POL00029281

Document Title: Major Incident Report for Online Transaction Failures on Monday 16th February 2004

Document Type: Report

Release:

Abstract: Report on loss of all on-line services at 920 branches on Monday 16 February

Document Status: For approval

Originator & Dept: Peter Burden - POA Customer Service

Contributors: Mike Stewart, Mark Jones, Bill Mitchell

Internal Distribution: As per section 0.2 plus Pete Jeram, Liam Foley, Colin Lenton-Smith, Ian Lamb, Richard Brunskill, Ian Morrison, Bill Mitchell

External Distribution: Ruth Holleran, Dave Hulbert

Approval Authorities: *(see PA/PRO/010 for Approval roles)*

Name	Position	Signature	Date
Martin Riddell	FS POA Service Director		

POL00029281

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	17/2/2004	Initial Draft	
(0.2	18/2/04	Update following initial POA comments)	
0.3	19/2/04	Interim draft for visibility to Post Office Limited	
0.4	26/2/04	Update on Corrective Action dates and issued to Martin Riddell for approval	

0.2 Review Details

Review Comments by :	
Review Comments to :	*Peter Burden+ Mike Stewart*

Mandatory Review Authority	Name
See Review Role Matrix in PA/PRO/010	
Fujitsu Services Post Office Account	Steve Parker
Fujitsu Services Post Office Account	Bill Mitchell
Fujitsu Services Post Office Account	Martin Riddell
Fujitsu Services Post Office Account	Mark Jones
Fujitsu Services Post Office Account	Tony Wicks
Fujitsu Services Post Office Account	Mike Stewart
Fujitsu Services Post Office Account	Simon Fawkes
Fujitsu Services Post Office Account	Dave Tanner
Fujitsu Services Post Office Account	Richard Brunskill
Fujitsu Services Post Office Account	Julie Welsh
Fujitsu Services Post Office Account	Dave Law
Optional Review / Issued for Information	

(*) = Reviewers that returned comments

0.3 Associated Documents

POL00029281

Reference	Version	Date	Title	Source

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
BCM	Business Continuity Manager
CS	Customer Service (in POA)
DM	Duty Manager
FAD	Financial Accounts Division (Post Office)
HSH	Horizon System Helpdesk
IVR	Interactive Voice Response
NB	Network Banking
PM	Problem Manager
PMDB	Problem Management Database
PO	Post Office
POA	Post Office Account
POL	Post Office Limited
SSC	Software Support Centre (Third-line support)
TSD	Technical Services Desk
VPN	Virtual Private Network

0.5 Changes in this Version

Version	Changes
0.1	This is the first draft
0.3	Updates following further comments by POA staff
0.4	Updates on Corrective Action dates

POL00029281

0.6 Changes Expected

Changes

POL00029281

0.7 Table of Contents

POL00029281

1.0 Introduction

This document reports on the issues that arose from a major incident affecting on-line transactions that occurred on 16 February 2004.

This report covers:

- How the problem came to light
- The impact on the branch service
- The investigation
- The resolution
- The root cause
- Actions to prevent recurrence

2.0 Scope

The scope of this report is the major incident that occurred on Monday February 16th that affected all online transactions at 920 Branches.

3.0 Management Summary

On Monday 16th February 920 Branches were unable to perform online transactions. The problem was caused by the expiry of keys on the VPN Servers in the Data Centre. The key expired at midnight on 14th February. Any Branch that needed to reconnect to the Data Centres after that time was affected by the problem

The HSH took 500 calls on the problem and a further 597 calls were abandoned.

The Engineer Service as provided to Branches was also impacted - details are in Section 4.1.1.

Initial investigation by support and development staff centred around cryptographic keys, because there had been an issue on Sunday with the expiry of the Key Disc on the VPN Loopback Work Station (an administration tool not required as part of live service). No problems were found (there were no system events to suggest any issues) and the investigations widened to look at the network. It was not until the middle of the day that the problem was diagnosed.

Following the production of new keys, the VPN servers at Wigan began to be rebooted from around 16:30 which allowed gradual restoration of on-line service to the affected Branches.

