (and execute?) these program objects. *(Note there is some capability to organise the Message Store in a hierarchical structure and the ability to place Access Control Lists on Objects, however the sufficiency, practicality and assurance of these controls has yet to be proven).*
- Further information is required on when the digital signature check is performed (i.e. when they are loaded or at every invocation?). If the check is performed at load time then further information is required on how the Message Store Object Cache is secured.
- Fundamentally, the proposed solution critically lacks a viable crypto architecture and infrastructure, for example:
  - Who is responsible and how are objects signed?
  - What algorithm is used, what strength?
  - What is the key change frequency?
  - How are Keys changed?
  - How is a Key compromise handled?
  - How are Keys revoked?
- Whilst a number of the above factors can be solved by agreements and/or procedural measures (e.g. who signs the objects), other aspects (e.g. key revocation) are significant technical issues for which WebRiposte does not provide the appropriate crypto infrastructure. If cryptographic mechanisms are to be applied in the manner proposed then we need a more fundamental understanding of the objectives to be achieved. For example, if we were to assume that, in the future, there will multiple and distinct web applications it may be logical to propose that each application should be in its own cryptographic domain; the supporting crypto infrastructure would then support this concept.

6.9.5 Validating the WebRiposte Environment

There is an explicit need for Pathway to validate not only NBS XML transactions but also elements of the WebRiposte environment; in particular, the DTDs' or any XML schemas'. The purpose of this exercise is not only to validate the correctness, in terms of application functionality, but also to gain assurance that there cannot be any malicious/deleterious impact on the rest of the Horizon activities from the NBS environment. In real terms this is almost impossible to achieve. In security terms we should be looking at the equivalent of DoD B-level or ITSEC E3/5 assurance. If reliance is to be placed on some of the security features of WebRiposte there might also be some value in requesting an independent evaluation by a CLEF (takes a long time and costs 'buckets' of money).

6.9.6 Software Distribution

It has been suggested that WebRiposte program objects (e.g. Java Objects, XML transaction definitions, Framework DTDs) – which Escher propose to hold in the

POL00043744

message store - should be distributed via Riposte as a form of Reference Data. Some "trigger" Reference Data, presumed to be time/date based, would control invocation of these program objects. This suggestion omits the functions of inventory and configuration management that are essential to control the Horizon estate – for which the necessary interfaces to the extant environment would need to be built - and focuses purely only on the delivery mechanism. Even at this level the suggestion is deficient in that facilities/capabilities for regression and assured, controlled delivery are not available. This subject is further discussed in the Section on System Management.

6.1.7 Conclusion

WebRiposte has some capabilities to implement separation of objects and provide access controls but further information is required on the scope, applicability and sufficiency of these controls; in addition further technical information is required in several areas.

At this moment it is not possible to determine whether WebRiposte has sufficient security mechanisms to meet the requirements of NBS and secure operation with Horizon.Further review will be necessary when the information required becomes available.

POL00043744

7 Systems Management, Software Maintenance & Distribution

7.1 Summary

ICL Pathway has developed an extensive Systems Management infrastructure to support the complexity and scale of the Horizon infrastructure. These facilities are built around the following toolkits:

- Tivoli Management Environment, used to provide overall management support and specific management of NT platforms
- BMC Patrol, used for specific management of Sequent Dynix platforms
- Maestro, used to provide workload scheduling on both Sequent and NT platforms
- HP OpenView, used for specific management of Cisco Routers

ICL Pathway has developed an extensive set of facilities on top of these standard products, particularly to support Software Distribution. These include:

- A Counter process control environment that supports the Software Distribution facilities
- Targeted and scheduled software distribution that exploits the capacity available on the ISDN network
- Inventory facilities that monitor the exact software state of each Counter in each Outlet and provide vital information to support staff
- Facilities to package software updates, including regression capabilities

These facilities are endorsed by [GENAPI], a Contract Controlled Document that defines the management and support environment for new Counter Applications.

ICL Pathway is concerned that the WebRiposte facilities developed by Escher do not fit within this Systems Management model, In our view, this would introduce two discrete software distribution mechanisms with incompatible sets of functionality. The Escher facilities do not support many of the features developed for Horizon for well researched support reasons and hence are, in our view, unable to be used to support the SLAs for Counter stability that are a contractual requirement on ICL Pathway.

There are two possible approaches to these concerns.

- Enhance Riposte so that it provides the full set of software distribution facilities believed necessary by ICL Pathway, including specific inventory, version control and regression
- Provide facilities for Riposte to load specific WebRiposte Objects from the Counter filestore.

The first is unacceptable to ICL Pathway as the Riposte tools can only manage software that forms part of the Riposte environment, whereas there are aspects of the Counter infrastructure, such as device drivers and NT Service Packs, that cannot be handled via Riposte.

ICL Pathway raised this issue with Escher during the discussions on the Network Banking Browser - Proof of Concept in mid 2000, and received written confirmation from Escher that they would enhance the WebRiposte facilities to enable web applications to be distributed via the Counter filestore, and loaded from filestore without subsequent replication via the Message Store. This is recorded in [PoC]. Facilities already exist in Riposte to load Persistent Objects from filestore locations.

