FUJ00139162

Document Title:	Counter supportability requirements
Document Type:	Requirements
Release:	N/A
Abstract:	This document examines the supportability issues within Pathway in the context of counter-related activities. It provides an overview of the current third line support processes and defines the supportability requirements for third and second line support.
Document Status:	DRAFT
Originator & Dept:	Kath Greenwood and Peter Boyd, TDA
Contributors:	Glenn Stephens, Mik Peach
Reviewed By:	Glenn Stephens, Mik Peach, Peter Burden, Cliff Wakeman, Patrick Carroll, Steve Parker, John Simpkins, Simon Fawkes, Allan Hodgkinson, Gareth Jenkins, Kristine Neiras, Peter Wiles, Brian Orzel, Mark Taylor, Geoffrey Vane, Peter Robinson, James Stinchcombe
Comments By:	
Comments To:	Pathway Document Controller and Originator
Distribution:	ICL Pathway Document Management, Glenn Stephens, Mik Peach, Peter Burden, Cliff Wakeman, Patrick Carroll, Steve Parker, John Simpkins, Simon Fawkes, Allan Hodgkinson, Gareth Jenkins, Kristine Neiras, Peter Wiles, Brian Orzel, Mark Taylor, Geoffrey Vane, Peter Robinson, James Stinchcombe

FUJ00139162

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	26-Mar-2001	First draft	
0.2	17-May-2001	Second Draft	

0.2 Approval Authorities

Name	Position	Signature	Date

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001			ICL Pathway Document Template	PVCS
DE/PRO/003 {DEPRO3}			ICL Pathway Development Directorate Processes	PVCS
Wish list		20 Nov 2000	Supportability Wish list	e_mail from Mik Peach
RS/FSP/001 {SFS}			System Functional Specification	PVCS
RS/POL/003 {ACP}			Access Control Policy	PVCS
CS/QMS/004 {CSQMS004}			CS Support Services Operations Manual	PVCS
TD/STD/004 {GENAPI}			Generalised API for OPS/TMS	PVCS
CSCP280			Changing counter background colour	

FUJ00139162

CP2775			Formal Introduction of the "Wing" correspondence servers	PVCS

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

0.4 Abbreviations/Definitions

Abbreviation	Definition
CP	Change Proposal
FAD	Reference number by which post office is known within Pathway.
FSM	Field Service Manager. Liaises between postmaster and Pathway support.
HSH	Horizon System Helpdesk (first and second line support for counter problems)
KEL	Known Error Log
MCO	Multiple counter outlet
OTT	Operational Test Team
PMS	Performance Monitoring System. Metron Athene software which is being deployed throughout the live estate.
RM	Release Management
SCO	Single counter outlet
SSC	Software Support Centre (provides third line Pathway support)
WI	Work Instruction
WP	Work Package

0.5 Changes in this Version

Version	Changes
0.1	None.
0.2	Updates resulting from comments on version 0.1 Requirements renumbered to differentiate between counter-specific (prefixed CR) and generic supportability (pre-fixed SR). Diagnostic Tracing has been moved to a separate section, 4.2 such

FUJ00139162

	that subsequent sections have been renumbered. Section 4.11 – Diagnostician access to counters has now been amended to include access to message store data and expanded to include short term and longer term requirements. Section 5 – Documentation Requirements has been added. Appendix 1 – Process for handling sensitive data has been added.

FUJ00139162

0.6 Changes Expected

Changes
1. As the Pathway solution evolves to include new areas e.g. Network Banking, GGP, Web Riposte this document will be updated.
2. Following discussions with SMC, it is envisaged that further requirements for second line support will be added.
3. Section 4.8 Connectivity will be expanded when further analysis work has been completed.

FUJ00139162

0.7 Table of Contents

FUJ00139162

FUJ00139162

1.0 Introduction

1.1 Summary

This document provides a brief description of the roles of each level of support and provides an overview of the current third line Pathway support process. Following on from that it defines the requirements to improve the supportability when handling counter-related problems. The requirements are primarily aimed at improving the effectiveness and efficiency of third line support. In order to realise these improvements, it is necessary to provide better tools for use by third line support; it is also necessary to extend the tools available for use by second line support and to improve the standards for diagnostics in the applications.

1.2 Background

As the Pathway solution has evolved, certain aspects of supportability have evolved in a rather ad hoc manner. As a result, a number of activities performed by third line support are repetitive, requiring low skill levels; diagnosing problems in some areas is difficult and searching for relevant documentation can be time-consuming.

The roles currently in operation by third and second line support are not as technical as defined in {CSQMS004}.

The route and mechanism for access to counters is another area which requires review. This is currently achieved via command line interface tools so is both cumbersome to use and lacking in auditability.

Various wish lists and suggestions have been produced in the past in an attempt to improve the supportability within the Pathway project. Previously there has been insufficient TDA resource to underpin the necessary changes. This resource has now been specifically allocated.

1.3 Terminology

Application log file	Any log file written by counter desktop applications; currently includes audit.log and PSStandard.log files.
Balance Report	Functionality requested by the postmaster e.g. from the “reports” or “Stock Balancing” menus on the counter.
Blue screen	Term widely used as synonymous with NT system crash. May be referred to elsewhere as BSOD or Blue Screen Of Death.
Counter	Live post office counter (gateway or slave)

FUJ00139162

Counter application	Any application process running on a post office Counter. Unless otherwise specified, requirements apply to any counter application.
Counter process set	List of processes which should be running on a counter to support PO business
counter profile	Specification of which data and software set is present on a counter at a given release/version/fix level
counter service set	List of services which should be running on a counter to support PO business
Counter support toolset	Formal support tools to be produced as identified in this document
Diagnostician	Anyone fulfilling a second or third line support role.
Identification of Requirements	Throughout the document requirements are identified as either applying specifically to counters (CRn.mmm) or being a generic supportability requirement (SRn.mmm) where n is the section number & mmm is a unique identifier starting from 1.
Office working hours	The hours when post office staff are running their business; it may extend beyond opening hours e.g. balancing on Wednesday.
Senior Diagnostician	Anyone fulfilling a third line support role
Sensitive Data	See Appendix 1 for a definition
Software Inventory	Definition of software on a counter - Baseline definition plus Tivoli packages.
Source Module	Any functional unit of source code.

