



Operational Level Agreement HNGx Application 4th line support

**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**



Document Title: Operational Level Agreement for Application 4th line support of HNGX

Document Reference: SVM/SDM/OLA/0017

Document Type: Operational Level Agreement

Release: Not Applicable

Abstract: This OLA is a description of the HNGx Application 4th line Operations Service provided under contract to the Post Office Account & Post Office Limited

Document Status: APPROVED

Author & Dept: Mukesh Mehta, Post Office Account

External Distribution: None

Security Risk Assessment Confirmed YES

Approval Authorities:

Name	Role	Signature	Date
Keith Tarran	Applications Development Manager, Post Office Account		
Nana Parry	BAS Tower Lead, Post Office Account		



0 Document Control

0.1 Table of Contents

0	DOCUMENT CONTROL.....	2
0.1	Table of Contents.....	2
0.2	Document History.....	4
0.3	Review Details.....	4
0.4	Associated Documents (Internal & External).....	5
0.5	Abbreviations.....	7
0.6	Glossary.....	8
0.7	Changes Expected.....	8
0.8	Accuracy.....	8
0.9	Security Risk Assessment.....	8
1	SERVICE PRINCIPLES.....	10
2.1	4LS Service Team.....	10
1.1	Service Hours.....	10
1.2	Incident Management.....	10
1.2.1	System Incident.....	11
1.2.2	Major Incidents.....	11
1.2.3	Service Targets.....	11
1.3	Problem Management.....	12
1.3.1	Service Targets.....	12
1.3.2	Business Impact Review.....	12
1.3.3	Known Errors.....	13
1.4	Change Management.....	13
1.4.1	Change Proposals (CPs).....	13
1.4.2	Managed Service Change (MSC).....	13
1.5	Configuration Management.....	14
1.6	Release Management.....	14
2	4LS EXTERNAL INTERFACES AND SERVICE COMMITMENT.....	15
2.1	3LS Commitment in support of 4LS.....	15
2.2	4LS Commitments to 3LS.....	17
2.3	Operations Reference Data Team Commitment to 4LS.....	18
2.4	Agreement between POA Operations and 4LS.....	18
2.5	Commitments between Live Support Testing and 4LS.....	19
2.6	4LS Internal Interfaces.....	19
3	4LS DEVELOPMENT SYSTEMS AVAILABILITY MANAGEMENT.....	20
3.1	Capacity Management.....	20
3.2	Supplier Management.....	20
3.3	Security Management.....	20
4	DOCUMENTATION.....	21
5	4LS SERVICE GOVERNANCE.....	22
5.1	Financial Management.....	22



5.2	Service Reviews/Service Reporting.....	22
5.3	Service Improvements.....	22
5.4	Risk.....	23
APPENDIX A – 4LS APPLICATIONS.....		24
Counter/BAL.....		24
Data Center Host Applications.....		24
Branch Connectivity.....		25
APPENDIX B – 4LS INTERNAL INTERFACES.....		26
Commitments between Integration Team and 4LS Teams.....		26
Commitments between INFREL DEV and Counter 4LS Team.....		26
Commitments between CTR, BAL, Datacenter Audit, Host and EM Sysman Teams.....		26
APPENDIX C – 4LS DEVELOPMENT INFRASTRUCTURE SUPPORT.....		28
Operating system configuration.....		28
Hardware and Event Monitoring.....		28
Third party management.....		28
Operating system housekeeping.....		28
Problem diagnosis and resolution.....		28
Backup and restore.....		29
Operating system patch management.....		29
Anti-virus software maintenance.....		29
Capacity monitoring.....		29
Recording service history.....		29
GDC 4LS Development Infrastructure Support.....		29
Firewall Management.....		29
4LS Counter build.....		30
REMOVE RED PIKE FROM UTIMACO VPN ON COUNTERS.....		30
Step 1 Configure Counter not to reference Red Pike and switch off encryption.....		30
Step 2 Sign Policy File.....		31
Step 3 on Counter deregister RedPike.....		31
Step 4 Reboot.....		31
Step 5 Remove Red Pike Object.....		31



0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	1/6/2009	New OLA created to reflect the operational levels agreement between 3 rd and ODC 4 th line HNGX support	
0.2	9/6/2009	Updated with Tony Little's comments	
0.3	25/6/2009	Updated with information from Adam Cousins	
0.4	3/7/2009	Updated following review with Steve Godson	
0.5	5/08/2009	Updated following information provided by Infinite on ITSG support.	
0.6	15/8/2009	Updated follow latest round of reviews and to include firewall proposal	
0.7	25/8/2009	Updated to include comments from Graham Allen	
0.8	26/8/2009	Updated following formal review with Infinite and 4LS UK	
0.9	7/10/2009	Updated following review with Ian Turner	
0.11	26-Nov-2009	Reviewer list updated, draft version number applied	
0.12	11 Jan 2010	Update from Infinite review – change CIS to 4LS on page 30	
0.13	12 Jan 2010	Updates from RMG BU review	
1.0	14-Jan-2010	Approval version	
1.1	20 Aug 2010	Revised draft following updates from REL2	
1.2	13-SEP-2010	Updated following review	
1.3	09 Dec 2010	Update after group review	
1.4	30 Dec 2010	Major updates and document reformatting post group review output	
1.5	16-Mar-2011	Update to security classification and reviewer list	
1.6	16-Nov-2011	Updated following review and to include account name change to POA	
1.7	11-Mar-2013	Updated following review with Keith Tarran	
1.8	22-Mar-2013	Ready for approval	
1.9	04-Apr-2013	Minor corrections	
2.0	05-Apr-2013	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	mukesh.meht & PostOfficeAccountDocumentManagement GRO
Mandatory Review	
Role	Name
Applications Service Delivery Manager	Yannis Symvoulidis
SSC and Reference Data Manager	Steve Parker(*)