7.2 Horizon Systems Management

POL00043744

This Section records the current operation of the Horizon Systems Management facilities.

7.2.1 The Horizon Systems Management Toolset

ICL Pathway has developed an extensive Systems Management infrastructure to support the complexity and scale of the Horizon infrastructure. These facilities are built around the following toolkits:

7.2.1.1 Tivoli Management Environment (TME)

Tivoli Management Environment is used to provide enterprise level management support of all domains, and specific management of NT platforms. Each managed platform includes a Tivoli client that supports event management and software distribution facilities. In addition, the Counter platforms contain Tivoli remote management facilities that are provided for use by support staff. Within the Campuses, a set of NT and Solaris platforms is used to provide management facilities including software distribution and event aggregation, processing and display functions.

Tivoli was chosen to fulfil this task as it demonstrated the ability to handle 40,000 end points, and can operate properly given the distributed nature of the solution and the fact that Outlets are not always in communication with the Campuses.

7.2.1.2 BMC Patrol

This is the primary tool used for management of Sequent Dynix platforms. It uses a set of Knowledge Modules, some standard and some bespoke for the particular applications that run on these platforms. Events that cannot be handled by BMC Patrol are fed into the enterprise level Tivoli Management system.

7.2.1.3 Maestro

Batch scheduling of processes on both NT and Dynix platforms is provided by Maestro (now known as Tivoli Workload Scheduler).

7.2.1.4 HP OpenView

This is used by Network Management staff for specific management of Cisco Routers and other network kit.

7.2.1.5 Time Synchronisation

This is a significant part of the Systems Management facilities, not least because:

- Times at which a particular event occurred can be significant, for audit purposes or for conformance to (for example) the banks' End of Day processing deadlines
- SLA calculations are impossible unless there is a high degree of co-ordination of the clocks on various platforms.

Time synchronisation within the Campuses is provided by the NTP protocol using GPS satellites as the time source

Time synchronisation of Counters in Outlets is carried out by the Correspondence Servers each time the Outlet connects to the Campus.

7.2.2 Horizon Systems Management Developments

An extensive set of bespoke facilities have been developed on top of these standard products, particularly to support Software Distribution. These include the following.

7.2.2.1 Software Inventory

POL00043744

A Web enabled repository (using Oracle) has been developed that records:

- Events from all platforms
- Details of all Outlets and Counters
- Software inventory for each Counter (and Campus platforms)
- Details for automated estate management (roll out and steady state)
- Details of all Campus platforms (and remote FTMS platforms)

7.2.2.2 Software Distribution

Software Distribution facilities run off this repository and exploit the capacity available on the ISDN network to do network sympathetic scheduling and targeting of software distribution to Outlets

Software is distributed in the form of a "package" that includes installation scripts and regression capabilities. These scripts are developed individually for each distributed package. Software can be digitally signed, and the signature checked when it is loaded.

These facilities are endorsed by [GENAPI], a Contract Controlled Document that defines the management and support environment for new Counter Applications.

7.2.2.3 Auto Configuration

Counter PCs are delivered to Outlets in a "vanilla" state. This applies both to new installations during the National Roll-out of Horizon, and to Counters installed as spares to replace faulty units. Once installed, a Counter undergoes an "auto configuration" process, whereby it communicates with a server within the Campus that provides it with its identity and delivers the latest software state to it.

This process will need to be enhanced to configure aspects of the Web Riposte Desktop on replacement Counters

7.2.2.4 Counter Process Control

A Counter process control environment is provided that supports the desktop management and Software Distribution facilities. One or more of the Web Riposte Desktop components operate as NT Services. Within the Counter architecture, these services are initiated explicitly by the Process Control function that is run each morning at 03:00.

The Process Control function would need to be enhanced to cater for the additional NT service required by WebRiposte.

7.3 Systems Management and Network Banking

This Chapter discusses the likely impact on the Systems Management facilities of the introduction of the Network Banking Service into Horizon. The principal cause of any such change is the requirement to support this service as a web enabled application within the Counter, supported by Escher's WebRiposte facilities.

Any successfully managed system will require the Systems Management product set to closely track the operational footprint of the applications. This task is significantly eased if guidance is provided to application suppliers on the operational footprint of their applications. Various Pathway documents provide this guidance, including the following

- [HADDIS] for Host platforms
- [GENAPI] for Counter applications

7.3.1 Management of Counters

POL00043744

7.3.1.1 Counter Application Architecture

The emerging NBS solution includes:

- WebRiposte, which includes an enhanced Riposte Message Server supporting XML messaging and other facilities
- A new application development component, currently known as the *WebRiposte Framework*, needed to support the NB Counter Application
- The Network Banking transaction code, possibly supplied by a third party.

These will thus present new objects for the Systems Management facilities to manage, including DTD, XML and Java objects. These object types are used to construct the application code mentioned above. Each of these is discussed below but to set the context it is worth restating some of the compliance statements in [GENAPI].

