FUJ00001419



# 2. SERVICE ARCHITECTURE

## 2.1 SERVICE INFORMATION FLOWS

Figure 2-1 shows the Pathway-centric view of the information flows between Pathway and entities external to Pathway.

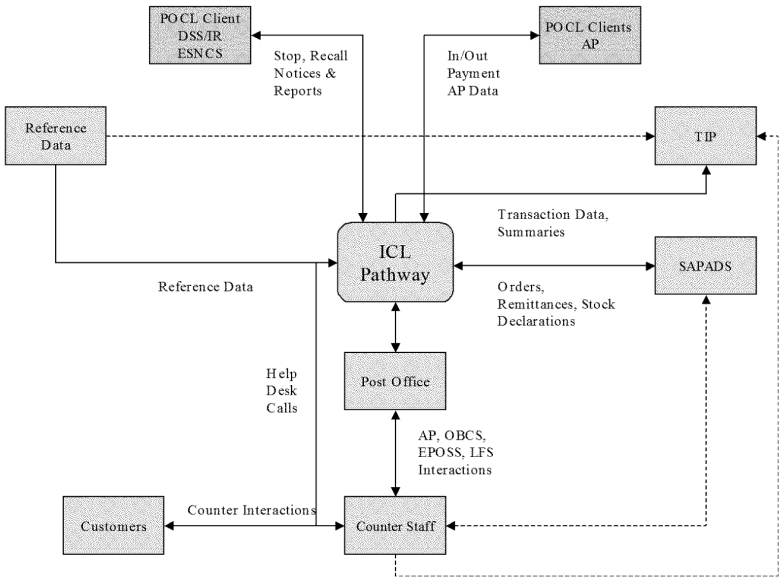


*Figure 2-1: Pathway Service information flows*

The dotted lines represent significant information flows that are outside of the Horizon system.

Many of the information flows are program-based, but some are paper- or voice-based. For example:

- A customer paying a bill is served at the counter. The Pathway AP and TPS service will effect the logical completion of the information flow by notifying both the POCL client and the POCL transaction accounting system TIP.
- A customer collecting his benefit by way of a bar-coded order book will be able to do so because the book is not present on the stop list that ICL Pathway has constructed from information supplied by ESNCS and has made visible to the OBCS application. Pathway will subsequently complete the end-to-end flow by notifying ESNCS

FUJ00001419



of the amount paid and notifying TIP that the post office made the payment.

- A post master may encounter a counter equipment failure and will speak on the telephone to the Pathway Horizon System Help Desk (HSHD). The HSHD will complete the logical information flow by arranging for an engineer to attend and rectify the fault.

## 2.2 PATHWAY SERVICE COMPONENT RELATIONSHIPS

Figure 2-2 shows how the total Pathway service is divided into its major service elements and the relationships between them, and the program-based entities within POCL.

It also illustrates how the principal program information flows referred to above are mapped between the service elements. For example:

- The stop list flow starts at ESNCS. OBCS Host transfers stop list entries to TMS, which thus become visible to OBCS Counter. If a customer book is not stop-listed the OBCS Counter controls the payment process and records the transaction within TMS. OBCS Host will notify ESNCS of the amount paid and the post office accounting routines within EPOSS will notify POCL's TIP system of the transaction.
- The bill payment flow proceeds from the APS or EPOSS service to the recipient POCL client. The post office accounting routines within EPOSS will notify POCL's TIP system of the transaction.

FUJ00001419



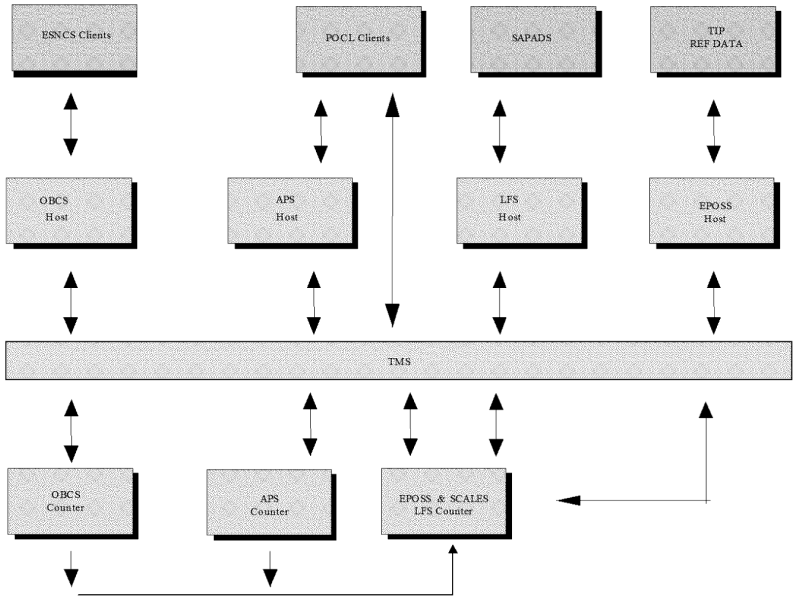


*Figure 2-2: Pathway major service component relationships*

## [REMOVED]

## 2.4 BUSINESS CONTINUITY

### 2.4.1 CONTINGENCY

[R830]

