FUJ00087658

FUJITSU

shaping tomorrow with you

Horizon Core Audit Process

08/03/18

Pete Newsome

Torstein Godeseth

FUJ00087658

Exec Summary

FUJITSU

- The Horizon Application has been designed to ensure that accurate and auditable records are kept of all sub-postmaster transactions
- When a transaction is conducted at a counter, an auditable mechanism has been built in to ensure these transactions are taken from the counter, stored in the Horizon main branch database and then copied to an audit database
- This mechanism can be considered a ‘closed loop’ where information is securely exchanged from the counter to the Horizon branch database and then on to the audit database
- Whilst copies of transaction data are provided to numerous external systems from the main Horizon database, once an audit record is created, it becomes security sealed and time stamped. Audit records cannot then be accessed or altered without detection and the creation of further auditable events
- The Core Audit Process is designed to provide a definitive log of all transactions. As such it is the “base” upon which any assessment as to “what was entered at the counter” should be derived from to the exclusion of all other systems that may take a feed of data from the Branch Database
- A number of ‘assertions’ can be independently examined to test the robustness of the Core Audit Process, these are listed from page 7 of this presentation

FUJ00087658

Exec Summary continued

FUJITSU

- The enclosed summary and embedded documents provide an overview and technical description of the Horizon 'Core Audit Process' (CAP)
- This illustrates the design principles and safeguards built into the CAP to ensure that a record of sub-postmasters transactions are created, maintained and protected for the 7 year term from creation as required under contract
- There are 2 documents enclosed. These describe the audit processes for the original 'Horizon Core Audit Process' and also the revised 'Horizon Online Core Audit Process (Post 2010)
  - ARCGENREP0004.HorizonDataIntegrity.doc
  - HorizonOnlineDataIntegrity_POL.doc
- The documents are written in sufficient detail for an Independent Expert to gain an understanding of the key principles, technologies and processes involved in the CAP

