FUJ00232549

FUJITSU SERVICES

MAJOR INCIDENT REPORT

Ref: MI:
Status: Initial: V1
Owner:

Date of Incident	Time of Service Outage	Time Service Restored
8th February 2006	08:50	10:42

Service Impacted	Debit Card & ETU service experienced 100% transaction timeouts across the whole Post Office Limited infrastructure.

Scale of Impact: 100% loss of service for DCS and ETU was identified at 08:50 through the systems management toolset.

Investigation by the SSC (3rd line support) and development team immediately took place and service impact was identified as being due to 'Cryapi' key having expired.

A new key was applied to the affected servers in the Bootle data centre and full operational service was restored by 10:42 with both services running successfully through the Bootle data centre.

A decision was made upon the advice of our technical experts, that the new key will be applied to affected servers in the Wigan data centre through a controlled change process this evening.

Related References	Master Incident	Problem Record	No. of Linked Incidents
None	E-0602080145 E-0602080170		None

Previous Occurrence	MTTR	Action Required to Close
None	1hr 52 minutes	. Application of new 'Cryapi' security key

FUJ00232549

FUJITSU SERVICES

MAJOR INCIDENT REPORT

Ref: MI:
Status: Initial: V1
Owner:

What happened?

At 08:50 events were seen on Tivoli. The message, stated “cryapi key expired” for “key 44_3243_60119_10002”. SSC and SMC began investigations and a PINICL PC0131994 was logged.

At 09:03 it was reported that calls began to come into the HSD, and the POA Duty Manager was alerted. Immediately following this, further calls between the POA DM, SSC and SMC established that there was a 100% loss of transactions on DCS and ETU.

The SSC and development team were immediately diagnosing the problem and continued working in the background until a replacement key was ultimately created and successfully implemented to restore the service.

At 09:14 management escalation commenced throughout both POL and POA.

At 09:50 a technical bridge was invoked. This confirmed that the security key had expired. A resolution plan was confirmed in the 10:15 technical bridge.

At 10:45 it was confirmed that DCS and ETU services had returned to service at 10:42. This was following the updating of the security key at Bootle. The application of the same security key at Wigan is scheduled for 18:00.

The full impact of this incident is that between **08:50 and 10:42** there were a total of 23819 DCS and 31464 ETU transaction failures. It should be noted that numerous retries are typically attempted in such a situation.

The following shows the number of transactions experienced over the last four Wednesdays. Please note that there is typically an increased volume of transactions at the end/start of the month:

01/02/2006	**DCS**	**16080**	**ETU**	**18476**
25/01/2006		**8971**		**17973**
18/01/2006		**7948**		**17852**
11/01/2006		**7583**		**16841**

The comparison suggests several attempted transaction retries.

The transaction comparison between 08:00 and 16:00 for the last 4 Wednesdays is recorded as follows to indicate the expected transactions for the day:

01/02/2006	**DCS**	**115410**	**ETU**	**53555**
25/01/2006		**76829**	**ETU**	**50896**
18/01/2006		**67542**	**ETU**	**50644**
11/01/2006		**64956**	**ETU**	**49177**

By comparison on 08/02/2006 the totals from 08:00 to 16:00 were as follows:

DCS 53043 ETU 33252

FUJ00232549

FUJITSU SERVICES

MAJOR INCIDENT REPORT

Ref: MI:
Status: Initial: V1
Owner:

The Call Patterns to the HSD were as follows:

HSH 30 Minute SLA Conformance

	ACD Calls Offer	Total Ans Calls	Totl Call Aban	Avail to be Ans	Aban 40 secs	Abn >40 secs	**Abn > 40 SLA </=5%**	Ans 30 secs	**Ans < 30 SLA**
07:30	0	0	0	0	0	0	-	0	-
08:00	15	15	0	15	0	0	0.00%	15	100.00%
08:30	67	65	1	66	1	0	0.00%	65	98.48%
09:00	337	170	166	336	35	131	38.99%	72	21.43%
09:30	305	226	78	304	28	50	16.45%	47	15.46%
10:00	237	188	46	234	18	28	11.97%	71	30.34%
10:30	112	109	3	112	3	0	0.00%	106	94.64%
11:00	33	32	1	33	1	0	0.00%	32	96.97%
11:30	0	0	0	0	0	0	-	0	-
12:00	0	0	0	0	0	0	-	0	-
12:30	0	0	0	0	0	0	-	0	-
13:00	0	0	0	0	0	0	-	0	-
13:30	0	0	0	0	0	0	-	0	-
14:00	0	0	0	0	0	0	-	0	-
14:30	0	0	0	0	0	0	-	0	-
15:00	0	0	0	0	0	0	-	0	-
15:30	0	0	0	0	0	0	-	0	-
16:00	0	0	0	0	0	0	-	0	-
16:30	0	0	0	0	0	0	-	0	-
17:00	0	0	0	0	0	0	-	0	-
17:30	0	0	0	0	0	0	-	0	-
18:00	0	0	0	0	0	0	-	0	-
18:30	0	0	0	0	0	0	-	0	-
19:00	0	0	0	0	0	0	-	0	-
19:30	0	0	0	0	0	0	-	0	-
20:00	0	0	0	0	0	0	-	0	-
TOTAL	1106	805	295	1100	86	208	19.00%	408	37.09%

After initial enquiries int[illegible] a "manual" TK key had not been extracted [illegible] Card System Agent Servers (W[illegible]nd Bootle), before the previous key ex[illegible]

The existing (TK) key expired at approximately 02:00 today and the SSC alert system highlighted and reported this just before 09:00. As a result of this alert, a search was carried out and the key identified. The key was ultimately passed to the key custodian in the data centers who in turn installed the new key via a re-boot of the servers. This was completed at approximately 10:45.

The process of TK renewal is as follows:

The KMA automatically generates a task notifying the requirement for a key replacement on the KMA workstation, stating that the new key needs extracting from the system. The key extraction is a manual process carried out by the Key Manager and involves extracting the new key on to a floppy disk that is in turn copied on to the appropriate server at Wigan & Bootle.

This task generated, is of one line and can vary in amount per day from as little as 10 tasks to as many as 200. They are often different tasks generated by the KMA on the Task list, and all but 1 or 2 of these tasks that are generated, are due to pre CSR+ activities and can be ignored. On a daily basis the Key manager identifies any that require attention and deletes the rest. Once these tasks have been removed they are unrecoverable and the only record is that "a task" was generated. No details are available. There is also no record of tasks generated or sent to the KMA.

Without conformation of receipt of this task, it can be presumed that there is a possibility that the task may have been inadvertently deleted.

The task is the only form of notification given to the key manager that the key is going to expire in the

FUJ00232549

FUJITSU SERVICES

MAJOR INCIDENT REPORT

Ref: MI:
Status: Initial: V1
Owner:

future. If this is lost there is no other expiry warning or notice provided.

Future Actions	Owner	By	Status	PEAK
A check has been carried out to ensure that there are no keys due for expiry in the next 72 hours.	SSC	8/02/06	Complete	
With immediate effect a manual check will be carried out weekly to ascertain the forthcoming 7 days changes. This will ensure that the changes are actively monitored.	POA security	8/02/06	In place	
This incident is now recognised as a SPOF (single point of failure) and does not provide for adequate auditing. To avoid any possible recurrence security has been in discussion with SSC to incorporate **ALL** imminent key expirees on to the Horizon PSE Report for Counter Key Refresh. This report is generated and distributed on a weekly basis. It has also been agreed with the SSC that the responsibility of this report is to be handed over to the KMA Key Manager security, and this will take place from 20th Feb.	KMA Key Manager	28/2/06	Ongoing	PC0131994

Fix Applied	CP Reference	CT / CR Reference

Date Closed	Fujitsu Approval	Post Office Approval