Counter & BAL 4LS Manager	Mukesh Mehta
Data Centre Development Manager	Adam Spurgeon
Estate Management Manager	Steve Evans
Head of Application Services Development	Keith Tarran
Integration Team Manager	Vijesh Pandya
Optional Review	
Test Manager	Sheila Bamber
LST Manager	Mark Ascott
Problem Manager	Steve Bansal
Operational Security	Donna Munro
Technical Architect	Pete Jobson
CISO	Brad Warren
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001(D O NOT REMOVE)	4.0	21-Nov-2008	POA HNG-X Generic Document Template	Dimensions
SVM/SDM/PRO/0018			POA Customer Service Incident Management Process	Dimensions
SVM/SDM/PRO/0001			POA Customer Service Major Incident Management Process	Dimensions
SVM/SDM/SD/0003			Data Centre Operations Service Description	Dimensions
CS/FSP/002			Horizon Service Desk Call Enquiry Matrix and Incident Prioritisation	Dimensions
SVM/SDM/PRO/0025			POA Customer Service Problem Management Process	Dimensions
SVM/SDM/SIP/0001			POA Customer Service Business Continuity Framework	Dimensions
PGM/CHM/PRO/0001			POA Change Management Process (for CPs)	Dimensions
SVM/SDM/PRO/1184			POA Customer Service Change Management Process (for OCPs)	Dimensions
C-MSv1.6			Managed Service Change (MSC) Process	Café Vik
SVM/SDM/SD/0004			Third Line Support Service: Service	Dimensions



			Description	
SVM/SDM/SD/0005			Application Support Service(Fourth Line)	Dimensions
CS/FSP/006			End to End Support Process, Operational Level Agreement	Dimensions
DEV/INF/LLD/0112			LST Test Services	Dimensions
DEV/GEN/TEM/0009			Counter Support Risk Management Process	Dimensions
C-MP 1.2			Fujitsu Services Risk Management Process	Café Vik
SVM/SDM/STP/0001			Application Services (4th Line) offshore service governance.	Dimensions

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

0.5 Abbreviations

Abbreviation	Definition
ADSL	Asynchronous Digital Subscriber Line
AP	Automated Payment
CCD	Contract Controlled Document
CIT	Continuous Integration and Test
CP	Change Proposal
CSIP	Continuous Service Improvement Plan
DVLA	Driver Vehicle Licensing Agency
EM	Estate Management
GDC	Global Delivery Centre
HSD	Horizon Service Desk
ISDN	Integrated Services Digital Network
ITIL	Information Technology Infrastructure Library
ITSG	GDC IT Support Group
KEL	Known Error Log (and support knowledge entries)
LAN	Local Area Network
LST	Live Support Testing
MSC	Managed Service Change
NNM	Network Node Manager
Peak	POA proprietary call management system
PIT	Post Office (Fujitsu) System Integration Team
PTF	Peak Targeting Forum
PVB	Product Version Baseline
ODC	Off- Shore Delivery Centre
OCP	Operational Change Proposal



OLA	Operational Level Agreement
3LS	Software Support Centre (3LS)
3LS	3 rd Line support
4LS	4 th line support for HNGx
MOR	Model Office Release
POA	Post Office Account
RADIUS	Remote Authentication Dial In User Service
RDT	Ref Data Team
SLA	Service Level Agreement
SLT	Service Level Target
SMC	Service Management Centre
WAN	Wide Area Network

0.6 Glossary

Term	Definition
Branch	For the purposes of this document "Branch" shall mean all Post Office Premises with the HNG-X Service Infrastructure. For the avoidance of doubt, this excludes stand alone HNG-X terminals.

0.7 Changes Expected

Changes

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.



1 Service Summary

4th Line Support Service

The 4LS provides Application Software Support to the HNGx Business Capabilities and Support Facilities using appropriately trained operational staff.

The operational scope of the service covers:

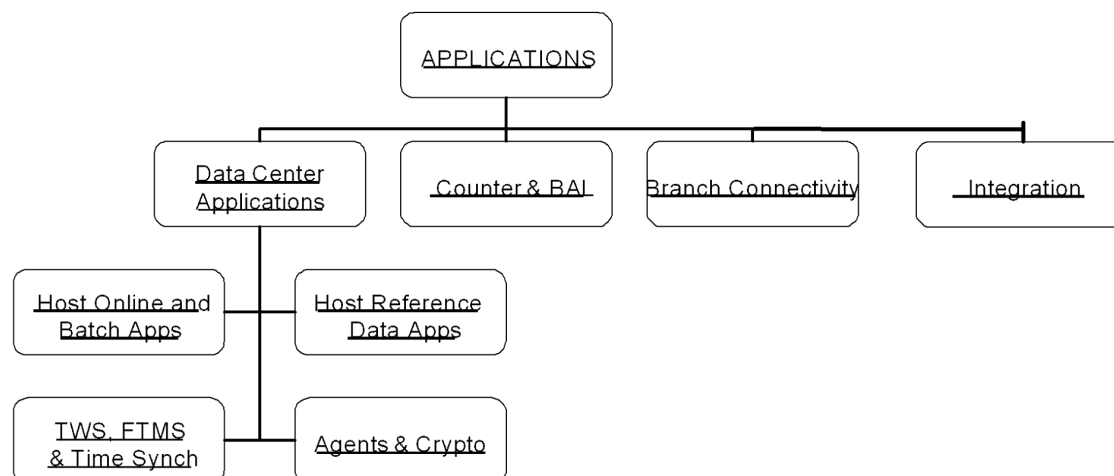
- (a) Investigation and resolution of new Application Software Incidents within the Branch Infrastructure and HNG-X Central Infrastructure environments and application code, which cannot be otherwise resolved by the Third Line Support teams. The initial investigation and resolution of known Software Incidents, which is classed as "first line", "second line" and "third line" support respectively, is described in the Contract Controlled Documents (CCDs) entitled "*Service Desk Service: Service Description*" (SVM/SDM/SD/0001), "*Systems Management Service, Service Description*" (SVM/SDM/SD/0006), "*Third Line Support Service, Service Description*" (SVM/SDM/SD/0004);
- (b) Root cause analysis of Application Software problems and provision of coded fixes
- (c) Programme support, the detail of which is set out in Annex A in the Applications Support Service (Fourth Line) Service Description(SVM/SDM/SD/0005)
- (d) Deliver secure coding training on an annual basis.
- (e) Maintain the secure guidelines on an annual basis
- (f) Maintain the secure coding template on an annual basis