FUJ00139162

2.0 Scope and aims

This document defines a set of requirements aimed at driving down support costs while improving the security and auditability of the diagnosticians' actions related to a counter.

One of the main aims of this document is to enable the second and third line support units to operate at their defined technical levels of support.

This document defines the requirements for the supportability improvements related to the diagnosis of counter problems.

It defines the requirements for methods and route of access to a live counter and also for tools and methods for retrieving, improving and interpreting diagnostic information.

It defines a toolset which is needed by third line support to diagnose a problem with the use of any counter applications and where necessary to apply the solution to a problem. This toolset will be provided in such a (role-based) way as to permit the devolvement of certain read-only tools/tasks to second line support.

It defines the requirements for improving the amount of diagnostic information written by counter applications.

Any general requirements for additional documentation, diagnostics etc. should become a Pathway de facto standard and should be adhered to in other parts of the programme e.g Network Banking, GGP. Such requirements will be articulated throughout the document (see 1.3 Identification of Requirements).

2.1 Context within the Pathway Project

This is the first phase of an initiative to address the supportability issues within the Pathway project. Additional phases will address supportability issues in the rest of the live estate.

2.2 Areas covered

The requirements are grouped under the following separate topics:

- Diagnostic data
  - log files
  - application tracing and diagnostics
- Business data
  - message store
- NT infrastructure
  - NT system
  - counter platform

FUJ00139162

  - counter file system
  - counter NT processes
- Support infrastructure
  - access route to counter
  - access route to message store data
- Health Status
  - NT
  - comms
  - application
- Tool production process

FUJ00139162

3.0 Current Support Activities

3.1 Overview

Before a support call for a counter problem arrives in third line support it has already been handled by first and second line at HSH/SMC. The call is taken from the postmaster, or FSM on behalf of the postmaster, by a member of the front line HSH help desk staff. The terminology used to describe the problem is naturally very business-oriented.

The call is then passed to second line support. This is also provided by HSH for counter problems. They consult the KEL, obtain any further information from the postmaster and if they suspect a software problem or the KEL indicates thus, the call is passed through to third line support. Currently second line support only have a limited toolset so are constrained to a fairly small set of support actions eg. they do not have access to message stores.

Within third line support, the call is initially updated by the call administrator for the addition of product, target release etc. then allocated to a diagnostician by the pre-scanner. In order to pursue the call, the diagnostician requires to access the live network to perform data collection, investigation and possibly to apply a corrective action to the problem.

Once diagnosis is complete (the call may or may not have been sent to fourth line), either the root cause of failure has been identified or the problem is unresolved. The call is then either sent back to second line support or to another support unit.

{CSQMS004} describes the roles of the different levels of support.

3.2 Third line support activities

3.2.1 Diagnosis Phase

- Understand/define the problem in technical terms
- Speak to postmaster for further details
- Search KEL/Raise KEL
- Obtain standard evidence from counter/correspondence server – message store, event, audit, PSStandard logs (performance, security issues)
- Produce/collect additional evidence from counter (performance, security issues)
- Reproduce problem on test rig - OTT or SSC counter (environmental issues)
- Import message store (security and environmental issues)
- Diagnose cause of problem (supportability, usability, security issues)
- Send call to fourth line support who perform additional in depth diagnosis using additional tools etc.

FUJ00139162

3.2.2 Implementation of Solution

3.2.2.1 Existing corrective action at counter

KELs/WIs document known corrective actions which include:

- Amend/add/delete file, configuration setting on counter
- Start/stop process running on counter

3.2.2.2 Existing corrective action at correspondence server

KELs/WIs document known corrective actions which include:

- Amend message store or other riposte data requiring write access for subsequent replication to counter.

3.2.2.3 New corrective action

On the first occurrence of a new problem, the diagnostician implements the change at counter or correspondence server and raises a KEL for future reference.

3.2.2.4 New application software fault

This involves a code change and subsequent release to the live estate which is the responsibility of fourth line support and is therefore outside the scope of this document.

3.2.3 Call Closure

The call is updated with details about the cause of the problem and solution. If a resolution has been found (by third or fourth line support), the closing support unit should ensure that the call includes accurate details of the failing product component for future statistical use. (SR3.1)

The closing support unit should also ensure that any reference numbers – CP, WP etc. are included on the call to enable the progress of the solution to live to be tracked and for reference purposes in the future. (SR3.2)

If fourth line support have been unable to resolve the problem with the evidence supplied, they should specify the additional evidence requirements. (SR3.3)

FUJ00139162

4.0 Requirements

4.1 Log files

4.1.1 Desktop application log files

The main desktop application log files currently used are the audit log (written by EPOSS) and PSStandard log (written by Escher peripheral server).

The former provides supplementary information relating to (back office printer) reports. It also includes the current EPOSS dll name and version information.

The latter provides supplementary information regarding interaction with peripherals – input (scanning/swiping) and output to the counter printer.

Unless otherwise stated, the term desktop application log file refers to any log file written by desktop applications; this currently includes audit log and PSStandard log file but is likely to be extended with the advent of Network Banking and web Riposte.