7.3.1.2 Event management

Applications must:

- Use the NT application event log. The security log may be used but this requires NT privileges and is therefore deprecated at the application level
- Identify all sub-sources used
- Document major events and suggested recovery actions
- Ensure correct usage of NT event types (i.e. errors, warnings, information).
- Document those events that are security related or security enforcing. (i.e. that affect or are reporting on the security integrity of the application and platform)
- Give some indication of event volumes in normal running
- Avoid floods of events through duplicates. The applications should treat these as inherent application state changes and fall back to periodic error reporting on the state

In general, existing desktop applications don't generate much in the way of events. Some generate separate diagnostic logs. It is not yet clear to ICL Pathway what trace and/or diagnostic features are provided by the WebRiposte Development Framework.

However, because of the potential mix of ICL Pathway and third party Application code at the Counter, and ICL Pathway's likely liabilities for fraud, misuse and SLAs, it is necessary that WebRiposte and the NBCA provide sufficient trace and diagnostic tools to identify the source of errors and problems.

7.3.1.3 Process Control

Applications must:

- If they are standalone processes outside the desk top then:
  - Document how they may be safely started and stopped. This may be API or documentation of the location of the specific executables to be invoked. If an API is provided then it must be synchronous and atomic (i.e. only return when all or no processes are started /stopped)
  - Document any dependencies to other processes/NT services that may affect their successful start up or shut down
  - Document whether they can be (safely) automatically restarted on failure
- If they are implemented as NT services then:
  - Document all service names used
  - Document any dependencies on other processes or NT services that may affect their successful start up or shut down
  - Document whether they can be (safely) automatically restarted on failure

POL00043744

It is assumed at present that none of this is applicable, since the WebRiposte application will run as part of the existing Desktop process. However, there may be an additional "WebRiposteAppServer" NT service introduced as part of WebRiposte.

Again, because of the potential mix of ICL Pathway and third party code on the Counters, it is necessary to be more proscriptive about the integration of new applications within the Counter. There is a need for standards that cover:

- Services with separate service accounts (where applicable)
- Separate filestore directories for new applications
- Start-up and shut-down processes
- Process "health check" APIs that can be used to monitor process hang-ups

7.3.1.4 Co*n*figuration

For any configuration data not held in the Riposte Message Store, applications must:

- Document any generic configurations, the APIs for setting the parameters and the underlying footprint on the NT registry (if used as the repository for these parameters). Applications must not modify the registry other than through such APIs.
- Document when changes to these parameters take effect. This must either be when the parameters are updated or by invoking another API. The necessity to restart the (Counter) application at that point is strongly deprecated, though may be unavoidable in some cases and where the changes can reasonably come into effect the next day, the application can assume the impact of the 03:00 desktop reload.
- Document any dependencies on the configuration of other applications/NT subsystems and indicate the synchronisation of these dependencies
- All the above clauses equally apply to Counter specific configuration items

7.3.1.5 Software Distribution

Applications must be delivered to ICL Pathway with documentation such that they can be installed and regressed in unattended mode, provide some persistent signature as to their existence and co-exist with the target platform environment.

All fixes to applications must be provided as deltas, with associated documentation to indicate how to apply and activate the fix. They must not require attended operation to be installed or regressed.

In this sense, a "delta" is an addition, deletion or replacement of complete files, or specific and regressible changes to the Registry invoked via an appropriate API from in installation script. The Software Distribution facilities do not provide any mechanisms to change the internal content of files.

ICL Pathway notes that Java introduces the concept of having Jars containing many pieces of Java code. Thus, if there is any requirement to add, delete or replace these individual components, it may be necessary to investigate further the granularity of control.

7.3.1.6 Error Handling, Diagnosability and Continuous Operation

All Counters are remotely managed and have no onsite IT experienced support. They are required to be continuously available

The NBS application design needs to be aware of this and obey engineering principles to support this environment. These principles include:

- They must never silently fail

POL00043744

- Provide diagnostic facilities that can be remotely managed. A suggested model is:
  - Provide an API to switch on/off specific diagnostics. Such changes shall be immediately actioned by the application, or a separate API may be provided to make the application recognise the new values. Applications must not need to be restarted to turn diagnostics on or off
  - These diagnostics should include the capability to all procedure entry and exit points, including called parameters and exit values (including success/failure indications)
  - Event driven code (e.g. peripheral events) should be able to log all events received, with any parameters.
  - Such diagnostics shall go to one or more diagnostic files. All files (whether disk or memory resident) must be cyclic
  - The diagnostic files shall be English text format or, if encoded in other ways (e.g. binary, language locales) then there must be facilities to transform the data to English text format at source
  - A minimum level of tracing should be turned on at all times
- Applications must never rely on an operating system reboot or application restart to free dynamic resources such as memory, semaphores or temporary disk storage
- Applications must successfully manage transitions across time changes such as in BST. At the least, their behaviour shall be documented in conditions where the time changes (e.g. if the application relies on any time based recovery) and they must never fail
- Applications that change the time should be configurable to post a Time Change message
- In general, applications should work in UCT. Local time should only be used for display purposes.
- Applications must provide recovery from all conditions. Ideally, this is always automated but if not then documentation is provided to describe the recovery action. Recovery conditions must cover an uncontrolled system shut down (e.g. power loss) and therefore an application must design out (or minimise) exposure to critical sections in the code
- Faults, if they occur, should be reported through the NT event log, though care needs to be given to the number and frequency of events that are raised in this way. In addition, Tivoli generates an ISDN call for every Error Event sent to the Campus, and thus Event Storms can cause network meltdown and impair ICL Pathway's ability to support other systems.