A list of Software Application areas maintained under this OLA can be found at Appendix A



Service Principles

2.1 4LS Service Team



The latest organisational chart can be found at

IRRELEVANT

1.1 Service Hours

The Application Support Service (Fourth Line) is not directly available to Post Office. It is a service internal to Fujitsu Services and is available between 09:00hrs to 17:30hrs Monday to Thursday and 09:00hrs to 17:00hrs Friday.

The Application Support Service (Fourth Line) is available on-call during other times for pre-planned events as agreed between Service Operations and the respective Development Managers.

If Ad-Hoc out of hours support is required to respond to, for example, a major incident, then any 4LS Application Support response will be on an availability basis.

1.2 Incident Management

The Application 4LS and 3LS work closely together in the analysis and resolution of Software Incidents.

The Application 4LS will provide Software support by:

- (a) Receiving from the 3LS, Software related Incidents which cannot be resolved by the 3LS. Such Incidents will have been originally logged by the Service Desk following a call from a Branch, or having been logged by the Systems Management Service, the Central Network Service or the Data Centre Operations Service.
- (b) Ensuring the internal Fujitsu Services Incident Management systems are updated with the Incident resolution details prior to return to the 3LS together with the method of recreating the problem;
- (c) Ensuring that the known error log is updated with the detail of the resolution for that incident.
- (d) Ensuring that any resolutions which are returned to 3LS have been tested and have been correctly authorised in accordance with the Release Authorisation Process.



1.2.1 System Incident

The 4th Line team will assist 3rd Line Support to resolve any system incidents in accordance with the incident management process (as described in SVM/SDM/PRO/0018 and detailed in section 3.2 of this document).

All incidents must have been logged in Triole for service (TFS). It is the responsibility of the HSD or SMC to understand the severity and status of the incident - then the call is passed to Peak for 3LS if necessary. It is the responsibility of the 3LS to determine the status of the incident and whether it requires further analysis in which case the analysis details will be logged in Peak.

1.2.2 Major Incidents

Major incidents affecting the HNGx service delivery to Post Office Ltd

In the event of a major incident affecting the HNGX services, an incident will be logged and managed in accordance with the SVM/SDM/PRO/0001 and Fujitsu CPM31 processes to ensure that all communication is clear, concise and occurs quickly. For a definition of a Major incident please refer to section 3 of SVM/SDM/PRO/001.

Investigation and diagnosis of the incident may require attendance at technical bridge teleconferences. The team will be required to provide updates on the current impact of the incident, perform corrective actions and record information in the major incident template at regular intervals for the duration of the incident.

As part of an on-going service assurance activity, team members will be mandatory participants in regular Major Incident and Post Incident Reviews.

Major incident affecting the delivery of the 4LS service from IND49.

These are incidents that affect the provision of the 4LS service from IND49 and should be raised by the GDC Operations Manager to the UK 4LS Applications Manager.

1.2.3 Service Targets

This section describes the operational service targets that have been agreed with Service Operations to underpin operational delivery of the service. The identified targets will be measured at 95% achievement over a rolling 3 month period.

The 4LS is not subject to contractual SLAs or Operational Service Targets. To ensure that appropriate timely response is enabled incidents managed between 3LS and 4LS will be subject to the following conditions and timeframes:

3LS will ensure that all incidents passed to 4LS will be transferred within half life for each of the identified priorities and timescales defined below:

- **A Priority - 2 working days**
- **B Priority - 4 working days**
- **C Priority - 7 working days**
- **D Priority - 28 working days**

For example:

Priority "B" Incident



- Will be passed to 4LS within 2 days of receipt by 3rd Line Support
- An incident resolution, as agreed with 3LS, will be provided by 4LS within the overall 4 day 3LS window.

It is essential that incidents are proactively managed and that regular updates are provided on Peak to ensure that all parties are kept informed on progress to resolution. To achieve this, the following guidelines are provided:

- **A Priority – ongoing review, incident update provided at least once day**
- **B Priority – review and update at least once every 2 working days.**
- C and D priority should be reviewed and updated when the peak is actioned.

3LS will endeavour to pass incidents to 4LS at the earliest opportunity within the agreed half life and provide early warning for higher priority incidents.

3LS will ensure that any incident passed to 4LS will contain the minimum data set of information as required by any associated support guide for the application area of concern.