The key requirement is that information written by counter Desktop applications should be:

- common – all desktop application code should use a common audit log file for non-verbose diagnostic data. (CR4.1)
- appropriate - a separate diagnostic log file should be used for additional verbose or ad hoc diagnostic data. (see section 4.1.2)
- consistent – all desktop applications should write equivalent diagnostic messages to the appropriate log file, both on start up and run-time. (CR4.2)
- predictable – all application log files must reside in the same NT directory (CR4.3); names should have a common format. (CR4.4). The content of the file should not normally change between major software; if it does, the changes should be documented in a CP in order that the change can be impacted. (CR4.5).
- sufficient to diagnose the cause of all but the most complex of counter problems (at least 95% of problems passed to third line support) (CR4.6)
- unique – duplication of diagnostic information to multiple log files should be avoided. (CR4.6a)
- available instantly for urgent problems (CR4.6b)

4.1.1.1 Functionality of audit log file

There is a need to increase the present audit logging functionality to include all Balancing and report processing functions e.g. include Adjust Stock as well as actual printed reports. (CR4.7)

FUJ00139162

A diagnostic message must be written at the start and end of each Balancing and report processing activity initiated by a single key/button press (currently it is just the end of printed reports). (CR4.8)

Each diagnostic message should be time-stamped to the nearest microsecond and should include the originating source module name. (CR4.8a)

If a balance process or report production requires multiple key presses, then delimiting diagnostic messages must be written for each. (CR4.9)

For message store searches, the search criteria, number of records searched (low/high marks) and number selected should be logged. (CR4.10)

There should be a process which enables diagnosticians to input requests for changes to the logging of application-written messages. (SR4.10a)

{GENAPI} should be updated to include the standard for the content, introduction, review and deletion of application log messages via application code. (SR4.11)

4.1.1.2 Security

Sensitive data in application log files will be handled according to the rules in Appendix 1. (CR4.12)

4.1.1.3 Performance

The logging of diagnostic application messages must not incur performance overheads on the business application (CR4.13)

Retrieval of application log files must be non-intrusive on counter performance. (CR4.13a)

4.1.1.4 Usability

Diagnostic information in application log files should be self-documenting to reduce maintainability issues. (SR4.14) A web format support guide should provide further explanation. (SR4.15)

4.1.1.5 Configuration Management

Application log files will be automatically tidied after 4 weeks. (CR4.16)

They must be cyclic and/or have a maximum size limitation. (CR4.17) The appropriate design standards in {GENAPI} should specify details. (CR4.17a)

4.1.1.6 Availability

Application log files must always be available for inspection or retrieval. (CR4.18)

They must be retained over a counter swap. (CR4.21)

4.1.2 Support activity log

There is a need for a auditing of support activity on a counter. (CR4.50)

FUJ00139162

All read, write or update access at a counter by support must be recorded in an appropriate log file. Details logged must include username, computer name, FAD/counter name, timestamp, activity performed, error code returned. (CR4.51)

The file must reside in a location which prevents support users from modifying or deleting information (including the file itself). (CR4.52)

It is possible that the event log is the preferred file to avoid introducing additional files types.

4.1.2.1 Security

No sensitive data will be written. (CR4.53)

4.1.2.2 Performance

It must not affect the performance of the desktop applications. (CR4.54)

4.1.2.3 Usability

Any information written to the activity log must be self-explanatory. (CR4.55)

4.1.2.4 Configuration Management

The support activity log file will be cyclic; size configurable up to a maximum. (CR4.56)

Historical information must be available for at least one year. (CR4.56a)

4.1.2.5 Availability

It must always be available for inspection or retrieval. It must be retained over a counter swap. (CR4.21)

4.1.3 System (Event) Logs

This section refers to the NT event log. Events written here are picked up as real-time alerts.

The event log must be used by all counter applications to record important system events e.g. those which indicate a potential performance or hardware problem. (SR4.57)

The text of the event should include the originating source module. (SR4.57a)

To avoid obliterating important information in the event log, any information which indicates "normal running" should be written to an application log file instead of the event log (SR4.57b);

{GENAPI} should be updated to include the standard for content, introduction, review and deletion of event log messages via application code. (SR4.58)

4.1.3.1 Auditability

It must be possible to establish which source module and dll has written the event. (SR4.59)

FUJ00139162

4.1.3.2 Performance

Any detrimental effect caused by event storms should be minimised (e.g. such that the original failure event is lost by wrap-around). (SR4.60)

Retrieval of event logs must be non-intrusive at the counter. (CR4.61)

4.1.3.3 Usability

The meaning of application written events should be self-documenting to reduce maintainability issues. (SR4.14) A web format support guide should provide further explanation. (SR4.15)

Where the recovery action is not self-evident (e.g. not a "run out of disk space" type problem), it must be documented in a support guide. (SR4.62)

4.1.3.4 Configuration Management

The size of event log should be such that application events are available for at least the previous four weeks (SR4.63) and system events for at least one year (SR4.63a).

4.1.3.5 Availability

It must always be available for inspection or retrieval. It must be retained over a counter swap. (CR4.21)

4.1.4 Retrieval of Log Files

There is a set of common requirements regarding evidence file retrievals from counters. In addition all the requirements in section 4.10 apply.

- Automated support tools must be provided for predictable file retrievals (CR4.64)
- All desktop application log and diagnostic files must be retrievable via a support tool (CR4.64a)
- Retrieval must use existing systems management infrastructure (CR4.65)
- Tools must allow retrieval of multiple files/file types. (CR4.66)
- Tools must allow information to be filtered before retrieval i.e. partial file retrieval. (CR4.67)
- Tools must have compression facilities for large files (CR4.68)
- Retrieval tools must be available to second and third line support (CR4.69)
- It must be possible to retrieve evidence files from a counter while the application is running. (CR4.69a)
- It is of paramount importance that any retrieval tool does not impact the performance of the business application on the counter. (CR4.69b)

FUJ00139162

4.2 Diagnostic Tracing

Additional configurable diagnostic tracing, sufficient to find the root cause of any Pathway application problem, must be available for invocation on request by support. (SR4.20).

A standard approach is required for the design of diagnostics in all Pathway applications. A generic stand-alone tracing package written in an efficient language (e.g. C) should be written. It must have a well-documented interface such that it can be called efficiently from any Pathway application. (SR4.21)

All new Pathway applications must use the new trace package. Existing counter applications should be retro-fitted when they are the subject of a design change, or a PinICL or CP change.

