FUJ00171905

Document Title:	EUM Balancing Enhancements Customer Solution Proposal
Document Reference:	ARC/SOL/CSP/3694
Release:	TBS
Abstract:	This is the solution design for changes to EUM related to Balancing and Locking.
Document Status:	DRAFT
Author & Dept:	Hulme, Jon
External Distribution:	
Security Risk Assessment Confirmed	YES, security risks have been assessed, see section 0.9 for details.

Approval Authorities:

Name	Role	
Torstein Godeseth	Chief Architect	See Dimensions for record
Programme Manager	Marion Chave-Jones	See Dimensions for record

FUJ00171905

0 Document Control

0.1 Table of Contents

FUJ00171905

FUJ00171905

0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CP/CCN/PEAK Reference
0.1	10/01/2019	First version	TBS

0.3 Review Details

Review Comments by:	17/01/19
Review Comments to:	jon.hulme GRO POA Document Management

Mandatory Review	
Role	**Name**
Solution Design / Development	Ramesh Kalavakolla
Principal CSA	Tim Jones
Post	Esther Harvey
Senior Operations Manager	Alex Kemp
Security Architect	Dave Haywood; Adrian Ellis
Network Architect	Steve Freke
SV&I Manager	Amit Chorgi
Testing Manager	Mark Ascott
CISO	Stephen.Godfrey@ GRO
SSC Manager	Steve Parker; S GRO
Architect – Counter and BAL	Andy Thomas
Infrastructure Implementation	Rob Etherington
Service Archtiect	Phil Boardman
POA BAS Lead	Steve Bansal
POL EUM Product Owner	Shaun Turner

Optional Review	
Role	**Name**
Lead Architect	Tim Jones
Chief Architect	Torstein Godeseth
Application Development Manager	Graham Allen
Lead Hosting Architect	Mia Angell
System Management Group	John Bradley
Solution Design Architect, Agent	Clare Keane
Solution Design Architect, Crypto	Stuart Honey
Solution Design Architect, Crypto, Web Svcs	Sarah Selwyn
Security & Risk Team	CSPOA.Security@ GRO
Integration / SCM	Matt Swain

FUJ00171905

Project Manager	Rajinder Bath
Programme Manager HNG-X	Marion Chave-Jones
Operational Change/Release Management	Alan Wright
Business Continuity	Almizan Khan
Network Operations Manager	Chris Harrison
Systems Management Manager	Jerry Acton
Infrastructure Operations Manager	Andrew Hemingway
Application Lead SDM, Risk and Service Introduction	Yannis Symvoulidis
Solution Design / Development	Pavan Vejendla
Requirements Manager	Steve Evans
Business Analyst	Phil Moss
Domain Architect	Steve Porter
Domain Architect	Alan Holmes
Domain Architect	Gareth Seemungal
Support Specialist	John Simpkins
Service Manager	Kevin McKeown
POL EUM Project Manager	Esther Harvey
POL Head of IT Service (Retail)	Martin Godbold
POL Senior Business Analyst	Alan Bamber
POL EUM Technical Architect	Steve Page
ATOS EUM Technical Delivery Manager	Graham Bevan

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ARC/SOL/TEM/3033 *(DO NOT REMOVE)*	See note above	See note above	Template for Project Solution Design Documents.	Dimensions
PGM/DCM/ION/0001 *(DO NOT REMOVE)*			POA Document Reviewers/Approvers Role Matrix	Dimensions
REQ/GEN/PRO/0735			HNG-X GENERIC ACCEPTANCE PROCESS	Dimensions
DES/APP/HLD/0126			HNG-X Branch Accounting Counter HLD	Dimensions
DES/APP/HLD/0083			HNG-X Counter Subsystem: Recovery Management	Dimensions
REQ/CUS/BRS/3693	0.5		EUM-REQ-DOC-005 EUM Horizon Balancing Enhancements Business Requirements Specification	Dimensions

0.5 Abbreviations

FUJ00171905

Abbreviation	Definition
BAL	Branch Access Layer
BP	Balance Period
BRDB	Branch Database
CIT	Component Integration Test
CP	Change Proposal
DPIA	Data Protection Impact Assessment – a standard GDPR assessment
EUM	End User Management
FJ	Fujitsu
GDPR	General Data Protection Regulations See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
HBS	Horizon Business Server
HNG-X	The name used in the contract between Post Office Limited and Fujitsu to refer to the Horizon system.
HUID	Horizon User Id
LST	Live System Test
POID	Post Office User Id
POL	Post Office Limited
RTS	Retail Transaction Service
SSC	System Support Centre
SV&I	System Validation & Integration
TP	Trading Period
UAT	User Acceptance Test

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes
Changes due to review comments.

0.8 Potential for Change

There are no known future requirements to be considered.

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Security Risk Assessment

FUJ00171905

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

There is no GDPR impact due to these changes. See section 11.1.

FUJ00171905

1 Scope

This solution design is in response to Change Request CWO0075 "RTQ0002243 EUM Balancing enhancements".

The End User Management (EUM) project was released into pilot at the end of July 2018, and the functionality was subsequently rolled out across the estate.

This changed a fundamental assumption of the Horizon design, which is that a single Horizon user can only be logged in once at any one point in time. If the Horizon user attempts to login concurrently on a second counter, then a "concurrent login" message is output and Horizon will forcibly terminate the previous user session.

