FUJ00152171

Document Title:	Production of System Information for Evidential Purposes
Document Type:	Procedure
Release:	N/A
Abstract:	Requirements and procedure for the production of evidential information to support potential prosecutions and procedure for the creation of Witness Statements.
Document Status:	DRAFT
Originator & Dept:	Graham Hooper
Contributors:	Tony Brown, Chris Billings
Reviewed By:	Dave Groom, Chris Billings, Tony Brown
Comments By:	
Comments To:	Document Controller & Originator
Distribution:	ICL Pathway Library, Graham Hooper, Chris Billings

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	30-1-00	Initial Draft	

0.2 Approval Authorities

Name	Position	Signature	Date
Martyn Bennett	Director of Quality		

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001			ICL Pathway Document Template	PVCS
PD 0008:1999		1999	Legal Admissibility and Evidential Weight of Information Stored Electronically	BSI
IA/PRO/003			Conducting Data Extractions at CSR+	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

0.5 Changes in this Version

Version	Changes

0.6 Changes Expected

Changes

0.7 Table of Contents

1.0 Introduction

Prima facie evidence to be presented in support of criminal prosecutions is obtained solely from the Horizon System Audit Server. This computer output is admissible in evidence provided that the integrity of the system can be demonstrated if required. On some occasions it may be necessary to provide "honest" certification of computer generated evidence or provide "expert" witness.

There is an additional requirement to produce witness statements in support of Post office instigated prosecutions.

2.0 Scope

This process describes the production of computer evidence originating within the Horizon system to support criminal prosecutions in England, Wales and Northern Ireland. This process also identifies secondary evidence, which may be required to demonstrate the integrity of the system and the information contained within it.
This process also describes the required content of witness statements produced in support of evidence submitted to the Courts.

3.0 Production and Retention of Computer Evidence

4.0 Certification

4.1 Certificates

Traditionally, PACE certificates are signed by a senior member of the Computer Operations staff responsible for managing the computer installation and its associated networks. ICL Outsourcing performs this role as a managed service for ICL Pathway, and it is assumed that the information required for their assurance is already available to them in day-to-day operational documentation and as management information - DN Outsourcing (Les Fereday) to provide more appropriate wording.

The certificate (see example at Appendix A) contains a declaration including the statement "*I sign this certificate knowing that I shall be liable for prosecution if I have stated in it anything which I know to be false or do not believe to be true*", it is therefore in his rational self-interest to ensure a) that the logs are adequately comprehensive and b) that they are investigated thoroughly.

4.2 Certification Process

The manager of the ICL Pathway Fraud Risk Management team, or his deputy, will advise a nominated member of ICL Outsourcing of the relevant dates and times for which a PACE certificate is required. The ICL Outsourcing nominee will consult operational records pertaining to computer and network operations on the dates and times advised, in order to satisfy himself that the certificate can be signed with confidence. A statement should accompany the certificate to the effect that additional (supporting) evidence to uphold the certificate can be produced if so desired. To offer all the evidence without it being requested would only serve to flood the courtroom with documentation.

5.0 Supporting Evidence

5.1 Requirement

In order to demonstrate the integrity of a Horizon PACE certificate for the Benefit Payment Service, it is necessary to describe the information flow from CAPS to OPS and from OPS to the FCMS and to illustrate where cryptographic and integrity protection are applied.

5.2 Types of Evidence

Given the size and complexity of the Horizon system, it is conceivable that the integrity of the PACE certificate will be challenged by Counsel in order to discredit a prosecution. If it is not possible to demonstrate the certificate's integrity to the Court's satisfaction, a very dangerous precedent will have been set and all subsequent prosecutions will be automatically jeopardised. However, the corollary is also true and a successful demonstration of honest certification will stand all subsequent prosecutions in good stead.

Comprehensive records pertaining to the site(s), services and individuals concerned should be able to be produced for all material times. These records will serve to show that the relevant services were available at all material times, were operating properly and had not been used inappropriately.