The tracing information should be written to a cyclic log file. This file, which could be the event log as it satisfies these requirements, will be appended such that there is only one file per counter. (SR4.22). There should be a separate classification (in the event log) for diagnostic messages to enable them to be filtered in/out. (SR4.23)

The advantages of using the event log file are that the infrastructure to write and retrieve data already exists. It should be noted that all the event log requirements documented in section 4.1.3 must be satisfied as a pre-condition for use for tracing purposes. (SR4.24)

Tracing diagnostics must be configurable and controllable remotely by third line support staff by use of a tool. (SR4.25) The tool must allow tracing to be switched on or off and must allow the trace level to be set. (SR4.26)

A process must be defined for the running of tracing on a counter: (CR4.27)

- To specify that diagnostics must only be used on a live counter if the problem can not be reproduced on a test rig.
- To record that diagnostic tracing has been run.

Third line support must have access to a test rig where they can reproduce counter problems, switch on diagnostics and retrieve resultant evidence files to an SSC workstation. (CR4.28)

4.2.1 Functionality

Tracing must be configurable to enable different levels of tracing; the levels envisaged are none, minimum and full. (SR4.29)

Under normal running, tracing must be switched off. (SR4.30)

Trace points must be inserted on all interface points to third party software. (SR4.31) This is particularly important for network banking.

Trace points must be inserted on entry to and exit from each different sub-system including point of initial entry from user action and final exit point. (SR4.32)

The minimum requirement is for the source module name, trace point identifier, product or sub-system name and a time-stamp to be logged at each trace point. (SR4.33)

FUJ00139162

All time-stamps must be at the microsecond level of granularity. (SR4.34)

There must be a further (configurable) level of tracing which causes additional context or application specific data to be logged as specified by the Pathway application. (SR4.35)

Trace points may be inserted on entry to and exit from other key modules or at other pertinent points in the code as defined by the Pathway business application. (SR4.36)

It must be possible to start/stop tracing dynamically without needing to close down or recycle the application. (SR4.36a)

It is not envisaged that diagnostic tracing should change between major software releases. This should only occur where there is a business justification to solve a problem which can not be solved with the existing level of tracing. In this case, the changes must be documented in a CP in order that the change can be impacted. (SR4.37)

{GENAPI} should be updated to include the standard for the content, introduction, review and deletion of diagnostic tracing messages via application code. (SR4.38)

4.2.2 Performance

Additional diagnostics may cause performance overheads. The facility will only be used on a live counter when third line support have no other means of solving the problem. (SR4.39)

There may be levels of tracing which may only be exercised on a live counter by prior agreement with the postmaster. (CR4.40)

Performance measurements must be taken to measure the effect of running with maximum level diagnostics switched on (SR4.41)

Retrieval of diagnostic log files must be non-intrusive. (CR4.13)

4.2.3 Reliability

The diagnostic tracing and associated enabling tools will be developed according to {DEPRO3}. (SR4.42)

4.2.4 Supportability

The diagnostic tracing package must be written in structured way such that it will be easily maintained and enhanced. (SR4.43)

4.2.5 Usability

A support guide must be produced to document how to use the tools to configure and invoke the diagnostics. (CR4.44)

Diagnostic tracing should be self-documenting to reduce maintainability issues. (SR4.45) A web format support guide should provide further explanation of the meaning of the tracing output. (SR4.46)

FUJ00139162

4.2.6 Configuration Management

The file containing diagnostic tracing must be cyclic. The size must be configurable up to an agreed maximum. (CR4.47) The use of the event log for tracing must not conflict with the requirement to retain 4 weeks worth of event data. (CR4.48)

If necessary, the event log size will be increased prior to switching on diagnostics on a live counter. The process for running diagnostics on a counter must resolve and document this. (CR4.49)

4.2.7 Availability

Diagnostic trace information must always be available for inspection or retrieval. It must be retained over a counter swap. (CR4.21)

4.3 Message Store

The message store is the repository for business data used by counter desktop applications.

The related support activities are:

- retrieve bulk data – part of all of a counter message store.
- read
- write

These are currently achieved, in general, by use of command line tools which invoke Riposte API calls. The problem with the command line tools is that they combine the functionality of a number of related Riposte API calls; thus the same command line tool may allow read, write, delete, update or list access. There is a requirement to package the tools for repetitive, well-understood support actions. (CR4.70)

The point of invocation of these command line tools is the currently the correspondence server. The tools generally act on the content of a message store file at the correspondence server but certain problems require access to the content of the message store at the counter. In a small minority of cases, there is a further requirement to retrieve the actual message store (i.e. messagestore.dat) rather than its content.

With the current architecture, the possible points of invocation of message store access tools are a correspondence server or Wing Server. As the latter are back-ups for the correspondence servers they should be used in preference as the point of invocation for message store access. (CR4.71)

It is recognised that it will not be possible to deliver a fully comprehensive toolset for all possible third line support actions, so for these situations, direct access will still be required but should be auditable. (CR4.72)

The existence of repeating problems requiring write access by support must be flagged to development for root cause analysis/resolution. (CR4.73) If the agreed resolution, due to cost

FUJ00139162

constraints, is still the updating of data, this fact must be recorded. {CSQMS004} must be updated accordingly to document the procedure for this.

4.3.1 Functionality

Generic requirements for all message store-related tools are:

- Separate role-based tools must be provided for write/update access and for read access so that read-only tools can be made available to second line support roles while write/update access tools are restricted to third line support roles. (CR4.74)
- The tools must ensure that support actions (especially write/update) are auditable. (CR4.75)
- They must act on the content of a message store at either the Data Centre or the counter (in that order of preference). (CR4.75a)
- Data retrieval will be to a central support server with an option to automatically download the file to the diagnostician's PC. (CR4.75b)

In the case of message store retrieval, a tool is needed to retrieve a complete message store or filter the data according to any attribute or combination of attributes eg. NodeId, Date, Time, ProductNo, SaleValue etc. (CR4.76)

4.3.2 Security

Packaging of Riposte functionality will ensure controlled, auditable write access to the message store.

Tools which allow write access will have restricted availability to third line support. (see CR4.74)

Write access tools must come with the caveat that they are a temporary measure pending an architectural solution. (see CR4.73)

4.3.3 Performance

Performance at the counter or Data Centre must not be adversely affected by use of the tools. (CR4.77)

4.3.4 Reliability

Message Store retrieval is vital to the investigation of all counter problems, so the evidence retrieval tools must be very reliable.

