POL00125569

Initial Review: Proposal for investigation into the integrity of the Post Office Horizon Online accounting system

Prof. Jeff Kramer

Dr. Naranker Dulay

Imperial College Consultants
3rd Floor, 58 Prince's Gate
Exhibition Road, London SW7 2PG, UK

Date: 26 June 2014

Background

1 The Horizon Online accounting system is a point of sale and back-office accounting system which provides access to a number of government, financial, telephony, Royal Mail and other private sector services from Crown Offices and sub-post office branches. Following concerns regarding its integrity, and a report commissioned from Second Sight Support Services Ltd. which identified some defects, the reputation of the Horizon system has been damaged. Post Office Ltd. wish to restore confidence in the system and provide a basis for analysing and responding to anomalies and challenges.

System Complexity

2 There are apparently around 350 Crown Offices and over 11,800 sub-post office branches located across the country from which over 6 million of transactions are conducted every day. Horizon is required to record all transactions at every post office counter across the country, and to interface with government and private service systems. The system is thus highly complex, widely distributed and expected to be robust and reliable.

3 Can such complex systems ever be determined to operate "without defect or error, securely, robustly and with integrity"? This is simply not possible. No complex system can be certified as bug (defect) free. Through testing and analysis, it is possible to show the presence of bugs, but not their absence[1], particularly in systems such as Horizon which include complex requirements such as distribution, parallelism, and subsystem service interactions. For instance, distribution introduces the problems of failures of parts of the system while other parts continue to operate and of maintaining consistency between local and remote data; multiple machines operating in parallel can cause concurrency problems of interference and non-determinacy (different results depending on the order or timing of computations); and service interactions are dependent on the correct behaviour of protocols and services. Moreover, user interactions and (mis)interpretation of system operation can exacerbate the situation.

Proposal

4 How then should an investigation into the integrity of Horizon proceed? The aim should be to provide a report on the extent to which the system is fit for purpose, supports integrity and robustness, and facilitates maintenance and upgrade. A

[1] Dijkstra: Turing Award Lecture 1972

particular focus of the report should be the facilities in place for the production of audit trails which accurately and reliably record the system actions at a sufficient level of detail so as to support analysis of system performance, identification of potential defects and evidence for resolution of disputes.

5 Overall system: study the interactions between the central system and local branch sub-systems and the interaction with external services.

6 Fit for purpose: examine the extent to which the Horizon system provides a usable and useful service to users and sub-postmasters, particularly for financial transactions including confirmation of successful and unsuccessful transactions.

7 Integrity and Reliability: Examine the means for transaction auditing, testing and bug reporting, including the means for transaction correction and data reconciliation.

8 Maintenance and update: examine the maintenance and update procedures, including the mechanisms for software update of the central servers and local terminals, for version control and for testing.

9 Disputes: examine the provision for audit trails and support for transaction analysis when discrepancies occur, including sufficient event granularity to provide clear details of events for both users and system providers.

10 Case studies: examine a number of diverse case studies which can be used to illustrate system operation and demonstrate the attributes above: fit for purpose, support for integrity and reliability, performance of maintenance and update and audit trail information and analysis for dispute resolution.

Phase 2 - Initial Steps

11 The following steps will be undertaken at the start of phase 2.

- Clarification by POL on which version(s) of the Horizon system should form the basis of the report.
- Assignment by POL of one or more technical experts to liaise with ICON.
- Initial meeting with POL technical experts to review the Horizon system.
- POL to provide a spreadsheet listing all documents relating to the Horizon system, to include document title, reference, type, release, abstract, status, date created, date last updated.
- POL to provide a spreadsheet listing all technical documents related to POL evidence of system operation in Horizon disputes/POL prosecutions.

- Visit to the Horizon data centre in Northern Ireland.
- Visit to a Crown Office and a Sub-post office branch.
- Visit to Fujitsu Development Centre.
- Spreadsheet of all documents relating to the Horizon system, to include document title, reference, type, release, abstract, status, date created, date last updated.
- Spreadsheet of all documents related to disputes.

Phase 2 - Documents Requested

12 Development Process and Procedures:

- Details of the development process and procedures at POL and Fujitsu responsible for Horizon.

13 Horizon System:

- Description of software and hardware architecture of the Horizon system including software and hardware located in branches.
- Description of the external systems that interact with the Horizon system and how they interact with Horizon.
- Description of applications running in branches, including details of what information can be checked and printed at a branch by Sub-Postmaster, including transaction and event logs.
- Description of the interaction, transaction and communication system used between branch Horizon machines and the central Horizon system.

14 Integrity and Reliability:

- Detailed description of how Horizon ensures integrity and reliability.
- Detailed description of the support Horizon provides for auditing, including details of facilities for producing audit trails of local and central events and transactions, and including some typical examples.
- Description of the development procedures used, including testing, deployment. Examples of tests used to ensure integrity and reliability.
- Description of the Horizon reconciliation and transaction correction mechanisms and procedures.

15 Maintenance:

- Details of the process used to update software on central servers and on branch terminals.
- Details of the main revisions/updates made to the Horizon system in the past 5 years.
- Details of bugs/defects fixed in the last 5 years.

16 Disputes:

- Dispute procedures and history of disputes plus outcomes.
- Details of documents requested and made available to Second Sight for their investigation.
- Copies of Second Sight documents supporting their Interim Report.

Phase 2 - Proposed Workplan

17 Summary of main activities and estimate of days required:

Description	**Estimate of the consultancy days required from Professor Kramer and Dr Dulay**
Study and analyse material above	±18
Visits to Horizon, data centre, Fujitsu development centre, Crown and sub-branch PO	±6
Identify any issues and potential for errors and failures based on case studies and documentation	±6
Conduct particular investigations necessary to confirm issues and validate the integrity of Horizon	±10
Report preliminary results and recommendations on Horizon and, if necessary, define work for final phase.	±10
Total Consultancy Days	**±50**