This secondary evidence should include, but is not restricted to, the following (list to be confirmed following consultation with relevant expert):

- An external Auditor's certificate of data integrity;

- Logs of calls to the Horizon System Helpdesk and the Payment Card Helpline detailing incidents of error, inaccuracy or malfunction pertaining to the sites, equipment, services and individuals concerned;
- A log of ISDN ‘ping’ records which demonstrate the availability of network communications between the affected site(s) and the Data Centre;
- Operational logs and shift handover documentation to demonstrate consistent operation and availability of the service;
- Secure NT, Dynix and SecurID definitions;
- Testimony from expert witnesses stating that, in their experience similar incidents have never happened or, if they had, that they would be reflected in the relevant audit log.

6.0 Witness Statements

6.1 Statements in support of Data Extractions

6.2 Statements in support of System Integrity

7.0 Annex A

Witness Statement

CJ Act 1967, s.9: MC Act 1980, ss.5A(3)(a) and 5B: MC Rules 1981,r.70)

ent of: ____
Age if under 18: ___________ (if over 18 insert 'Over 18')
Occupation: ___________________

This statement (consisting of 4 pages, each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything I know to be false or do not believe to be true.

Dated the day of 2001
Signature: ___________________

I have been employed by ICL Pathway for x months. I have been employed as IT Security Analyst responsible for Audit Data Extraction and IT Security. I have working knowledge of the computer system known as Horizon, which is the computer system used by Post Office Counters Ltd. I am authorised by ICL Pathway Ltd to undertake extractions of audit data held on the Horizon system.

Prior to the system being introduced, Post Offices ran a weekly manual or electronic cash balance on a counter register system. This was the system in which all transactions performed by counter clerks would be entered on a daily basis onto their weekly balance sheets or input into their computer systems. At the end of the accounting period they would amalgamate the daily transactions, include their stock and cash on hand and arrive at a balance.

A new system has been introduced within the Post Office Counters Offices and this is known as Horizon. Each counter position has a computer terminal, a visual display unit and a keyboard and printer. This individual system records all transactions input by the counter clerk working at that counter position. Each clerk logs on to the system by using a series of passwords. The transactions performed by each clerk, and the associated cash and stock level information are recorded by the computer system in a stock unit. Once logged on, any transactions performed by the clerk must be recorded and entered on the computer and are accounted for within the user's allocated stock unit. The Horizon system consistently records time in GMT and therefore takes no account of Civil Time Displacements. The clock incorporated into the desktop application on the counter visual display units is however configured to indicate local time.

The Horizon system provides a number of daily and weekly records of all transactions input into it. It enables Post Office users to obtain computer summaries for individual clients of Post Office Counters Limited e.g. National Savings Bank, Giro, Driving Licence Agency and Pension and Allowances. The Horizon system also enables the clerk to produce a weekly balance of cash and stock on hand combined with the other transactions performed in that accounting period.
The system also allows for information to be transferred to the main accounting department at Chesterfield in order for the Office accounts to be balanced.

Signature………………………………… Signature witnessed by……………………….

Continuation sheet No.
Continuation of Statement of:____

The Post Office counter processing functions are provided through a series of counter applications: the Order Book Control Service (OBCS) that ascertains the validity of Benefit Agency order books before payment is made; the Electronic Point of Sale Service (EPOSS) that enables PostMasters to conduct general retail trade at the counter and sell products on behalf of their clients; the Automated Payments Service (APS) provides support for utility companies and others who provide incremental in-payment mechanisms based on the use of cards and other tokens and the Logistics Feeder Service (LFS) which supports the management of cash and value stock movements to and from the outlet, principally to minimise cash held overnight in outlets.

The counter desktop service and the office platform service on which it runs provides various common functions for transaction recording and settlement as well as user access control and session management. Information from counter transactions is written into a local database and then replicated automatically to databases on all other counters within a Post Office outlet. The information is then forwarded over ISDN (or other communication service) to databases on a set of central Correspondence Servers at the ICL Pathway Datacentres. This is undertaken by a messaging transport system within the Transaction Management Service (TMS). Various systems then transfer information to Central Servers that control the flow of information to various support services including the Pathway Data Warehouse where an historic record of all data is stored.

Details of outlet transactions are normally sent at least daily via the system. Details relating to the outlet's stock holding and cash account are sent weekly. Details are then forwarded daily via a file transfer service to the Post Office accounting Department at Chesterfield and also, where appropriate, to other Post Office Clients.