The incident clock related to 4LS support will start from the point that 4LS receives the incident as a Peak.

The 4LS incident clock will stop when the incident has been identified resolved as agreed with 3LS.

It is expected that although calls may enter 3LS at high priority, in the majority of cases, 3LS will produce a resolution for the incident. 3LS will subsequently review the priority of any peak related to a resolved incident that requires further root cause analysis and update that priority in agreement with service operations.

1.3 Problem Management

The 4LS team will be actively involved in the problem management process (as described in SVM/SDM/PRO/0025) to proactively perform investigations into the root cause of incidents.

All known errors should be recorded and changes should be proposed to resolve problems. These will be discussed at the regular service review.

1.3.1 Service Targets

There are no Service Targets applied to problem management and root cause analysis of resolved incidents, although Service Operations may determine a priority of a root cause based on service impact. These priorities will be determined on a case by case basis.

1.3.2 Business Impact Review

Prior to 3LS passing any resolved incident to 4LS for root cause analysis or code fixing, the peak will be reviewed by Business Impact Forum to agree that a root cause analysis or a coded fix are required to maintain the operational service. It is expected that BIF will ensure that a business impact statement is provided on peak prior to the peak being passed to 4LS.

1.3.3 Known Errors



In most cases 3LS will have raised an entry in the KEL identifying a “known error” following receipt of the incident. Where 4LS identify a KEL has not been raised for a peak passed to 4LS for root cause analysis, 4LS will raise a KEL as required and determined by the analysis.

Where a KEL has been previously raised by 3LS then 4LS will update the KEL based on the analysis and further update the KEL where the root cause is identified

4LS will ensure that KEL information is communicated to 3LS who will approve that the Known Error Log (KEL) has been appropriately updated and confirm the information is disseminated to the Service Desk to enable the resolution of similar Incidents;

1.4 Change Management

This section covers:

- Change Proposals for change that will affect the whole service delivery model and
- Managed Service Change (MSC) raised for operational change in the delivery of the service by 4LS teams
- Managed Service Change required to GDC support services infrastructure (for example changes in infrastructure/operation in IND49).

4LS will follow the defined framework for Post Office Account change management (as defined in PA/PRO/001) Change Proposals (CPs)

As part of the major release process 4LS teams will participate in, provide feedback to and undertake the activities identified during the planning of major releases.

For operational changes (MSC) 4LS teams will create and impact MSCs (Managed Service Change Process on Café Vik) for operational changes being carried out on the Post Office Account's infrastructure for the services.

For GDC support service change a MSC will be raised to allow proper impacting of any change and authorisation as required by the relevant GDC SoW

1.4.1 Change Proposals (CPs)

4LS will impact CPs (as described in PGM/CHM/PRO/0001) with an accurate prediction of the time and expenses required to perform the proposed activities. Where there is ambiguity then the team will seek to clarify with the CP author before submitting their impact.

Where required, 4LS may be requested to implement urgent change proposals as part of a maintenance release. This will be on the authorisation of the account's operations and programme management teams.

1.4.2 Managed Service Change (MSC)

4LS will create and impact MSCs (Managed Service Change Process on Café Vik) for operational changes being carried out on the Post Office Account's infrastructure for the services (as described in 1 Service Summary).

- No changes will be carried out without an approved MSC. Any changes related to an incident should be authorised via MSC. Only if the change is extremely urgent and there is not enough time for formal MSC approval should the MSC be raised retrospectively – this change would still require authorisation from service operations.
- No changes will be carried out that will cause an interruption of service.



- The change originator is responsible for ensuring that the change is completed in accordance to best working practices and operational standards. Appropriate levels of implementation, communication, regression and test planning must be completed.
- Team members may be required to support MSCs raised by other teams.
- Following the successful completion of an MSC, the team will update any localised working instructions and documentation to ensure the detail reflects the service being provided.

1.5 Configuration Management

4LS will comply with the POA Configuration Management procedures and policy statements (PGM/CM/MAN/0004).

4LS are expected to maintain a high level inventory of the support infrastructure and tooling for the purposes of call-logging, security vulnerability checking etc. Each member of the team is expected to work with other teams to gain a good working knowledge of exactly how the Infrastructure underpins the delivery of services to the Post Office Account.

4LS is to create and maintain an asset register of all inventory associated with the 4LS service.

This includes any additions and amendments to, and removals from:

- A Support Infrastructure Host, Server or process
- Changes to the configuration of the existing Software/ hardware configurations across the Support Infrastructure.
- Backup Schedule.

1.6 Release Management

The team will support the Release Management function within the Post Office Account in consulting on planned releases. All new releases will be implemented as planned changes performed under the MSC Process and in accordance with the POA Release Management Procedure: SVM/SDM/PRO/0030.

4LS will support the Release Management function by attending the Release Management/Fault Management forums on a regular basis. The forum will review the forward schedule of releases and agree prioritisation.



2 4LS External Interfaces and Service Commitment

The following sections define the interfaces to parties external to the 4LS Application Service and the commitments between the parties in delivery of the service.