There are similarities between this incident and the Smart-card Acknowledgement Key expiry incident of 31st July 2002.

Although Post Office Limited were kept updated on the problem during the day, it was not possible to advise on how much of the estate was affected.

POL00029281

On the subsequent day (Tuesday 17th February) the estate was running normally. In the morning of the 17th the third-line support team were unable to contact 348 Branches but non-polled checks, monitoring of calls to the HSH and proactive calls made by HSH to Branches showed that in practice the estate was back to business as usual.

A set of corrective actions has been identified and they are listed in Section 7.

4.0 Description of the fault and service failure

4.1 Symptoms and Business Impact

4.1.1 Symptoms as seen by Branches

920 branches would have seen the "on-line services unavailable" message and were unable to undertake on-line transactions for all of (or in some cases the greater part of) the day. There would have been a corresponding impact on customers visiting those Branches.

The Engineer Service as provided to Branches was impacted in the following areas:

- Break Fix: Gateway PC calls could not be resolved. However peripherals faults received an engineer visit as normal and slave counter faults requiring a base unit swap received an engineer visit once it was confirmed that the Gateway at the branch was still in contact with the data centre
- ADSL hardware roll out: Out of 41 scheduled upgrades, 15 jobs were cancelled and rescheduled.
- OBC Branch Change: No “opens” were scheduled for this day, however 4 “counter increases” were cancelled and rescheduled to 17th February with the agreement of Post Office Ltd, NIET Chesterfield.
- Bureau de Change Upgrades: 14 Bureau de Change upgrades were scheduled and following discussion with Barry Evans, Post Office Ltd, the decision was taken at approximately 1.15pm to cancel 13 jobs (1 branch had been successfully upgraded).
- Data Retrieval: All data retrieval calls were suspended.

4.1.2 Symptoms as seen by Fujitsu Services

On Sunday 15th February a key expiry on the VPN loopback workstation was noted. No VPN Server events were generated at that time. Further immediate action was deemed not to be

POL00029281

necessary and, as the VPN loopback workstation is not business-critical, this was logged for resolution on Monday.

On 16th February a trend of calls to the HSH was noted shortly after 9.00 and the escalation process began. During the day HSH took 500 calls stating online services were unavailable. A further 597 calls were abandoned.

The issue identified on the 15th led to initial investigations into the problems experienced by the Branches being focussed in the area of VPN keys. However, no symptoms of key expiry on the VPN Servers were found during the first round of investigations by support and development staff.

4.2 Detailed explanation of the incident

Although not recognised at the time, the keys on the VPN servers expired on 14th February. Following this expiry any Branch which became disconnected from the data centres would not be successful in reconnecting and would thus not be able to perform on-line transactions.

A key expiry on the VPN loopback workstation (which does not form part of the live service) was noted on 15th February during a business continuity test where a VPN Server had been disconnected and then reconnected. This informed the first investigations on the morning of 16th February when the initial calls to the HSH, stating inability to perform on-line transactions, were received.

These initial investigations, which involved both support and development staff, did not locate the fact that the keys on the VPN servers had expired as there were no system events to suggest any issues. The scope of the investigation widened to encompass the network.

Following investigation during the morning it was established by CS Security, in checking back through their records from the time the keys were first installed, that the VPN server keys had in fact expired and that new keys needed to be generated. Due to a problem with the key generation workstation at Bracknell the Key Manager was relocated to Feltham and the work undertaken there.

At the end of the afternoon the VPN servers at Wigan were updated with the new key. The Bootle VPN servers were updated during the evening.

The number of Post Offices on the non-polled report overnight was normal for a Monday night. There were 31 calls to the HSH on the morning of Tuesday 17th February - of these 21 were cleared by a reboot and the rest went for resolution by Energis - again, normal business.

The picture was clouded by the fact that the third line support team were unable to contact 348 Branches when doing their check. However, checks by HSH and further work by SSC confirmed that there were not any on-going issues.