7.3.1.7 Code Verification

To mitigate the risks to the stability of the Horizon platform associated with introducing third party software onto the Counter, a strict regime of software proving is suggested, including:

- Design reviews
- Code inspections (therefore access to the source)
- Thorough testing, concentrating on performance, reliability and migration issues
- Limited initial rollout (say 100 Counters) with a bedding-in period where Counter performance and reliability SLAs do not apply. This would enable ICL Pathway to review the application's use of Events in "live" use
- It should be possible to disable any such software by Reference Data in the event of failures that affect other applications.

Note that this militates against rapid functionality. roll-out, and is absolutely necessary for the introduction of radical changes such as the introduction of WebRiposte or the

POL00043744

first web-enabled application. However, careful design of this application should ensure that subsequent data-only changes (for example to add new banks) can be effected via changes to Reference Data, in the same way as EPOSS is an application but details of the products to be sold are Reference Data.

7.3.1.8 New Counter Components

7.3.1.8.1 Web Riposte

Any new Riposte deliveries are expected to comply with these requirements. It should be noted that existing Riposte versions have never met many of these standards, though the mixed application environment likely to arise with Network Banking makes it much more important that future Riposte versions do comply with them. It is only through continued adherence to these standards that ICL Pathway can continue to support contractual liabilities in terms of Counter stability and SLAs

Note that the pre-requisites for the NT run time environment will have implication on the Tivoli product support. ICL Pathway will need an exact statement from Escher on all run time NT requirements, including NT Service Pack levels

7.3.1.8.2 New Software Objects

Escher's declared position is that the objects new object types (DTD, XML, Java objects):

- Are distributed by message replication
- Are digitally signed, and such signature is checked when the code is loaded
- Are executed from the message store
- Any XML includes tight coupling with the versions of the Java objects it uses

From a Systems Management perspective, this raises many issues. This Document is not the appropriate place to debate the whole question but it is worth making some observations and then recommending a System Management position

First some observations.

- There is an argument that the DTD, XML and Java objects are software components, and hence should be handled by the same mechanisms as other Counter code
- The distribution and inventory paradigms between software delivery and Riposte replication provide significantly different Quality of Service (QOS)
- Riposte offers no confirmed delivery, no software inventory, freewheeling scheduling, and regression has to be performed by re-delivery of the original "code". Riposte does, though, offer a highly resilient delivery service. Objects are replicated to all nodes in a group, and this means that regression is very complicated, though somewhat eased by the concept of "trigger objects", where regression can be achieved be replacing the new trigger with the old trigger
- The Class D mechanisms currently used to distribute Reference Data cannot handle the requirements for scheduled software distribution. For example, they do not handle "BLOBs" and would thus need to be enhanced to handle WebRiposte Objects or Subscription Groups.
- Enhancements to Riposte would be required to provide acceptable solutions to these issues. In addition, if the Horizon system moves to use Subscription Groups to reduce the amount of data held in Correspondence Servers, then further changes would be required to this function. Escher are aware of ICL Pathway's requirements in this area.

POL00043744

- Tivoli offers a Counter level software inventory; network sympathetic scheduling, and Outlet targeting that is only constrained by SQL Select statements on its Oracle database. All work is synchronous, and regression capabilities are provided as part of the installation scripts. Tivoli uses peer-to-peer synchronous protocols. This inventory is specified by the Codified Agreement [G01-032/S477]. There are no equivalent facilities in Riposte at present to register the versions of software delivered via Reference Data.
- ICL Pathway has developed an Oracle database (RDMC) to hold Reference Data, and an accompanying database (RDDS) to distribute it
- ICL Pathway has developed some elements of a confirmed delivery service layered over Riposte replication, to satisfy SLAs. It does not report back to the RDMC, so there is no end to end service
- ICL Pathway has developed distribution processes that include "wrapping" the package for ease of installation and to provide a regression capability. No such facilities are provided by Riposte
- The DTD, XML and Java objects are digitally signed and this is checked when they are accessed. Note that the keys are not integrated with KMS
- Regardless of any enhancements made by Escher to the Riposte facilities, these facilities can only handle the distribution of components of the Counter application layer. Other desktop components, including Riposte itself, drivers and NT Service Packs, or indeed any change that requires a Counter reboot, will continue to need the Tivoli software distribution facilities. It is not sensible to use two different software distribution paradigms, however much they can be made to provide similar facility levels
- The Tivoli mechanisms and surrounding software facilities are tailored to schedule software download and activation in a way that avoids impacting on "normal business".
- They also provide the facility to target specific Outlets for new software version. This has been used extensively over the past year, for example to run Live Trials of new software in selected Outlets, or to pilot new Eicon drivers. Riposte Reference Data distribution lacks this close degree of control

The ICL Pathway System Management recommendation is as follows.