2.1 3LS Commitment in support of 4LS

Commitment	Measurement/Metric
To ensure that all incidents or problems passed to 4LS are logged on a call management system (currently Peak)	No incidents or problems are progressed or chased with 4LS that are not first passed on Peak.
To “filter” all incidents for which the problem is already known to the support community and for which a resolution is already known or has been generated. This includes problems for which a resolution is known to 3LS but not yet incorporated into the known deficiencies register available to HSD/IMT/SMC.	No incidents passed to 4LS which are subsequently identified as known errors, except in cases where the resolution was known to 4LS, but this information had not been passed to 3LS in the form of a KEL or diagnostic guide.
To retain in the Peak system, under the 3LS “stack” duplicate incidents - i.e. incidents which are repetitions of an incident which has already been passed to 4LS, and to ensure that when the resolved incident is received by 3LS, the duplicated incident records in peak are closed. Under normal circumstances, where a duplicate incident is identified by 3LS, this will be reported back to the HSD/IMT/SMC and closed as a duplicate incident on Peak.	No duplicated incidents passed to 4LS unless no KEL exists containing the PEAK number i.e. the duplicate incident could not have been found.


**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**


Commitment	Measurement/Metric
To ensure that the correct evidence for any incident or problem is collected prior to the incident or problem record in peak being passed to 4LS for investigation. This should also contain the method to recreate the incident or problem.	No incidents or problems rejected by 4LS on the basis that the evidence was inadequate. Specifically excluded from this measure are instances where, although the evidence was inadequate, 4LS had not indicated to 3LS that the evidence that would be required for such an incident. E.g. In a KEL or support guide.
To ensure that any incident which requires investigation by 4LS is assigned to the correct Peak team dependent on the specific product in which the incident has occurred.	No calls misrouted because of incorrect assignment by 3LS
To ensure that any incidents passed to 4LS units are passed in a timely manner. The timings will vary according to the total time allowed for resolution of the incident in the contract between Fujitsu Services Post Office Account and the customer. These timings will therefore be dependant on the priority of the incident, with (for example) less time allowed for an "A" priority call than will be permitted for a "C" priority.	Incidents are passed within the times specified in section 2.2.3
To ensure that the priority of any incident is assessed and recorded correctly	No incident is passed to 4LS whose priority does not conform to the specification defined in SVM/SDM/PRO/0875.
To "filter" all incidents and problems for which the anticipated resolution or root cause is not one of the following - i) Software error ii) Documentation error. iii) Design Error	No incidents or problems passed from 3LS to 4LS units to be subsequently resolved or root cause as anything other than software, documentation or design issues.
To ensure that for any incident passed to 4LS, the exact area of the incident or problem has been identified, and wherever possible a resolution already produced and the peak updated.	No cases identified by 4LS staff of inadequate diagnosis by 3LS
To create and maintain a register of known errors with the RMG Account solution, which include detail of the resolution for these incidents (where known), and to allow access to this register to 4LS units so that they can enter details of resolutions or root cause identified within their area	"Known error" record to be created and populated by 3LS with access provided to all of the support community.



2.2 4LS Commitments to 3LS

Commitment	Measurement/Metric
To ensure that any incidents or problems so received are maintained on the call management system used by Fujitsu Services RMG BU (Peak).	<p>No cases of lack of updates on incidents or problems on Peak.</p> <ul style="list-style-type: none"> • Priority A and B updated daily. • Priority C and D updated weekly.
To ensure that the incident reported is correctly resolved and the resolution recorded on the Peak system and the incident and resolution passed back to 3LS.	No cases of incidents being passed back for agreement on resolution, without clear and correct resolution recorded on the Peak.
To ensure that 3LS is made aware of the evidence requirements for any form of incident. This will be documented by the 3LS and maintained in accordance with the 3LS commitments to HSD/IMT/SMC . N.B, 4LS are also obliged to raise KELs or documents in this instance.	<p>No cases to arise of 3LS not knowing the evidence required to be collected for any call.</p> <p>A specific exception to this would be the situation in which a completely new type of call was received, where the new evidence requirements should be documented on a KEL.</p>
To enter resolution information into the known error register maintained by the 3LS.	No discrepancy to arise between the known resolutions for incidents and problems and those, which are documented, on the known error log.
Providing the 3LS with documentation and training relating to new Releases in sufficient time to enable the 3LS to become familiar with the new product or service prior to its Release into the Branch Infrastructure or HNG-X Central Infrastructure environments. This documentation will be in the form of a "support guide" which is defined in the Working Document entitled: "End to End Support Process – Operational Level Agreement" (CS/FSP/006); and a template provided in DEV/GEN/TEM/0009	3LS to be supplied with such documentation for any release at least 3 weeks prior to release to live for that product release, and preferably as a continual process during the course of development.
To ensure that the 3LS is supplied with access to source code developed within RMG Account development.	All source code for a release to be made available to the 3LS prior to the Release of that product



2.3 Operations Reference Data Team Commitment to 4LS

Commitment	Measurement/Metric
Operations Reference Data Team are responsible for ensuring that the 4LS development systems are kept up to and in the same state as the live service	Updates available and implemented on support services as required
RDT will provide an automated delivery mechanism for files to be transferred to the 4LS RDMC workstation in Bra01. This uses processes to clone the release state of live data onto the 4LS RDMC (Similar to the existing process for LST)	Automated delivery mechanism in place and operational
4LS must provide evidence that the data update has been completed successfully and confirm this with Reference Data before proceeding	Communication plan between RDT and 4LS agreed and in place

The data reference operations team is now part of 3LS.