FUJ00087658

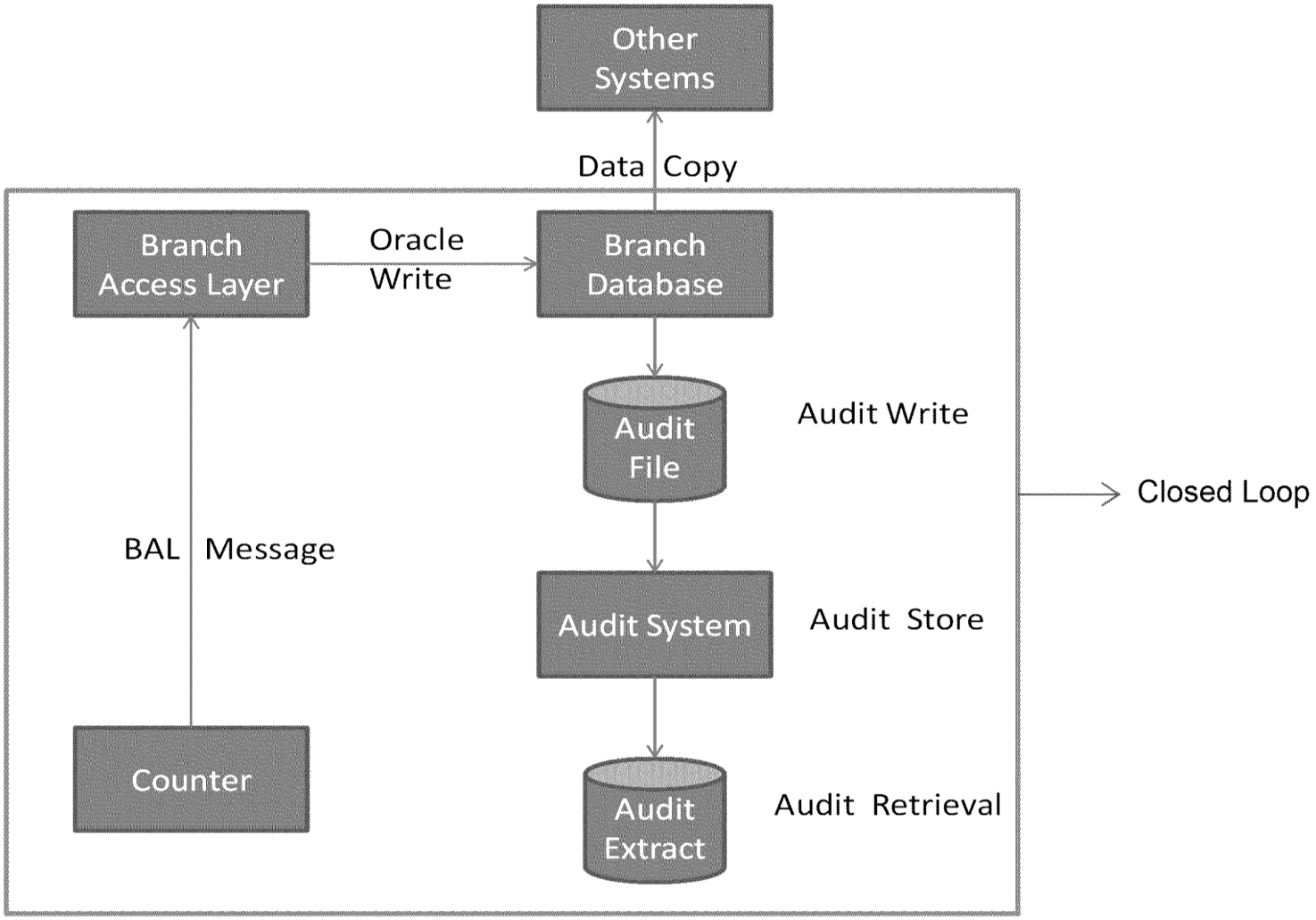
Key Principles

FUJITSU

- The Core Audit Process is designed to ensure that an exact record of counter transactions are created and kept in a secure audit database
- Safeguards are built into the process to check for transaction data corruption and integrity
- Principles of double entry book keeping are used to validate that items purchased are matched to monies received
- Each item in the audit trail has a unique incrementing sequence number. This means it is possible to detect if any transitions records have been lost
- Transaction records are ‘sealed’ using industry standard secure protocols
- All audit records are kept in a segregated audit database