Tools which write to the message store must not cause side-effects. (CR4.78)

Any tool providing write access will be developed according to {DEPRO3} and validated on a test rig to confirm reliability, resilience to user error etc. (CR4.78a)

FUJ00139162

4.3.5 Usability

Tools must be simple to use and must provide help information (on usage, error diagnosis etc.) on request. (CR4.79)

4.3.6 Configuration Management

Retrieved message store files must be automatically tidied from the Data Centre by the support tools. (CR4.80)

4.3.7 Availability

Read and retrieval access to a message store must be available to all diagnosticians. (CR4.81)

4.4 Control of counter processes

Diagnosticians need to know which software, services, processes etc. should be present/running on a counter at a particular time of day to enable the post office business to run. They need to be able to interrogate the system to establish what is actually running.

For each service and process, the following must be documented: (CR4.82)

- Process name associated with service; dll names associated with a process executable
- Brief description of the purpose
- Schedule – when each standard service/process is started/stopped & by what
- Predicted NT resource usage (average, maximum values) for desktop, riposte and other application processes (memory, disk access, riposte statistics etc.)

Diagnosticians need access to "footprint" information to know exactly what other Pathway/ISD activities have been run on counters especially during working hours. (see below)

- Software Distribution
- Reference Data distribution
- Log of Tivoli tasks run
- Other SSC actions (see CR4.50)

Any Tivoli task or support task which runs during office working hours must run at a lower priority than the processes which provide the post office business applications. (CR4.88)

4.4.1 Counter Status information

Process information required:

- List of services/processes/dlls/versions in baseline delivery. (CR4.83)

FUJ00139162

- List of changed services/processes/dlls/versions for a new Pathway release eg. CI4M1. (CR4.84)
- List of changed services/processes/dlls/versions for a Tivoli package. (CR4.85)

Reference Data Information required:

- distribution schedule (CR4.86)
- content information (CR4.87)

4.4.1.1 Functionality

Provide support access to the audit log of Tivoli jobs run on a counter. (CR4.88)

Provide a support tool which obtains a process/NT resource usage snapshot of the counter remotely (i.e. without needing to connect to the counter). (CR4.90)

The tool must allow the retrieval of either process summary information or details of individual dlls. (CR4.91) It must optionally allow NT resource information to be retrieved at either the process or thread level. (CR4.92) The information must be retrievable to a central support server.

4.4.1.2 Security

The security of the counter must not be compromised when obtaining this information. (CR4.93)

4.4.1.3 Performance

Any problem with a root cause in this area may well manifest itself as a counter performance problem. Obtaining a process snapshot should have minimal effect on a counter (which may well be sick already) (CR4.96)

4.4.1.4 Configuration Management

Any files produced by tools for this purpose must be self-tidying. (CR4.97)

4.4.1.5 Availability

Static definition information must be constantly available to diagnosticians. Dynamic snapshot information must be available on demand. (CR4.98)

4.4.2 Manipulation of counter processes

Where analysis of a problem indicates that it is due to the state of a process at the counter, it is necessary for third line support to start and/or stop the erroneous process. (e.g. to close/re-start desktop as it is running low on memory.)

For new problems a KEL must be raised with details of the actual change and the corrective action must be applied by third line support. (CR4.99)

FUJ00139162

For known, repeating problems:

- An auditable support tool must be provided to start/stop certain permitted counter processes. (CR4.100)
- The point of invocation of such tools must be as documented in section 4.10.
- the root cause of a problem in the counter process state must be established and a strategic solution deployed. (CR4.101)

4.4.2.1 Functionality

The inter-dependence of processes must be documented such that all related processes are controlled together as is done in the nightly 3am processing. (CR4.102)

There is a need for a tool to remotely recycle (re-boot) a counter. (see section 4.9)

4.4.2.2 Security

The tools described above must be restricted to third line support and must only act on pre-defined processes. (CR4.103)

4.4.2.3 Auditability

Any tool must ensure that any support action (and associated error/success information) which changes the process state at a counter is auditable. (CR4.104)

4.4.2.4 Performance

Any tool to start/stop a process must not cause any performance degradation either on the counter or at the point of invocation. (CR4.105)

4.4.2.5 Reliability

Any tool which manipulates a counter process state will be developed according to {DEPRO3} and must be fully validated on a test rig to confirm reliability, resilience to user error etc. (CR4.106)

4.4.2.6 Usability

Sufficient error information must be returned to the user to ensure that errors can be readily diagnosed. (CR4.107)

4.5 NT System

4.5.1 NT Crash Diagnostics

Windows NT system failures can record and save details of failure for subsequent analysis.

An event must be logged to the NT event system for each blue screen occurrence on a counter. (CR4.108)

FUJ00139162

Counters must auto-reboot following a blue screen (CR4.109)

The facility to retain a full or partial memory dump on a counter must be configurable (CR4.109a)

Several distinct tools are required for different levels of analysis. These tools should be made permanently available within all NT systems.

There must be no possible confusion to the postmaster as to what constitutes an NT crash situation. Currently "blue screen" is used to describe three separate problems. The symptoms of the different problems should be sufficiently unique as to identify the problem type. ({See CSCP280} which proposes changing the background screen colour to differentiate between the different problems.) (CR4.110)

4.5.1.1 Functionality

A mechanism is required to unconditionally save and extract at least minimal details for automatic harvesting for statistical analysis. (see CR4.109a)

A second configurable option is required to obtain an intermediate level of more detailed information for first level problem analysis and attribution. By default this option would normally be configured on, but there should be a tool to configure it off . (CR4.111)

A support tool is needed to provide this intermediate level of information as it is not available via normal NT functionality. (CR4.112)

A third configurable option is required to retain a complete system dump. By default this option would normally be switched off but there should be a tool to configure it on. (CR4.113)

4.5.1.2 Security

Sensitive data in all NT system dumps files will be handled according to the rules in Appendix 1. (CR4.114)

4.5.1.3 Auditability

The occurrence of all NT system crashes must be recorded permanently to enable trend analysis to be carried out. Access to and processing of (full or intermediate level) system dumps will be recorded in the support activity log. (CR4.115)

4.5.1.4 Performance

The processing and transfer of a system dump must have minimal impact on normal business. (CR4.116)

There must be automatic housekeeping of dump files. (CR4.116a)

A support tool is required to compress a system dump prior to retrieval from a counter. (CR4.117). A standard compression algorithm will be used.