- Escher provide an option whereby DTD, XML and Java objects can be executed from NT filestore (and this includes checking the digital signature also held in filestore). This was promised during the *Network Banking Browser - Proof of Concept* study carried out in mid 2000, as recorded in [PoC].
- ICL Pathway will support updates of DTD, XML and Java objects purely via Tivoli, into the Counter filestore, using the existing mechanisms. Riposte provides mechanisms to load messages from designated filestore areas, and to carry out load time digital signature checking
- ICL Pathway will review the whole area of Riposte signing and KMS integration. Currently, for example, there is no way to revoke Escher public keys should they be compromised. Some implications of this are given below.

7.3.1.8.3 Software Signing

Software is digitally signed in ICL Pathway's Feltham headquarters before it is issued, and the signature is checked before the software is run.

POL00043744

With WebRiposte, a web-based feed to a browser running within the Counter could possiblycontain:

- Executables such as Applets, JavaScripts and so on.
- Presentation objects such as .IMG or .JPG files.
- Text such as form field content or display messages

It would be necessary to ensure that executable objects came from an accredited source and were correct in their operation. This is particularly the case if they write to the Riposte Message Store. Any such applets would require extensive validation within ICL Pathway before they were distributed.

Once validated, WebRiposte requires that they are digitally signed before they are distributed to (or, at least, are loaded on) the Counter. Unsigned objects, or those that fail signature verification, will not load. This can be used to ensure that what is used at the Counter is what has been tested, and that it has not been tampered with subsequently. However, it does mean that ICL Pathway will need to develop a process for managing the signing of these objects. At present, the only signed executables on the Counter are those delivered by Escher, and these are signed under Escher's Pubic/Private key. Riposte has an in-built key that is used to sign other Keys, and Escher can provide third parties such as ICL Pathway with a signing Key. However, there are no subsequent mechanisms to manage these Keys, or to change them if they expire or become compromised. ICL Pathway has developed extensive facilities for Key management, and it will be necessary to include these in any new Software Signing processes, with a possible requirement to modify the Escher deliverables.

Escher use the Microsoft Crypto Architecture for software signing. This covers key formats, algorithms etc. If this is to change to use the SI Keys provided by KMS, then ICL Pathway will need to provide a Service Provider module for the DSA algorithm. In addition, there are service pack dependencies

7.3.1.9 Counter Migration

The introduction of the WebRiposte Desktop will require a Counter upgrade that includes a migration from IE4 to IE5, to support the software baseline required by WebRiposte. In addition, early indications are that the NT Service Pack used on the Counters platforms (currently SP3) will need to be upgraded to SP5 or later to support WebRiposte. The ensuing Counter upgrade is likely to be nearly as complex as the Counter CSR+ migration, and the migration process itself will need serious testing (to destruction, as recommended for CSR+). Note that the current IE4 implementation is a "cut down" version and moving away from this may present its own difficulties.

7.3.2 Management of the Network Banking Engine (NBE)

This sub-Section assumes that the NBE is located on ICL premises and is managed by ICL Pathway.

The following observations can be made.

7.3.2.1 Base build

There is a well-defined set of processes by which a Platform is introduced into the Horizon solution. This includes processes that:

a) Specify base hardware

b) Specify base OS (and repair level)

c) Specify live configurations for (a) and (b)

d) Specify optional layered OS products

POL00043744

e) Specify live configuration for (d)

f) Develop and test scripts to automate the deployment of (a) through (e)

Within ICL Pathway there are existing processes and owning units for most of these activities (although (c) and (e) are still subject to some debate). However, there are no IBM skills.

For the NBE it would have to be very clearly defined who owns each of these activities. For example, whether it is Pathway (and if so which unit) or IBM (and if so what standards do they use for documenting the handover).

7.3.2.2 Application Handover

The application is clearly supplied by IBM but standards would have to be agreed by which they handover base versions and operational fixes to Pathway.

After the handover, the NBS Counter Application would be treated within ICL Pathway as any other application, and in particular be incorporated within the Release management process. The most efficient way to do this is to appoint a proxy delivery unit for the NBE application. This unit will act as the IBM interface into Pathway, and handle the PVCS and Release management processes.

7.3.2.3 System Management Products

Strategically, ICL Pathway would approach these as follows.

7.3.2.3.1 NBE Platform

This would be a new management domain. ICL Pathway would choose tools that could be integrated into the existing Enterprise Domain (i.e. Tivoli) but also domain specific tools where they are superior to the enterprise tool set or reuse existing skill sets in the ISD group who manage the NBE. We are in receipt of a suggested set of System management products from IBM but they do not cover all strategic possibilities and also clash with existing Pathway solutions (for example Tivoli NetView has more affinity with HP OpenView (on which it is based) than any classical Tivoli product). These tools also do not cover Software Distribution and Time Synchronisation services.

The fundamental point is that if ICL Pathway is to manage the NBE, then ICL Pathway must decide the tools to be used, though clearly in co-operation with IBM.

It is recommended that a Technical Working Group is established at the appropriate time, with ICL Pathway, ICL ISD and IBM members, to move this forward. The scope of this Working Group would also include identifying the integration of the applications and OS/360 with the chosen system management product set.