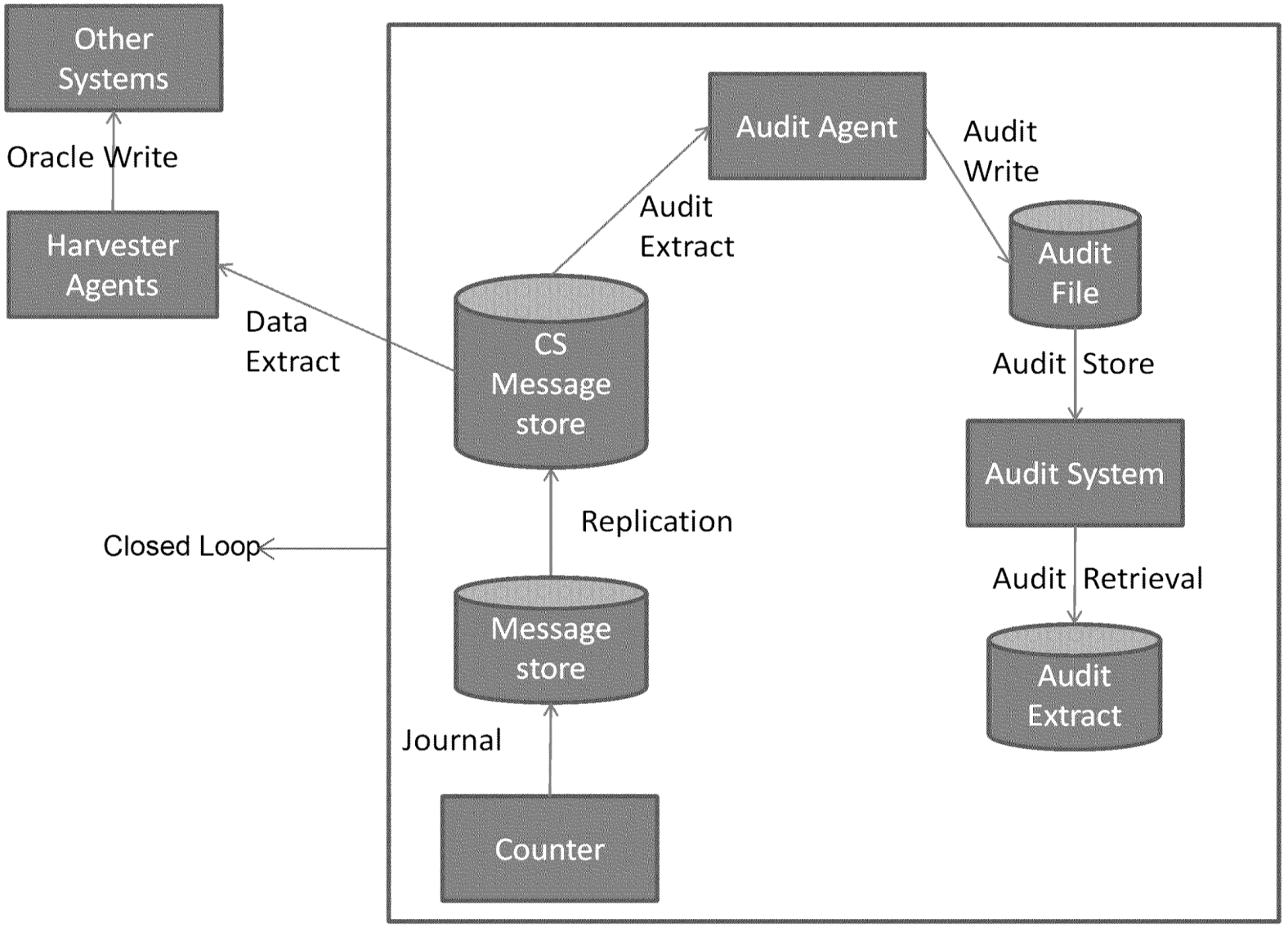
FUJ00087658

Horizon Online Core Audit Process



FUJ00087658

Horizon Core Audit Process



1

FUJ00087658

FUJITSU

shaping tomorrow with you

Horizon On Line Core Audit Process

Key Assertions

FUJ00087658

Summary

FUJITSU

- In order to provide assurance that the Core Audit Process is performing as designed for Horizon On-line*, a number of assertions related to the design and function of the CAP can be tested;
  - Baskets net to nil
  - Basket received is same as that seen by counter
  - Full basket enters audit trail
  - All baskets enter audit trail
  - No extra baskets enter audit trail
  - Audit trail has integrity

- *The Horizon Application was re-architected and rolled out in 2010 so the original implementation is no longer operational. Any examination of original Horizon transactions will need to refer to design documentation and archive data that still exists (kept for 7 years). It is important to note that the design principles of the CAP are consistent between the two versions.

FUJ00087658

Baskets Net to Nil

FUJITSU

- That all of the transactions in a basket (a basket is defined as any number of items for one customer) received from the Post Office branch counter balance to zero against the customer payment.
  - When the contents of a Basket are written to the Branch database a check is made that the net value of all the accounting lines is indeed zero and should it not be, then an alert is raised and the basket is discarded and an error response returned to the counter.
  - The transaction cannot be completed until a successful response has been received from the BAL indicating that the message has been stored
  - Any failures in committing Auditable activities at the Data Centre will result in an error response being returned to the counter. In all cases the User is informed of what is happening. Such failures will not be visible in the transaction audit, but in normal operation will be visible in the system Event Log.