2.4 Agreement between POA Operations and 4LS

Commitment	Measurement/Metric
4LS are responsible for providing POA Operations and Release Management with proof of adherence to process and procedures for each incident resolution or problem root cause solution delivered and for providing evidence of each mandatory step having been carried out	Peak updates as appropriate using defined process templates
POA Operations and Release Management are responsible for enabling prompt review of such evidence and feeding back to 4LS any divergence from process or any issues with quality of fixes.	Problem Managers and PTF review peaks as required
<p>Required details of the evidence for each incident resolution or problem root cause solution in peak are:</p> <ul style="list-style-type: none"> Evidence of Release Management approval to supply any code fix (via PEAK or an email confirmation) Updates to the relevant PEAK, detailing the incident resolution or root cause code fix that has been made (in sufficient detail to identify the detail of how the customer service incident is resolved or code changes provide root cause solution, to facilitate easy solution review) Evidence of successful unit testing (having created and run appropriate unit tests) 	Peak updated as appropriate for the incident or problem resolution



and/or automated tests) (test scripts and results supplied)	
<ul style="list-style-type: none"> • Evidence of successful CIT testing (successful test results produced) • Evidence of any necessary changes to the Support Guide (updated support guide produced) • Updates to KELs, if appropriate (confirmation of KEL updates produced) 	

2.5 Commitments between Live Support Testing and 4LS

Commitment	Measurement/Metric
Live Support Testing (LST) provides the testing service as part of the release management process. Further details on LST can be found in the LST service description DEV/INF/LLD/0112 in Dimensions	NA
LST will interact with 4LS in the event that problems/issues arise in the testing phase of a release in which case a defect would be raised in Peak and passed into 4LS.	Communication plan agreed and in place between LST and 4LS. Peak updated as required
4LS will be required to investigate any defect peaks passed from LST. It is expected that 4LS will action these in accordance with the impact of the test incident raised and the priority of the release.	Communication plan agreed and in place between LST and 4LS. Peak updated as required
Any arbitration required on delivery of a test incident solution to a release will be managed through Operations RMF.	Issues requiring arbitration escalated to the appropriate management level.

2.6 4LS Internal Interfaces

The interfaces for teams internal to 4LS are defined in Appendix B

3 4LS Development Systems Availability management.



4LS will assist the POA Applications Service Manager by ensuring that the 4LS service provided supports the service level targets underpinning the HNGX contract and will notify the POA Application Service Manager of specific issues in aspects of the 4LS service being managed by 4LS.

Development systems availability refers to both onshore and offshore support environments. If an activity or process specifically relates to either offshore or onshore services, then that will be clearly identified in the appropriate text.

4LS teams will recommend appropriate service improvement through CSIP activities for the life of the 4LS service.

As part of the 4LS service, ongoing support for the 4LS development infrastructure will be carried out. This ongoing support shall include the key elements as defined in Appendix C:

3.1 Capacity Management

4LS will ensure adequate controls are in place to ensure that there is sufficient capacity to run the 4LS Development services (scope as described in Service Summary).

4LS GDC services will implement a simple script based performance monitoring approach on the 4LS servers in IND49 to ensure that server utilisation does not exceed acceptable levels. This will be part of the standard server monitoring activities to be provided by the GDC server support team. Alert thresholds will be defined for the servers to clearly set out circumstances requiring escalation to management.

4LS will ensure that they have the appropriate resources necessary to deliver the 4LS service.

4LS GDC will use the BT Reporting Facility to monitor the ODC to UK connection.

3.2 Supplier Management

The 4LS teams will be responsible for supporting POA Application Service Management at 3rd party supplier service reviews and working alongside 3rd parties to resolve incidents across the system.

The team have no direct ownership of suppliers underpinning the HNGX service; all contracts with 3rd parties are managed by the POA Application Service Manager.

3.3 Security Management

The 4LS teams will be responsible for working within the framework provided by the account in relation to the Confidentiality, Integrity and Availability of the services (as described in 1.0 Service Summary) and will adhere to security policies defined by the account and Corporate Infrastructure Services and the POA security policy.

The GDC provided 4LS support infrastructure is a shared space environment, providing a number of shared services including user Anti Virus, Active Directory, Email and printing.

To meet Post Office security requirements the 4LS GDC Support environment will be physically separate environments.

The Developer users in the 4LS GDC Support environment will be members of the GDC domain, and will use the existing domain controllers and exchange servers for authentication and email traffic. PGP encryption has been identified as a requirement to encrypt any confidential data sent via email. Two instances of PGP will be deployed within the environment in the 4LS GDC Support environment on



relevant Administrator/Managers desktops. If at that point the 4LS support team need to send any confidential documentation, this will need to be packaged up using the PGP desktop software to be a self extracting mechanism. Passphrases must be issued by a second means of communication and follow the POA Security Policy standards (e.g. SMS). To ensure that any data being printed does not leave the secure 4LS LAN a dedicated Print Server will be provided.

The RED Hat and Solaris servers in the environment will not integrate with either Fujitsu or GDC Active directories or any other LDAP server for authentication or access control. Consequently all user accounts and groups will be local ones.

The GDC 4LS LAN will be protected from the GDC network by the Cisco ASA pairs, which will in turn be protected from outside the GDC by the Checkpoint firewall pairs in the GDC.

The GDC firewalls will control access to the 4LS GDC Services and to the internet. Incoming access to the 4LS GDC network will be restricted to the reference data team in Bracknell. A restricted internet access will be allowed to named sites from the GDC 4LS LAN.

The internet VPN for backup of the main MPLS WAN link will use agreed security parameters, with the shared key issued and communicated by Fujitsu Services Core ISP implementation team to the partner company engineers on phone.