POL00029281

5.0 Incident Management

Date & time	*Avoidance, mitigation and resolution activities*	*Communication and escalation activities*	*Business Impact*
16/2/04			
9.07		*POA Duty Manager paged*	
9.10		*Richard Ashcroft (POL) called Tony Wicks and Mike Stewart takes the call*	*28 calls logged at HSH and 30+ abandoned (Master call - 167)*
9.25		*Mike Stewart updated Richard Ashcroft, but information is limited*	
9.25		*Peter Burden briefed Martin Riddell and Martin Riddell briefed Ruth Holleran*	
9.30	*Following initial investigations by NT support team, third line support are now involved*		
9.48		*POA Duty Manager advises POA senior managers*	
9.55	*Recommendation made to put an IVR message on the helpdesks*		*41 calls logged at HSH and 569 abandoned*
10.02	*Mike Stewart designated as Problem Manager*		
10.10		*Mike Stewart updates Richard Ashcroft*	*Lack of clarity as to how much of the estate is affected*
10.17	*Counter swaps as part of System Service are stopped*		
10.30			*160 calls logged at HSH and 570 abandoned*
10.45	*Scope of investigation broadened to include the network as support and development staff, although having looked at the VPN loopback workstation key expiry problem, have not found any underlying issues to cause the problems seen in the estate.* *CS Security team continue to focus on the key issue.*		

POL00029281

11.10		*Mike Stewart updated Richard Ashcroft to say that the network is now being looked at*	
11.20			*234 calls logged at HSH and 589 abandoned*
11.25		*Peter Burden updated Dave Hulbert (Post Office Limited)*	
11.30	*CS Security initiate generation of new key for VPN loopback workstation*		
12.30	*CS Security advise that key has expired on all VPN servers and Key Manager needs to relocate to Feltham to generate the keys as key generation workstation in Bracknell has a disc problem*		
13.00		*CS Security advised Post Office Limited Security (and liaison continued through the afternoon)*	
13.05		*Mike Stewart updated Richard Ashcroft*	
13.10		*Peter Burden updated Dave Hulbert*	
13.15	*Plan drafted for establishing the new keys at the data centre - Wigan at the end of the afternoon and Bootle later in the evening*		
13.30 +14.20		*Mike Stewart updated Richard Ashcroft*	
15.45	*New keys generated and sent to the data centre*		
16.05	*Rebooting of Wigan VPN servers with new key initiated*		
16.30	*Confirmation of successful reboot of first VPN server at Wigan*	*Mike Stewart updated Richard Ashcroft*	
17.18		*Peter Burden updated Dave Hulbert*	
17.30	*Four VPN servers at Wigan successfully rebooted*	*Mike Stewart updated Richard Ashcroft*	
18.10	*All VPN servers at Wigan rebooted*		*By the end of the day there had been 500 calls logged and 597 abandoned*
Over-night	*All VPN servers at Bootle rebooted*		

POL00029281

17/2/04			
7.00	*Third-line support initiate checks on the 920 Branches*		
8.45		*Peter Burden and Mike Stewart advise Dave Hulbert and Richard Ashcroft that the situation appears to be returning to normal*	
8.48	*Report shows 145 Branches out of full estate non-polled overnight.*		
9.00	*Third-line support advise that they cannot contact 348 of the affected Branches (Later noted that 12 of these were on the non-polled report)*		
9.15	*Information on the 348 sites and the days Non Polled passed to Richard Ashcroft*	*Mike Stewart phoned Richard Ashcroft*	
9.35			*22 calls to HSH advising that on-line service was not available*
9.55		*Richard Ashcroft phones Mike Stewart*	*Futher updates on Non Polled and checking on the 348 sites*
10.32	*List of 348 Branches is generated for subsequent provision to POL*		*31 calls to HSH*
10.45	*HSH to call sample of 348 to check their status*		
11.00	*List of 348 sites sent to Richard Ashcoft*	*Update also to Richard Ascroft on the first sample of HSH contacting the PMs*	
11.10	*7 Branches out of first 10 are OK, when called by HSH*		
11.45	*17 Branches out of first 20 are OK, when called by HSH*		
12.56	*32 Branches out of first 35 are OK, when called by HSH*	*Information passed to Richard Ashcroft by Mike Stewart, also informed him theat SSC are re-running the Ping check to all the 348 sites*	
13.02	*Third-line support "failure to contact" list now at 102*		
13.26	*Third-line support "failure to contact" list now at 69*		
14.13		*Peter Burden updates Dave Hulbert* *Mike Stewart Updates Richard Ashcroft Re the 69 sites of which*	

POL00029281

		HSH had contacted 35 of them and were now working through the remaining 34.	
15.30	*HSH have called half of Third-line support's latest list and all those Branches were OK*		

Senior management in POL were kept updated during the day.