FUJ00087658

Basket received is same as that seen by counter

FUJITSU

- To ensure that the message is not tampered with after being sent from the counter, each message has an associated Digital Signature. The mechanism for creating this Digital Signature is as follows:
  - At Log On, the Counter creates an RSA Public / Private key pair.
  - The Public key is sent to the BAL as part of the audited Log On message
  - The Log On message is concatenated with the Digital Signature and the BAL's signing certificate for its Public Key and signed by a BAL Private key (held in the data Centre Key Store) and added to the audit trail with a BAL generated jsn
  - All subsequent messages are digitally signed by the counter using the private key established at Log On.
  - Digitally Signing a message involves taking a SHA-1 Hash of the message and digitally signing the Hash value using RSA.
  - The Digital signature is stored alongside the message in the Journal table and is extracted with it into the Audit file as described below

FUJ00087658

Full basket enters audit trail

FUJITSU

- When the contents of a Basket are written to BRDB a check is made that the net value of all the accounting lines is indeed zero and should it not be, then an alert is raised, the basket is discarded and an error response returned to the counter.
- Each night after midnight, the contents of this message journal table for the previous day are copied from the BRDB to a number of serial files. During this copy process, a check is made that indeed there are no missing or duplicate jsns for any counter and should any be found an alert is raised.
- Should there be no response from the Data Centre following an attempted commit of an auditable activity within a timeout period (currently set to 30 seconds), an automatic retry is invoked. This sends identical business data to the Data Centre where a check is made to see if the Audit data has already been committed to BRDB. Should the retry also timeout, then the User is prompted and asked whether they wish to Retry or Cancel the Activity. Such time-outs and any retries will not be explicitly visible in the transaction audit, but in normal operation will be visible in the system Event Log.
- Continual failures to Update the Database at the Data Centre mean that it is not clear at the counter whether or not the database accurately reflects the situation in the Branch. Therefore the system will force a Log Off at the counter to ensure that when communications are re-established, that the Recovery process is invoked to reconcile the counter view with that on BRDB. If there is a basket currently being processed, then a special Disconnected Session Receipt will be produced showing which transactions have been discarded and which are to be recovered making it clear what money needs to be exchanged with the Customer.

FUJ00087658

No extra baskets enter audit trail

FUJITSU

- Within any counter (i.e. for a given Branch Id / Counter Id combination), the jsn will always increase by exactly one for each successive audit record. This enables a check to be made that there are no duplicated audit records
  - Every auditable request made by the counter will be logged in the message journal before the request is actioned by the BAL, The message journal performs two functions, firstly it provides auditing facility and secondly it provides a duplicate checking facility to prevent counter messages that may have been resent from being reprocessed.
  - Access to the counter system which enables the entry of transactions via the BAL is controlled through a secure key exchange mechanism which takes place as part of the Log on Process.
  - The jsn is stored within the message body which is securely encrypted using cryptographic keys
  - A check is made that there are no gaps or duplicates in the jsn sequence for any counter.

FUJ00087658

Audit trail has integrity

FUJITSU

- Each message within the audit trail has its message body encrypted using the cryptographic keys used by the counter submitting the basket.
  - The jsn is stored within the message body which is securely encrypted using cryptographic keys
  - Each night after midnight, the contents of the message table for the previous day are copied from the BRDB to a number of serial files.
  - These files are then copied to the Audit system where they are sealed with digital seals. They are held there for a period of 7 years during which time they may be retrieved and filtered to produce the relevant audit data for a particular Branch.
  - The Digital Seal is calculated using an MD5 hash of the entire content of the file being sealed. This value is stored in a separate “Seals Database” held on the Audit Server.
  - Whenever data is retrieved for audit enquiries a number of checks are carried out:

1. The audit files have not been tampered with (i.e. the Seals on the audit files are correct)
2. The individual Baskets (and other records) have their digital signatures checked to ensure that they have not been corrupted
3. A check is made that no records are missing or duplicated. I.e. a check is made that there are no gaps or duplicates in the jsn sequence for any counter

  - There is adequate synchronisation of server and counter clocks throughout the process for time and datestamping purposes

FUJ00087658

Detailed Documentation

FUJITSU

Horizon Online
CAP

Horizon CAP