ICL Pathway can start this activity at any time, but this level of detail appears beyond the scope of the current Work Package

The specific choice of system products are therefore not developed further in this document.

7.3.2.3.1.1.1 NBE Managed Service Operator

Any service provided by ICL Pathway to manage the NBE will be integrated into the overall Horizon management and operational environment.

7.3.2.3.2 NBE Specific Network Components

POL00043744

The NBE access to the Banks will clearly imply new network equipment on the ICL premises. It is not yet clear what that might be, but the strategy would be to expand the existing use of HP OpenView.

7.3.2.3.3 Reference Data

Figure 1 shows the need to distribute Reference Data to the NBE. However, there is no documented visibility of the semantics of the data, other than that it will, at minimum, contain data to route (and format) Counter transactions to the appropriate bank.

The diagram shows this data being passed by POCL directly to the NBE, with no ICL Pathway involvement. POCL would thus be responsible for co-ordinating the data feeds to ICL Pathway and to the NBE from their RDS (which already feeds RDMC and other POCL systems).

If the NBE is to be located outside the ICL Pathway Campuses, then that is an appropriate approach. However, should it be co-located with the Campuses, then it is worth considering an alternative. It is technically feasible to deliver Reference Data to the NBE via the ICL Pathway RDMC, and in a single management and operational environment there are significant benefits to using the RDMC to manage the data feed to the NBE. The RDMC already provides a data feed to Tivoli of the data that is needed by the support community.

- If the data feed goes via RDMC, this will need to be enhanced for the new feed.
- If the data feed goes direct to the NBE, then the only involvement is in setting up and managing the communications channel.

7.3.3 Management of Other Existing Platforms

This Section discusses the impact of Network Banking on existing Pathway platforms (other than Counters), and new or changed applications on them.

7.3.3.1 Host Central Servers

Any development on the Host Central Server (for example to support Reconciliation and Settlement) will follow the standards in [HADDIS]. Alerts will be handled by Patrol. Where they are security related, or they are operationally significant at the enterprise level, then they are also routed to Tivoli

Software distribution will follow normal Release management process.

7.3.3.2 Agent Servers

These will follow the existing management standards for Agent systems. Currently, Agent recovery uses Tivoli event forwarding as a transport mechanism. The on-line messaging requirements of Network Banking may require a switch to a synchronous protocol to provide the QoS required for Agent recovery where on line transaction is involved. This is a topic for the Resilience topic area.

7.3.4 Network

The network requirements for Network Banking are strikingly different from the current solution. How this is met will have implications on:

- Management and monitoring of the network. This is part of the network topic, but whatever is developed should retain a gateway capability to Tivoli
- The impact of the delivered QoS on the Software distribution and eventing solutions.

7.3.5 System Management Platforms

POL00043744

Given that Network Banking does not change the size of the Counter estate, then intrinsically there is no requirement for increasing the number or capacity of the Systems Management platforms. However, if we need to update the Tivoli product (for example as a result of the Web Riposte run time environment) then there may be a requirement for a few interim migration platforms to assist dual management strategies as we swing each managed node onto new client and management software. This is also covered elsewhere under technology refresh, but Network banking may be the catalyst for it.

POL00043744

8 Help Desk

This is covered in the ICL Pathway document CR/SPE/032 "Network Banking HelpDesk Options and Requirements".

POL00043744

9 Extensions to basic service / requirements

This is covered in ICL Pathway's response to WP9:

CR/REP/030 "Extension of Network Banking to cover Universal Banking"

CR/REP/031 "Network Banking WP9 – Report on extensions to cover EFTPOS"

POL00043744

10 Observations on Other Work Packages

Commentary on other work package in which ICL has been involved but is not responsible for producing the output.

10.1 Transaction flows (Work Package 1)

•

This is covered in ICL Pathway's response to WP1:

CR/SPE/028 "Network Banking – Transaction States and Data Flows"

10.2 Reconciliation (Work Package 5)

- WP has identified an architectural need for for client settlement which is not currently addressed
- Settlement & recon needs to be part of initial delivery
- Recon best place with ICL / Horizon development and operation services

10.3 ICL contract (Work Package 10)

- Need for single source of requirements which is referenced by the contract
- Acceptance against requirements spec
- SLAs need far greater clarity where service involves 3rd party s/w
- 3rd parties s/w suppliers must acceptance similar liabilities to Pathway (and hence provide similar support levels)

POL00043744

11 ICL Programme of Work

11.1 Outline Programme Plan

This is documented within the Level 1 plan which is currently under discussion.