4 Documentation

4LS will be responsible for the maintenance and management of local working instructions and support infrastructure documentation and will perform the following associated activities as required by the area of the service and the level and type of documentation:

- Regular review of all operating procedures, relating to this Service, updating and re-issuing those procedures when appropriate.
- Produce a full index of documentation in relation to supporting the live estate detailing the following elements:
 - Shift Operations documentation
 - Technical/Operations Work Procedures
 - Backup and Recovery Procedures provided by the account detailing recovery requirements for each application stream.
 - All documentation supporting the management of the respective onshore or offshore Infrastructure must be currently aligned to operational requirements within the live estate.
 - Support Agreements and appropriate contact details of those respective parties
- Any documentation supporting the management of the respective applications must be currently aligned to operational requirements within the live estate.
- 4LS GDC will provide an Access Control list produced monthly for sign off by POA Security.
- Both offshore and onshore 4LS are responsible for maintaining the design documentation associated with the relevant offshore or onshore provided 4LS service.

5 4LS Service Governance

5.1 Financial Management

4LS will use SST for the purposes of timesheet logging for all support activities.



5.2 Service Reviews/Service Reporting

POA Applications Service Manager will perform a service review at prescribed intervals with the team to review performance against the OLA and the overall service being delivered by the team

For the 4LS GDC service, the GDC Service Delivery Manager will prepare a service presentation in advance of the service review. This will cover service performance and detail any changes to the service and updates to the service on-going.

The POA Applications Service Manager will feedback to the GDC 4LS on the performance through the review.

The GDC 4LS Service Delivery Manager will provide a scorecard on a quarterly basis for review by the POA Application Service Manager. The scorecard will be based on the standard Core IS scorecard.

4LS will report against the following activities:

- Monthly Service level report including:
 - Percentage service level achieved against targets (RAG status against targets in service level management and service level targets)
 - Management summary
 - Incidents/issues summary
 - Changes/forward schedule of change
- Number of man hours including overtime in relation to time spent in performing CP activity
- Peaks
- Risk Register
- Update progress against Problem Management actions assigned to the team provided by the account
- Continuous Service Improvement Plans

Service Governance for the GDC 4LS service is described in SVM/SDM/STP/0001 Application Services (4th Line) offshore service governance.

5.3 Service Improvements

The 4LS will provide suggestions to improve the quality of the service and reduce operational costs to POA. Any proposed improvements will be reviewed for CSIP activities in line with the POA standard governance process.

Successful CSIP activities will be raised as CPs or MSC's depending on their scope and complexity. 4LS may be required to participate in these changes.

In addition, 4LS team members may be required to attend meetings to work on developing new ideas in areas of high customer visibility.



5.4 Risk

4LS will work alongside the POA Operations management team to produce a risk register, identify risks and provide appropriate input when required to maintain the risk register using Fujitsu Services 'Best Practice' Risk Management practices.

The risk register will be reviewed regularly as part of the monthly service review meeting. POA Application Service Manager will own the risk register.



Appendix A – 4LS Applications

Counter/BAL

BAC

BAD

BNK

CSM

IOP

Peripherals

Postal Services

RDM

SUC

UI

BAL/OSR

Data Center Host Applications

Host Reference Data

RDDS

RDMC

Host

Branch Database

Branch Support Database

NPS

DAT

MIS Workstation

TESQA Workstation

Audit

Audit Server

Audit Workstation

Agent

Web Agents

Banking Agents



Crypto

KMNG Server/Workstation

FTMS

CDG

SRG

EDG Local/Remote

Tip Local/Remote

Branch Connectivity:

Branch Router

DXC

NTP (Time Synch)

GPL/COTS Products:

VPN

EST

Counter

CNIM

Radius

BCMS



Operational Level Agreement HNGx Application 4th line support

**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**





Appendix B – 4LS Internal Interfaces

Commitments between Integration Team and 4LS Teams

4LS Team commitments to Integration

- a) To inform Integration well in advance of a delivery of a release so that they can plan it in. The timing is dependant on the nature of the release but should be at least 3 weeks for a scheduled release.
- b) To give Integration an initial idea of the number of baselines in the delivery.
- c) To ensure that a Release Note is delivered prior to a delivery stating all PVB's and any dependencies.
- d) To deliver all software into PVCS or Dimensions using agreed process and naming convention.
- e) To ensure that all package handover notes give accurate information including any special instructions (e.g. files / folders to delete, directory set up and access rights etc.
- f) To work with the Integration team during the processing of delivery.

Integration Team commitments to 4LS

- g) To raise calls for any software delivery issues.
- h) To check software delivery including each package handover note.
- i) To ensure that all dependant packages are integrated together as per Release Note.

Commitments between INFREL DEV and Counter 4LS Team

- INFREL Dev package all Counter deliveries for distribution to the Live Branches and for software catch-up for spares, prior to LST testing. As such they require the handover notes from 4LS to provide the correct level of information including how to roll back the change and notification of any errors which maybe encountered during installation.
- INFREL Dev will facilitate the delivery of a release into the live estate. INFREL Dev has limited commitments to 4LS.
- INFREL Dev may raise a Peak on the handover if the information is not adequate

Commitments between CTR, BAL, Datacenter Audit, Host and EM Sysman Teams

- Audit: Key commitment of 4LS to audit is to ensure that messages between Counter and BAL and other 4LS teams are controlled for Audit purposes. These messages are tracked and therefore it is essential that they don't change without prior agreement and coordination with the Audit team.
- Host Reference Data Team: 4LS and Host Ref data must pre approve any reference data changes before they are packaged into a release.
- Host Database Team: The Host Database team will have the commitment to deploy database patches onto the CIT RIG, whilst maintaining a patch register and being responsible for archiving and DBA activity on the CIT RIG.