FUJ00139162

4.5.1.5 Reliability

The processing of blue screen dumps must not impact the ability of the counter to run the post office business. (CR4.118)

4.5.1.6 Usability

The tools must be available via approved mechanisms and the existing support interfaces on NT systems. (CR4.119)

4.5.1.7 Configuration Management

The retention of dump information must be configurable (number of dump files retained and level of dump information saved). (CR4.120)

A meaningful identifying name must be given to each dump file. (CR4.120a)

4.5.1.8 Availability

It must always be possible to obtain access to system dumps. If a counter is swapped, it must be optionally possible to first save or copy a dump. (CR4.121)

4.5.2 Windows NT Registry Access

Support staff need to check the validity of configuration details held within the Windows NT Registry. In exceptional circumstances, support staff may need to make ad hoc changes to registry information for which no interface is available other than that of direct access to the registry.

4.5.2.1 Functionality

Support staff require to be able to drill down to specific items within the Registry to read and check values and also to retrieve details from the Registry into a file for later analysis.

A mechanism must use an approved access route and support interfaces on NT systems. (CR4.125)

A mechanism is required to enable restricted additions, changes and deletions to the Registry.

4.5.2.2 Security

Sensitive registry data will be handled according to the rules in Appendix 1. (CR4.126)

Tools to read Registry items on a counter will be available to second and third line support, however, any tool which provides update/delete access to the Registry must be restricted to third line support. (CR4.126a)

The integrity of the counter must not be compromised by access to registry data. (CR4.126b)

FUJ00139162

4.5.2.3 Performance

The performance of the counter must not be compromised by access to registry data. (CR4.127)

4.5.2.4 Auditability

All access to a counter registry will be performed via a fully auditable tool. (CR4.128)

4.5.2.5 Reliability

The actual technical details of registry changes must be checked and approved by the appropriate Pathway TDA. All changes (whether delivered via an approved tool or via an ad hoc action) must be fully tested on a test rig. (CR4.129)

Any possibility of side effects e.g. interlocks should be checked in validation. (CR4.129a)

4.5.3 Internal Windows Services

4.5.3.1 Print Queue(s)

4.5.3.1.1 Functionality

Mechanisms are required by diagnosticians via an approved access mechanism which:

- Monitor Print queues (CR4.130)
- Retrieve print logs (CR4.131)
- Clear/re-set print queues (CR4.132)

4.5.3.1.2 Auditability

A fully auditable tool must be provided for these purposes. (Details to include who, when, what etc.) (CR4.133)

4.5.3.1.3 Performance

Performing print queue housekeeping must not impact the post office business at the counter. (CR4.134)

4.5.3.1.4 Reliability

Any tool which changes the state of a print queue must be fully validated on a test rig. (CR4.135)

4.5.3.2 Support task scheduling and execution

Certain support accesses and interventions are accomplished by program execution on counter systems.

FUJ00139162

The 'at' scheduler is used to run both the nightly '3am' cleardesk processing and certain ad hoc support tasks.

4.5.3.2.1 Functionality

There is a requirement to run certain specific support tasks at a counter. (CR4.136)

4.5.3.2.2 Security

The submission/running of a support task must maintain the integrity of the system. (CR4.137)

4.5.3.2.3 Auditability

A mechanism is required to record details of all support tasks submitted and run at a counter. (Details to include who, when, what etc.) (CR4.138)

4.5.3.2.4 Reliability

A formal mechanism which allows the submission of support tasks will minimise the possibility of errors. (CR4.139)

Any tool for this purpose must be fully validated in a test environment which fully replicates live running. (CR4.140)

4.5.4 File System

The file system can be broken down into two logical sections:

- NT file system

An overview of the Pathway-specific parts of the NT directory hierarchy need to be available in a support guide. (CR4.141)

- Pathway software inventory

A baseline definition of a software release must be available to support (CR4.142)

4.5.4.1 NT file system

Tools are required for support staff to obtain file and disk information from Windows NT systems to confirm validity and correct functioning. (CR4.143)

4.5.4.1.1 Functionality

There is a need to view the names of and contents of Pathway-related directories. (CR4.144)

Tools are required to perform basic housekeeping checks on the disks and file to report: (CR4.145)

- available free space on disk
- size of largest files on disk etc.

FUJ00139162

- space used by each user or by directory

Tools to check the integrity of the disks are required. These checks are for flaws and/or errors. (CR4.146)

4.5.4.1.2 Security

The integrity of the counter system must not be compromised by retrieval of NT file system information. (CR4.147)

4.5.4.1.3 Performance

The performance of the counter must not be compromised by retrieval of NT file system information e.g. directory listings. (CR4.147a)

4.5.4.1.4 Usability

Diagnosticians must be able to retrieve NT file system information quickly and accurately. (CR4.148)

4.5.4.1.5 Availability

The information must be available to all diagnosticians. (CR4.149)

4.5.4.2 Software Inventory files

It must be possible to check exactly what software is or was present on a counter at a given time. This information must be available and correct historically and through the normal systems management routes such that it is possible to establish what versions of each dll were running when a particular application problem occurred.