11.2 Major Planning Assumptions

- The order of releases is
  - S3,S6,S10
  - Initial Infrastructure Release-1A
  - Pilot NWB-limited to 300 outlets
  - Infrastructure Release 1B
  - NWB Rollout

- NWB Pilot is full release ie robust and capable of rapid rollout
- Upgrade of Riposte will be required to enable Web objects to be retrieved from filestore
- No quantitative assumptions have been made re volumetrics
- NWB transactions will be signed
- NBE's will be remote
- There will be a move to a third data centre
- There will be a requirement for additional processing power at the data centre for reconciliation
- Reconciliation will be required for the pilot
- Riposte subscriber groups will be required
- No exploitation of SP5
- Support tools will be upgraded
- Existing applications do not need to change
- New versions of Tivoli can be laid down in parallel
- Rollout reference data can be available and distributed in advance of the application
- 8 weeks required for the migration
- Unix and NT boxes as 2 separate slots in data centre migration
- Work will be initiated to move VC6,VB6 into S10
- New version of Riposte will be backward compatible
- 3rd party bug fixes received in required timescales
- Test Application produced in-house
- Eschers close involvement from 5 Feb
- Network enhancements does not involve hardware visits to outlets
- Each campus connects to 2 MBE sites

POL00043744

- Service boundaries: Pathway Data Centre,Link gateway on NBE site
- EPOSS will change
- A method will exist to co-ordinate Pathway ref data with MBE ref data
- Pathway to supply training counter, not training documentation

11.3 Dependencies

- New Tivoli on live before upgrade to Main Infrastructure release 1B
- PO to ensure end to end signing paradigm implemented by all suppliers in E2E chain
- Completion of counter security review
- Test network is representative of new network before counter system test
- Network system specification documents available from PON. Also Interface strategy,AIS,TIS

POL00043744

12 Next Steps

The next step is a meeting with POCL to review this document and to decide on the next scoped level of work.

POL00043744

13 APPENDIX 1 -SECURITY DOMAIN ASSERTIONS

13.1 Bank(s) Domain

Whilst each Bank is a separate entity, and hence a separate Domain, for the purposes of this paper they are collectively viewed as a single Domain, with a generic set of security assertions, that will interact with the NBE. Schematically this is shown in **Error! Reference source not found.**. For any individual Bank, the general security assertions would need to be examined on a case-by-case basis and adjusted accordingly.

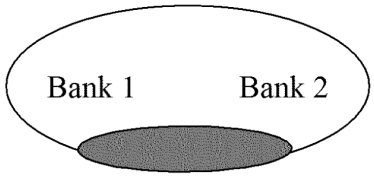


Figure 7 – Bank Domains

13.1.1 Assertions

- The Banking system(s) have an approved and authorised (BS7799 compliant?) Security Policy that defines the security posture, features, facilities and measures applied
- The implemented Banking Systems are compliant with the Bank(s) Security Policy
- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the security posture
- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the system and application environments
- Banking application systems will correctly process all NBS transactions and return valid responses to input requests
- Banking Systems will maintain the confidentiality of all NBS transaction within their Domain(s)
- Banking Systems ensure that there is no unauthorised or unlawful processing of NBS transactions
- Banking Systems will ensure that only authorised responses will be returned to NBS inputs
- Banking systems will maintain the integrity of all NBS transactions within their Domain(s)
- Banking Systems will ensure that all NBS transactions will only enter/leave their Domain through authorised ingress and egress points using agreed and approved communication, transfer and data protocols
- Banking Systems will ensure that no unauthorised connection or communication or communication protocol, to the NBE or Horizon, will originate from within their Domain

POL00043744

13.2 NBE Domain

The NBE is identified as a Domain in its own right. Although **Error! Reference source not found.** recommends that it is co-located with the ICL Pathway Campuses, to simplify the operation and management of the NBE, the security assertions are applicable in all scenarios. Schematically, the NBE Domain is as shown here.

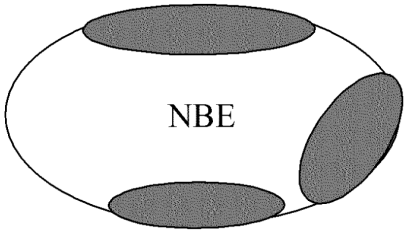


Figure 8 – NBE Domain

13.2.1 Assertions

- The NBE has an approved and authorised (BS7799 compliant?) Security Policy that defines the security posture, features, facilities and measures applied.
- The NBE Security Policy is approved and agreed with. POCL
- The implemented NBE is compliant with its own Security Policy
- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the security posture
- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the system and application environments
- NBE application systems will correctly process all NBS transactions
- NBE will maintain the confidentiality of all NBS transactions within its Domain
- NBE will ensure that there is that there is no unauthorised or unlawful processing of NBS transactions
- NBE will ensure that all valid NBS transactions received from Horizon will be passed to the Banks in a timely manner
- Where the NBE does not pass NBS transactions from Horizon to the Banks then the NBE will ensure that these transactions are only processed in an approved and authorised manner
- NBE will ensure that all valid NBS transactions received from Bank(s) will be passed to Horizon in a timely manner
- Where the NBE does not pass NBS transactions from the Banks to Horizon then the NBE will ensure that these transactions are only processed in an approved and authorised manner
- NBE systems will maintain the integrity of all NBS transactions within its domain
- NBE systems will ensure that all NBS transactions will only enter/leave its Domain through authorised ingress and egress points using agreed and approved communication, transfer and data protocols