An audit of all information handled by the TMS (the TMS journal) is taken daily by copying all new messages to archive media. This creates a record of all original outlet transaction details including its origin - outlet and counter, when it happened, who caused it to happen and the outcome. The TMS journal is maintained at each of the ICL Pathway Datacentre sites and is created by securely replicating all transaction records that occurred in every Outlet. They therefore provide the ability to compare the audit track record of the same transaction recorded in two places to verify that systems were operating correctly. All exceptions are investigated and reconciled. Records of all transactions are written to Digital Linear Tape (DLT) audit archive media. When information relating to individual transactions is requested, the tapes are loaded onto Audit Servers and the data extracted via Audit Workstations. Information is presented in exactly the same way as the data held in the archive although it can be filtered depending upon the type of information requested.

Where data is stored on a computer, there are no reasonable grounds for believing that the information is inaccurate because of improper use of the computer, and at all material times the computer was operating properly or if not, any respect in which it was not operating properly or was out of operation was not such as to affect the production of audit records or accuracy of their contents.

Signature…………………………. Signature witnessed by………………………

Continuation sheet No.

Continuation of Statement of:____

The integrity of audit data is guaranteed at all times from its origination, storage and retrieval to subsequent despatch to the requester. Controls have been established that provide assurances to Post Office Internal Audit (POIA) that this integrity is maintained.

During audit data extractions the following controls apply:

1. Extractions can only be made through the three Audit Workstations (AWs), which exist at ICL Pathway, Forest Road, Feltham Middlesex and the two Data Centres at ICL, Quayside Centre, Westwood Park, Wigan WN3 5GB and ICL, Bridal Road, Bootle GIR 0AA . These are all subject to rigorous physical security controls appropriate to that location. Specifically, the Feltham AW – where most extractions take place – is located in a secure room subject to proximity pass access within a secured ICL site.
2. Logical access to the AW and its functionality is controlled by dedicated Logins, password control and utilises the Microsoft Windows NT and Pathway security features defined in the overall Horizon security policy.
3. All extractions are logged on the AW and supported by documented Requests for Information (RFIs), authorised by nominated persons within POIA. This log can be scrutinised on the AW.
4. Extractions are only made by authorised individuals.
5. Upon receipt of an RFI from POIA they are interpreted by Pathway Internal Audit. The details are checked and the printed request filed.
6. The required files are identified and marked using the dedicated audit tools.
7. Using the above information the relevant archive tapes are identified.
8. A request to load the tapes at the Data Centre is made.
9. Checksum seals are calculated for audit data files when they are written to DLT (Digital Linear Tape) and re-calculated when the files are retrieved.
10. To assure the integrity of the audit data while on the DLT the checksum seal for the file is re-calculated by the Audit Track Sealer and compared to the original value calculated when the file was originally written to the DLT. The result is maintained in a Check Seal Table.
11. The specific RFI details are used to obtain the specific data.
12. The files are copied to the AW where they are checked and converted into the file type required by POIA.
13. The requested information is copied onto removal CD media, sealed to prevent modification and virus checked using the latest software. It is then despatched to the POCL (Post Office Counters Limited) Audit Manager or Investigations Manager using Royal Mail Special Delivery. This ensures that a receipt is provided to ICL Pathway confirming delivery.

Signature…………………………… Signature witnessed by……………………….

Continuation sheet No.

Continuation of Statement of:____

RFI *** was received on dd/mm/yyyy and asked for information in connection with the Post Office at *************** - FAD ******. **I produce a copy of RFI *** as Exhibit ZZ1**
On various dates and at various times between dd/mm/yyyy and dd/mm/yyyy, I undertook extractions of data held on the Horizon system in accordance with the requirements of RFI *** and followed the procedure outlined above.
I produce the resultant CD as Exhibit ZZ1.

The report is formatted with the following headings:
ID – relates to counter position
User – Person Logged on to System
TxnData.Container
TxnData.Start.Date – Date of transaction
TxnData.Start.Time – Time of transaction
TxnData.SessionId – A unique string relating to current customer session
TxnData.TxnId – A unique string relating to current transaction
TxnData.Mode – e.g. SC which translates to Serve Customer
EPOSSTransaction.ProductNo – Product Item Sold
EPOSSTransaction.Qty – Quantity of items sold
EPOSSTransaction.SaleValue – Value of items sold

The CD (Exhibit ZZ1) was sent to the Post Office Investigation section by Recorded Delivery on dd/mm/yyyy.

Signature…………………………… Signature witnessed by………………………