4.5.4.2.1 Functionality

It must be possible to check via the system management information to obtain an unambiguous view of what software is/was running on a counter at a particular time. (CR4.150)

It must be possible to verify that the software present on a counter is as expected. (CR4.151)

It must be possible to establish whether the solution to a particular problem (PinICL, CP) is/was running on a counter at a particular time. (CR4.152)

4.5.4.2.2 Reliability

The databases and tools which provide this information must always result in the correct information being returned. (CR4.153)

4.5.4.2.3 Usability

Diagnosticians must be able to retrieve this information quickly and accurately from existing electronic sources (Tivoli web-site, RM database, PVCS, SSC web-site). (CR4.154)

FUJ00139162

It must not require special technical skills (e.g. writing database queries) to obtain this information. (CR4.155)

Sufficient documentation, training and cross-reference information must be provided to ensure the required information is available. (CR4.156)

4.5.4.2.4 Availability

The information must be available to all diagnosticians. (CR4.157)

4.6 Performance

The existing support process involves using some fairly basic tools to obtain information regarding the performance of counter NT systems.

Performance requirements are being satisfied elsewhere i.e. PMS.

These requirements will not be considered further in this document.

4.7 Application problems

This section is concerned with problems caused by application code which are not manifested as incorrect functionality. Such problems can be broken down into two categories:

- Application crash
- Application processing malfunction or communication problem

4.7.1 Application crash

4.7.1.1 Functionality

A facility is required to capture application crash information. An alert in the event log is needed to highlight that an application crash has occurred. (CR4.161)

There should be no visibility of an application crash to the post master, however he must be advised that the system is busy so that he does not re-boot the system. (CR4.162)

A configurable option should be provided to record further diagnostic details about an application crash. This information should be switched on by default but should be configurable “off”. (CR4.162a)

Diagnostic details relating to an application crash should be written to the same file as the diagnostic logging but with a different/unique classification. (CR4.163)

4.7.1.2 Security

Sensitive data must not be compromised when an application crashes. (CR4.164)

FUJ00139162

4.7.1.3 Performance

The performance of the counter must not be compromised by retrieval of application crash information. (CR4.165)

4.7.1.4 Usability

A support guide must document the meaning of information logged when an application crashes. (CR4.166)

4.7.2 Application processing malfunction or communication problem

4.7.2.1 Functionality

There is a requirement for the state of an application to be checked remotely. In the case of a distributed application it should provide some interworking health state checks which optionally return status information. (CR4.167)

Where an application appears to have hung, there is a requirement for a facility which monitors the behaviour of an application to ascertain abnormal behaviour characteristics. (CR4.168)

The periodicity of the facility must be configurable. (CR4.168a)

4.7.2.2 Performance

The above facilities must not incur any performance overheads. (CR4.169)

4.7.2.3 Usability

A support guide must document the content and purpose of such facilities. It must include any recovery or avoidance action for specific known problems. (CR4.170)

4.7.2.4 Availability

These facilities must be available to all diagnosticians. (CR4.171)

4.8 Connectivity

This section is concerned with application-level connectivity problems. It is assumed that any requirements on the network support community are detailed elsewhere.

4.8.1 Intra-LAN

Tools are required that will provide support staff with a capability for easily checking that all the PCs at a Post Office are intra-accessible. (CR4.180)

4.8.2 WAN

Tools are required that will provide support staff with a capability for easily checking that a counter PC can connect to the Correspondence Server. (CR4.181)

FUJ00139162

4.9 Counter Platform

4.9.1 Functionality

Tools are required that will provide diagnosticians with a capability for checking the status of a counter platform as a functioning entity. (CR4.185)

Tools are required that will provide diagnosticians with a capability to remotely recycle a counter platform. This will enable a re-boot and re-connection without postmaster intervention thus re-establishing operational capability to the level of Systems Management accesssibility. (CR4.186)

4.9.2 Security

This facility must not compromise the security at the counter. (CR4.187)

4.9.3 Auditability

The use of this facility must be fully auditable. (CR4.188)

4.9.4 Performance

The maximum time for remote re-boot and re-connection must be defined. (CR4.189)

4.9.5 Reliability

This facility must be fully validated on a test rig. (CR4.190)

4.9.6 Usability

Clear documentation of the steps needed to achieve this must be provided. (CR4.191)

4.10 Tool Production Process

Throughout this document, requirements for support tools are stated. The development process for support tools will be the standard process as documented in {DEPRO3}. The generic requirements are stated below.

4.10.1 Future support toolset

4.10.1.1 Functionality

- Tools must have a graphical or web-based user interface wherever possible (CR4.193)
- Use of tools must be auditable (CR4.200)
- An identical consistent toolset must be available across all similar support platforms (CR4.194)
- Tools must compress all files greater than a specified size before retrieval. (CR4.195)

FUJ00139162

- Tools must create any output file in a standard Pathway directory on the counter separate from NT temporary files. (CR4.196)
- Tools must name output files appropriately to identify their origin & contents e.g. FAD, counter, file type, date, instance after retrieval from the counter (CR4.197)
- Tools must act on either a test rig counter or a live counter (CR4.197a)
- A central repository for retrieved data is needed with an option to automatically download the file to the diagnostician's PC. (CR4.197b)
- Tools must be responsive, reliable and non-interactive (CR4.197c)
- Development, enhancement and installation of new tools (and new versions of existing tools) must be done in a responsive and controlled manner (CR4.197d)
-

4.10.1.2 Security

Sensitive data must not be compromised by a support tool. (CR4.198)

Read/retrieval mode tools will be available to second and third line support roles. Write/update access tools must be restricted to third line diagnosticians. (CR4.199)

4.10.1.3 Auditability

All support tools must write audit details. Details must include username, computer name, FAD/counter name, timestamp, activity performed, error code returned. (CR4.200)

4.10.1.4 Performance

All support tools must be non-invasive on a counter. (CR4.201)

Where possible, support tools should be run (CR4.202):

- outside office working hours
- at a lower priority than business applications.