Pathway has developed the contingency arrangements that are used to ensure continuity of service, as described in R830 and as defined in Section 4.1.6, *POCL Contingency Services.*

Pathway has defined detailed contingency plans developed from jointly developed impact and risk assessments. They describe the contingency actions and their time-tabling and set standards for testing including regression testing. See *Business Continuity Framework* and subsidiary references.

### 2.4.2 PATHWAY BUSINESS CONTINUITY

Pathway has developed and implemented procedures to ensure

FUJ00001419



continuity of its own operation, see *Business Continuity Framework*.

## 2.5 SECURITY INFRASTRUCTURE

### 2.5.1 INTRODUCTION

[R698]

Pathway has established a security infrastructure that minimises and controls liabilities to itself and POCL as specified in R698. The Pathway Security Policy is described in *ICL Pathway Security Policy* and the corresponding procedures in *Security Management Procedures.* Issues relating to data confidentiality, integrity and access control are described in the *Security Functional Specification* and *Access Control Policy.*

### 2.5.2 FRAUD RISK MANAGEMENT

[R698, R829, R832, R895]

The management of fraud risk within the Service Architecture is described in *ICL Pathway Security Policy* and in *Security Management Procedures.* Fraud risk may also be managed through the provision of Management Information System (MIS) reports. In addition, a fraud monitoring system, to profile certain irregular encashment patterns and identify potential fraud incidents is provided, see below

Pathway's policy is to identify and minimise the risk of fraud within the Pathway system. However, Pathway recognises that the threat of fraud incidents exists inside and outside Pathway's responsibility.

Of particular concern is the specification of procedures followed by POCL staff in an outlet automated with Horizon. Agreed procedures associated with the Horizon automated system are documented in *Processes & Procedures Descriptions* including *CSR+ Logistics Feeder Service: Processes And Procedures Description.*

Pathway's strategy is to identify high risk situations and adapt systems as necessary to:

- Minimise fraud exposure within the Pathway solution
- Provide information service to POCL to aid fraud investigation and to minimise fraud

The information provided is:

- Information to aid in the investigation of actual fraud incidents

FUJ00001419



- Certification relevant to operation of the system as required by Police & Criminal Evidence (PACE) Act, 1984 and equivalent legislation as required by the territory of operation (R829).
- Information for the investigation of system boundary related incidents and trends; for example, counter staff-related fraud with the aim of developing improved procedures
- Analysis of incidents and trends within Pathway's immediate control, to improve its systems

#### 2.5.2.1 MANAGEMENT INFORMATION SYSTEM REPORTS

[R837, R894, R914]

The standard MIS reports are defined in *POCL MIS Reports*

*[DN: This document is intentionally empty.]*

Ad hoc reports are available for EPOSS and the HSHD.

#### 2.5.2.2 IRREGULAR ENCASHMENT PATTERNS

[R895]

The Service Architecture is capable of monitoring and reporting irregular encashments.

Information is shared with POCL Audit/Security/Operations when it relates to a post office.

Daily reports are provided of transactions at outlets that have been notified to Pathway as temporarily out of commission, that is temporary and emergency closures.

## 2.6 DATA PROTECTION ACT

[R938]

Pathway is responsible for ensuring that any information supplied under the Data Protection Act is accurate and that assurances can be given as to the integrity of that information.

Pathway is responsible for delivering any information requested under the Data Protection Act to the requesting body, or person as appropriate.

The Data Protection Act 1984 came into effect on 11 November 1987 and the Data Protection Act 1998 on 24 October 1998. Pathway ensures that all subsequent alterations and reviews to this law are integrated and adhered to.

FUJ00001419



Pathway records all written requests for a data protection print from a customer or representative within five (5) days of receipt of the request in respect of data held on behalf of POCL.

All information provided under the Act is made available to facilitate inspection.

Details of a request and response made under the Act will be retained consistent with the Act's requirements.

## 2.7 OPERATIONAL AUDIT

[R472, R697, R699, R829]

The POCL Service Architecture provides for audit of its operation by auditors accredited by POCL and POCL's commercial Clients. The composition of the audit trail and its arrangement into audit tracks, appropriate to the roles and access rights of individual auditors, and the maintenance of, and access to, these tracks is described in *Audit Trail Functional Specification*.

The systematic controls inherent in the Pathway solution are described in *Solution & Service Reconciliation*.