-
- GDC 4LS Rig runners will pick up any changes to Agent with updates from the HOST team provided via Dimensions
 - Where required 4LS teams will liaise with Estate Management teams as determined through maintenance operations.



Operational Level Agreement HNGx Application 4th line support

**FUJITSU RESTRICTED (COMMERCIAL IN
CONFIDENCE)**





Appendix C – 4LS Development Infrastructure Support

Operating system configuration

4LS will implement:

- Any Goldbrick standards
- Swap file and dump file configuration
- Operating System parameters and settings for individual system components
- RAID settings
- System configuration policies

Hardware and Event Monitoring

4LS will proactively monitor event log files relating to hardware created either by the Operating System or by the hardware manufacturer's logging system. 4LS will take remedial action in response to reported failures or warnings. 4LS will raise Incidents on any third parties using the peak system, where this is necessary, to resolve a problem that is related to the Supported System. 4LS will manage any site visits by the third party's engineers.

Third party management

4LS will manage any third party involvement in the Supported System. This will include raising Incidents and escalating them to the third parties. Strict controls will be used to ensure that any changes that third parties make to the Supported System meet the requirements of both the HNGx service and Fujitsu.

Operating system housekeeping

4LS will carry out housekeeping tasks as required including:

- Deleting temporary files
- Trimming event log files
- Maintaining task schedules
- De-fragmenting disks
- Where configured, managing the Active Directory of Windows 2000 and Windows XP,
- Deleting and archiving Application Data where there is an agreed instruction from the Customer or Application vendor to do so
- 4LS will regularly tidy up any system log files, ensuring that the file system thresholds are kept to a manageable level. 4LS will add crontab entries to the relevant UNIX administration accounts to automate housekeeping routines as appropriate.

4LS will carry out each of these tasks according to a schedule to be agreed with 4LS management.

Problem diagnosis and resolution

4LS will endeavour to diagnose and resolve any Incidents related to the 4LS development environments raised by other support units, the customer or by the EM.

The resolution may take the form of:

- Provision of a known repair
- Escalation to third party if the Incident has not been raised before
- Circumvention of the problem until such time as a permanent solution is available



Backup and restore

4LS will conduct regular backup and recovery activities of its underpinning data repositories and server environments that are used to deliver the 4LS service.

- Ensure the successful completion of backups and respond to backup failures raised through the monitoring systems raising appropriate incident calls
- Recover data from the most recent backup set in the event of data loss.
- Test the successful restoration of backups at regular intervals where the account has provided a suitable test environment to carry out this activity

Operating system patch management

4LS will maintain the operating system at the patch level in accordance with the HNGx patch management policy .

Anti-virus software maintenance

4LS will maintain anti-virus software on the Supported System to the latest virus signature.

Capacity monitoring

4LS will proactively monitor the Capacity of the Supported System so that issues can be addressed before they become critical and affect the availability and performance of the Support System. Fujitsu will raise an appropriate Request for Change with POA Operations to implement corrective actions should any problem areas be identified.

Recording service history

Fujitsu will maintain records of all changes made to the supported infrastructure during the lifetime of the Service. A summary of the most important changes will be included in a monthly Service Report to the POA Applications Service Manager.

GDC 4LS Development Infrastructure Support

Firewall Management

4LS GDC will be responsible for the management of 4LS GDC firewalls. The firewall will be housed within the facility of GDC, currently in India at Bangalore and will be confined within the secured GDC POA-4LS server room. The IT Support group, in collaboration with GDC management for POA & 4LS will assign a team specifically to cater towards this service.

Key responsibilities include:

1. Monitoring & Reporting of Firewall

- Monitoring of availability
 - Configuring through SNMP
 - Monitoring through Orion (Solar winds)
- Setting up of SYSLOG server
- Capturing of the Log for any investigation purpose



- Update to POA team any anomalies that are found
- Monthly report for availability

2. Patch management (vendor –released patch)

- Evaluating the patch
- Testing of the patches
- Implementation of the patches

3. Backup

The support will include backing up of configuration files/data on the firewall

4LS Counter build

Full counter rebuilds will be required from time to time on HNGx and as part of this process it is essential that Red Pike is removed from the build before it is sent out of the UK to the GDC 4LS Teams.

The attached process **MUST** be followed for all new counter rebuilds being sent to the GDC 4LS Teams. Essentially, the process is that encryption is switched off with the RED Pike binary for Utimaco VPN removed.

<START>

Remove Red Pike from Utimaco VPN on Counters

Version 0.4 Mark Jarosz 10th July 2009

Step 1 Configure Counter not to reference Red Pike and switch off encryption

Edit C:\WINNT\sgvpn.ini

Replace

EncryptionOnSend=USER1

KeyEncryption1=USER1

EncryptionOnStartup=1

By

EncryptionOnSend=IDEA

KeyEncryption1=IDEA

EncryptionOnStartup=0

Step 2 Sign Policy File



From Command line;
Svpntstn function 2 then 0 then 99

Step 3 on Counter deregister RedPike

From Command Line;
gssetn -unregister US1
gssetn -register IDE

Step 4 Reboot

VPNADMIN->Info
Observe that list of installed algorithms does not include USER1
Also that it includes IDEA CBC

Step 5 Remove Red Pike Object

Sdelete -p 3 WINNT\System32\Drivers\GSEUS1m.sys

Reboot and confirm (no blue screen) and no red events in security event log

<END>

The HNGX system test team (LST) are responsible for applying the Red Pike removal process to any new counter builds before shipping it via CD to the 4LS GDC Service Delivery Manager. 4LS GDC RIG Runners will then complete the build