4.10.1.5 Reliability

All tools must be developed according to {DEPRO3} and be fully validated in a test environment that mirrors the way the tool will be run in live mode. (CR4.203)

4.10.1.6 Supportability

There will be full supporting design documentation to allow future understanding and enhancement of support tools. (CR4.204)

The tools will be fully supported within the Pathway project. (CR4.205)

FUJ00139162

4.10.1.7 Usability

Support tools must be simple to use with sufficient user documentation and online help for parameter descriptions, error messages etc. (CR4.206)

A register of the available counter support toolset must be produced and maintained on a support web-site. (CR4.207) In the longer term, it should be possible to invoke the tool from this web front-end. (CR4.207a)

4.10.1.8 Configuration Management

Output files must automatically be deleted from a counter if retrieved successfully. (CR4.208)

4.10.2 Existing diagnostic tools

Second, third and fourth line support currently have a distinct set of support tools for the activities that they perform. As second/third line support are taking on tasks that were formerly undertaken by third/fourth line support there is a need to review what is available at each level of support and make tools and knowledge available to other lines of support, where appropriate. (SR4.209)

4.10.2.1 Requirements for second line support

In addition to the above requirement, there is a need to review the Tivoli tasks currently available to second line support to see if they match the current requirements. For example, second line support are now retrieving PSStandard and Audit logs. There is a requirement for them to:

- have access to reliable retrieval tools which are fit for current purpose (CR4.210)
- understand the format of these log files (CR4.212)
- have access to any analysis tools currently used by third/fourth line support (CR4.214)

4.11 Diagnostician use of correspondence server

The current third line support point of access to a counter is the correspondence server. This conflicts with the use of the correspondence server for running Agents and other business critical processing. An additional usage of the correspondence server by third line support is for access (retrieval and occasionally update) to message store data. Support access to a correspondence server must be limited to the diagnosis of correspondence server problems.

Alternative means of achieving both the above already exist and do not involve the use of a correspondence server). The justification for the move is:

- Correspondence servers are not designed for support purposes
- Restricted availability of filestore on a correspondence server
- Support use could have a detrimental effect on running the business applications

FUJ00139162

There is a requirement to pursue these alternatives in the short term in a way that may be further enhanced in the future. (CR4.220)

4.11.1 Diagnostician Access to Counter

As stated above, there is a requirement to remove non-essential support activities from the correspondence servers. The target solution is to improve on the command line access tools; however this must not preclude changing the point of access to a counter from the correspondence server to a support server.

4.11.1.1 Functionality

There is a requirement that third line support activities involving access to a live counter are changed from going via the correspondence servers to go via a support server.

For access to a counter, auditable, mechanisms should be provided firstly to connect to a specific directory on a support server and secondly to connect from the support server to the desired counter. (CR4.222) This access will only be permitted to third line support (as now).

As a longer-term activity, as mentioned elsewhere in this document, there is a requirement for an improved method of access from the command line mode available at present. However, there will be situations where automation is not the answer and direct access will occasionally be needed.

4.11.1.2 Security

Access to counter NT systems must be role based and password controlled. (CR4.236)

Access to counter NT systems must not compromise any existing security policy in particular {SFS}, {ACP}. (CR4.238)

The security of access point must not be compromised by support access to a live counter. (CR4.240)

4.11.1.3 Auditability

Access to counter NT systems must be auditable to an individual (details must include, who, when, from where). (CR4.242)

All support activities must be recorded. (CR4.244)

4.11.1.4 Performance

Multiple point of access sessions must run concurrently without degradation of system performance and while giving support staff good system response. (CR4.246)

4.11.2 Diagnostician Access to Message Store Data

For the migration to CI4, Wing servers were utilised as back-ups for the correspondence servers. {CP2775} has subsequently been raised for the formal introduction of these to the

FUJ00139162

horizon architecture. Wing servers contain fully replicated message store data but do not have "agents" running on them.

There is currently a cluster of four Wing servers located at Bootle.

4.11.2.1 Functionality

There is a requirement that support activities involving access to message store data are changed from the correspondence servers to the Wing servers. (CR4.250) This access will only be permitted to third line support (as now).

As a longer-term activity, as mentioned elsewhere in this document, there is a requirement for formal message store access tools to be provided on the Wing Servers.

FUJ00139162

5.0 Documentation Requirements

Throughout this document, extensive reference is made to the requirement for support documentation including support guides. It should be noted that support documentation must be provided in a structured form. (SR5.1) In fact, the requirement is more widely scoped as a need to provide a structured knowledge base for the Pathway solution. (SR5.2) CafeVik has several examples of how this has been achieved within the company as a Solution Kit and what the benefits are in terms of manageability, cost reduction etc. See e.g.:

GRO

The structure and method of delivery of this documentation must be designed at the SOD stage. Within the overall framework, standards for product support guides must be defined – both for in-house and third party products. (SR5.3)

FUJ00139162

6.0 Appendix 1 Sensitive Data

e_mail from Graham Hooper:

-----Original Message-----

From: Hooper Graham J

Sent: 24 April 2001 10:57

To: Robinson Peter PJ

Subject: RE: Query regarding sensitive data.

Peter

I have prepared some guidelines here but they are not yet incorporated into agreed Pathway procedure. This will be done as soon as I can extricate myself from new business work.

In short there are two types of sensitive material - personal information and business information. The former currently relates to NINOs and possibly Bank details at a later stage. The latter to crypto type code. The DPA prohibits sending personal info outside the EEU (ie to Escher/Microsoft). Pathway Security policy and contractual obligations prohibits the release of crypto information outside the organisation.

I propose that system dumps should be examined under Pathway/ICL controlled secure conditions and by Pathway/ICL employees. Suitable secure areas would restrict access generally to those persons who have need to examine the data and appropriate controls (clear desk, standalone machines etc) maintained at all times.

I will advise as soon as I get this out.

Rgds

Graham

-----Original Message-----

From: Robinson Peter PJ

Sent: 23 April 2001 16:20

To: Hooper Graham J

Subject: FW: Query regarding sensitive data.

FUJ00139162

Graham, I believe I've heard you or Geoffrey state that provided system dumps etc are examined under the appropriate secure conditions they can contain "sensitive" material (I recall the conditions are also such that this material can not be made available to 3rd parties with which ICL doesn't have the appropriate agreements, eg Microsoft).

If my belief is correct do you know where this 'policy' is formally documented?

Rgds

PJR