POL00043744

- NBE will ensure that no unauthorised connection or communication or communication protocol, to the Bank(s) or Horizon will originate from their Domain
- NBE shall only retain data and/or information of NBS transactions that is approved and authorised (e.g. for audit and/or reconciliation purposes)
- NBS data and/or information retained by the NBE shall be stored in a secure manner that ensures its integrity and precludes unauthorised or unlawful processing
- NBE shall only record Reconciliation, Audit and MIS information of NBS transactions that is approved and authorised
- Reconciliation, Audit and MIS information recorded by the NBE shall accurately reflect NBS transactions processed by the NBE
- NBE shall only pass Reconciliation, Audit and MIS information to approved and authorised systems (POCL/Pathway)
- NBE shall preserve the integrity and confidentiality of all Reconciliation, Audit and MIS information within its Domain
- All users of the NBE will be Identified and Authenticated before access is granted to any of the system components, facilities and functions
- Any user of the NBE will only be granted access to system components, facilities and functions for which they are authorised

13.3 Horizon Domain

The Horizon system encompasses the Campus systems and Post Office Outlets Counter systems. This environment has been developed, and is operated, by ICL Pathway. The Horizon system is a separate Domain and is schematically shown as here.

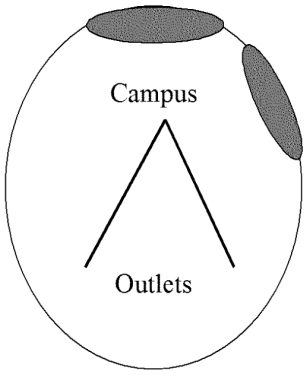


Figure 9 – Horizon Domain

13.3.1 Assertions

- Horizon has an approved and authorised (BS7799 compliant?) Security Policy that defines the security posture, features, facilities and measures applied
- The Horizon Security Policy is approved and agreed with POCL
- The implemented Horizon System is compliant with the Security Policy

POL00043744

- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the security posture
- Management, Technical and Procedural measures are implemented to ensure the integrity, maintenance and preservation of the system and application environments
- Horizon application systems will correctly process NBS transactions
- Horizon will maintain the confidentiality of NBS transactions
- Horizon will ensure that there is no unauthorised or unlawful processing of NBS transactions
- Horizon will ensure that all valid NBS transactions entered at a Counter will be passed to the NBE in a timely manner
- Where the Horizon does not pass NBS transactions from Horizon to the NBE then the Horizon will ensure that these transactions are only processed in an approved and authorised manner
- Horizon will ensure that all valid NBS transactions received from the NBE will be passed to the (originating) Counter in a timely manner
- Where the Horizon does not pass NBS transactions from the NBE to the (originating) Counter then Horizon will ensure that these transactions are only processed in an approved and authorised manner
- Horizon systems will maintain the integrity of all NBS transactions within its domain
- Horizon systems will ensure all NBS transactions will only enter/leave its Domain through authorised ingress and egress points using agreed and approved communication, transfer and data protocols
- Horizon will ensure that no unauthorised connection or communication or communication protocol, to the NBE will originate from its Domain
- Horizon shall only retain data and/or information of NBS transactions that is approved and authorised (e.g. for audit and/or reconciliation purposes)
- NBS data and/or information retained by Horizon shall be stored in a secure manner that ensures its integrity and precludes unauthorised or unlawful processing
- Horizon shall only record Reconciliation, Audit and MIS information of NBS transactions that is approved and authorised
- Reconciliation, Audit and MIS information recorded by Horizon shall accurately reflect NBS transactions processed by the Horizon
- Horizon shall only pass Reconciliation, Audit and MIS information to approved and authorised systems (POCL/Pathway)
- Horizon shall preserve the integrity and confidentiality of all Reconciliation, Audit and MIS information within its Domain
- All users of the Horizon will be Identified and Authenticated before access is granted to any of the system components, facilities and functions
- Any user of the Horizon will only be granted access to system components, facilities and functions for which they are authorised

Note: if the NBS Counter Application is supplied by a third party then many of the above assertions cannot be met, as ICL Pathway could not be responsible for the third

POL00043744

party application. This raises significant questions as to how conformance is to be achieved, what evidence is required and who would accept responsibility and liability for these assertions.

13.4 Generic Inter-Connection Assertions

The requirements of Inter-connection security are broadly the same, irrespective of the parties involved or type of connection and can thus be addressed by a generic set of assertions. Consideration of a specific inter-connection will need to address each of the assertions, in turn, and identify either:

- How the assertion is to be satisfied, or
- State that the assertion is not required (together with supporting rationale), or
- State that the risk, without the assertion, is to be accepted.

13.4.1 Assertions

- The transmitting site can be identified and authenticated as an approved and authorised site for connection attempts
- The Originator (within an authorised site) can be identified and authenticated as an approved and authorised Source for the information
- The receiving site is an approved and authorised site for the receipt of information
- The Recipient (within an authorised site) can be identified and authenticated as an approved and authorised destination for the information
- All communications over the bearer network are protected against external attacks
- All exchanges can recover from communication and information transfer failure
- All exchanges have an assured delivery mechanism
- The integrity of the information is preserved between the Originator and the Recipient
- All connections between (authorised) entities will only permit authorised connections, communications and exchanges
- All connection points are protected against unauthorised connection attempts, communication protocols and exchanges
- The method/mechanism of Information transfer has a non-repudiation mechanism