6.0 Problem Management

The processes for problem management regarding escalation and communication were followed. However, there were a number of issues.

It took too long to diagnose the underlying problem. There were no system events that indicated that there was a problem with the keys on the VPN Servers.

Once diagnosed, there was a delay of some 30 minutes in the production of the new keys due to problems with the key generation workstation at Bracknell.

On Monday 16th Fujitsu Services were not able to advise Post Office Limited of the number of affected Branches. It was only possible to estimate the figure of 920 Branches after the problem was diagnosed.

The checking by third-line support staff on the Tuesday morning of the 920 Branches, by then known to have been affected on the Monday, took too long to enable timely information to be provided to Post Office Limited. Furthermore the result of the checks indicated that there were still problems in the estate, when in practice this was not the case.

Problem 455 has been logged on the Problem Management database for this incident.

POL00029281

7.0 Corrective Actions

Incident/problem Issue	*Action to be taken*	*By Whom*	*By When*	*Progress made*
CS/REP/148 (the Report on the Smart-card Acknowledgement Key Expiry Potential MBCI that occurred on the 31st of July 200)2 stated that in addition to local records, the expiry dates of all manual keys will be recorded on the KMS system to ensure that the Key Manager receives automatic prompts of impending key change dates. This action was completed for all manual keys in the 'live' service at that time, however, the VPN key was not included as this had not been released to the 'live service' at the time.	1. *Initiate an audit of all current cryptographic keys to ascertain their validity, renewal dates and refresh method.* 2. *Place all current manual cryptographic keys not already in automated notification on the KMS onto the system.* 3. *Develop / amend and implement process to move all new cryptographic keys from development into 'live' and add them to the KMS automated notification process.* 4. *Ensure that where possible key refresh dates are staggered between data centres / servers to improve resilience.*	*Bill Mitchell*	*Audit complete by 5th March 2004* *10th March 2004* *Draft process by 31st March 2004 and approved by 14th April* *31st March 2004 for VPN key.* *Plan for rest of keys by 31st March*	

POL00029281

Disc problems on the Certificate Authority Workstation (CAW)- key generation workstation - at Bracknell delayed investigation and resolution of the problem and forced the key manager into a fail over situation using the Feltham CAW.	*1. Investigate and implement repairs to the current Bracknell CAW.* *2. Investigate the upgrade / replacement of the Bracknell CAW.*	*Bill Mitchell*	*Completed 17 Feb 2004* *31st March 2004*	
Problem with the VPN server was not picked up during the business continuity test on 15th February due to the "clean" nature of the test	*Review Business Continuity scripts (essentially a continuation of the action in this area from CS/REP/177 (Incident on 5th January))*	*Bill Mitchell/Peter Burden*	*31st March 2004*	
Initial investigations on the morning of 16th February did not find any problems with the VPN servers	*A method of alerting that a VPN Server key has expired will be investigated*	*Simon Fawkes*	*31st March 2004*	
Fujitsu Services not able to advise POL of the Branches affected	*The implementation of the Softek reports is designed to cater for this - specifically in the case of Silver Branches*	*Dave Tanner*	*Early March 2004*	
It took too long for the third-	*Better estimates for Branch checks*	*Peter Burden*	*31st March 2004*	

POL00029281

line support team to check Branch status on 17th February	*to be established*			
The "failure to contact" list produced by third-line support on 17th February was not a fair reflection of the actual status of Branches	*The implementation of the Softek reports is designed to cater for this - specifically in the case of Silver Branches*	*Dave Tanner*	*Early March 2004*	