The EUM project changed this assumption so that a given EUM user is able to lock a counter and then log on to another counter. The user can later lock or log off from this counter and eventually resume the user session on the original counter. There can be multiple sessions in a locked state, but only one user session actually active at any point in time.

The change has caused incidents to occur in the live estate (e.g. PC0275532, PC0275564) primarily related to balancing. Design changes are therefore required in order tighten up concurrent use of Horizon with the same EUM Horizon user id.

1.1 Purpose of Document

The purpose of this document is:

1. To allow review of the technical solution by other architects.
2. To provide sufficient detail for Development and Test to impact this change and to direct their activities.

1.2 Target Audience for This Document

The readers are assumed to be technical and familiar with Horizon.

1.3 Overview

The problem areas and associated solutions are listed in overview below:

1. **Stock Unit Balancing**
   - Do not allow stock unit balancing to be started if the same EUM Horizon user id is logged in on another node.
   - Do not allow an EUM user to login if that Horizon user id is balancing the stock unit on another node, unless they terminate the other session.
   - See section 3.1 for the problem details, and section 4.1 for the solution details.

2. **Branch Balancing**
   - Do not allow branch balancing to be started if the same EUM Horizon user id is logged in on another node and is balancing the branch.
   - Do not allow an EUM user to login if that Horizon user id is balancing the branch on another node, unless they terminate the other session.
   - See section 3.2 for the problem details, and section 4.2 for the solution details.

FUJ00171905

3. **Attach User To Stock Unit**
   - Do not allow an EUM user to change their stock unit attachment if that Horizon user id is logged in (and locked) on another node, unless they terminate the other session.
   - See section 3.3 for the problem details, and section 4.3 for the solution details.

4. **Unlocking**
   - When unlocking the counter, check that the current TP, BP and stock unit are still correct. If not, record a system error and force log off.
   - See section 3.4 for the problem details, and section 4.4 for the solution details.

5. **Auto settlement on inactivity timeout**
   - When auto-settling the basket due to inactivity timeout, check that the current TP, BP and stock unit are still correct. If not, record a system error and force log off.
   - See section 3.5 for the problem details, and section 4.5 for the solution details.

6. **Move the Lock button**
   - The counter UI Lock button is to be swapped with the Screen Entry button.
   - See section 3.6 for the problem details, and section 4.6 for the solution details.

7. **Testing**
   - Test the functional changes (described above).
   - Regression test that they have no impact on existing EUM locking, stock unit balancing, or branch balancing functionality.
   - Test that the data centre changes have no impact on the existing counters.
   - Test other named areas for concurrency issues.
   - Consider off script testing for other concurrency issues
   - See section 6 for details.

FUJ00171905

2 Requirements

The requirements from the CR are listed in section 10, and are cross-referenced in the following sections.

Note that by design [EUM-HBE-SUB-040] will not output a UI error message.

A new requirements are needed for the scenario in section 4.2.2.2.

FUJ00171905

3 Problem Description

3.1 Stock Unit Balancing

3.1.1 An Unlocked Counter Is Not Aware Of Stock Unit Rollover

Consider the scenario:

a. An EUM user locks counter A.
b. The same HUID logs into counter B.
c. Counter B rolls over the stock unit.
d. Counter B is locked or logged off.
e. The same user unlocks counter A.

Now counter A is not aware that the stock unit has rolled over, and will now trade in the old TP/BP, until it logs out.

This scenario has occurred in the live estate. The SSC can detect when it has happened by looking for transactions that have occurred for a given TP/BP after the date/time on which that TP/BP rolled over.

A variant of this scenario is that counter A times out due to inactivity, rather than being unlocked, after counter B has rolled over. Since timeout auto settles any items in the basket to cash, in this scenario any items in the basket would be settled in the old TP/BP.

Another variant of this scenario is that counter A may attempt to rollover the stock unit after counter B has already rolled it over. This eventually leads to MSG31314 "The stock unit <su> TP or BP is inconsistent. Balancing cannot continue" and rollover is aborted, however misleading trial and final reports may have been produced prior to this message.

Another variant of this scenario is that counter A may attempt to rollover the branch after counter B has rolled over the stock unit into the next TP. This causes a non-zero trading position to be reported and the trading statement produced is incorrect (notably the Carried Forward cash position is identical to the Brought Forward cash position). The only financial figures written by the branch rollover process are the branch suspense opening balances for the trading period rolled into, which may be incorrect if a non-zero net value is present in suspense.

3.1.2 A Second Counter Removes The SU Balancing Lock

3.1.2.1 At Logon

Consider the scenario:

a. An EUM user logs in to counter A.
b. The user presses the button to balance the stock unit.
c. The stock unit is locked for balancing.
d. The balancing process is started.
e. The user locks the counter.
f. The same EUM HUID user logs in to counter B.
g. This unlocks the stock unit for balancing since the user is the same as the locking user.
h. Any user may trade in the stock unit since it is not locked for balancing.
i. The current user rolls over the stock unit.
j. The user locks or logs out from Counter B.
k. The user unlocks counter A.
l. The user resumes stock unit balancing.

Investigation shows that this causes a system error message and fails the stock unit rollover because the system detects the stock unit is no longer locked.

FUJ00171905

Note however that the system error is not output until the end of the rollover process, and so:

i) A balance report is printed prior to the rollover failure.

ii) The financial position reported by the rollover process, including declarations, discrepancies and making good local suspense may not be based on the latest position in the stock unit.

Note that if a user with a different HUID (even if linked to the same POID) attempts to login while the first session in the above scenario is locked, they are correctly unable to login since the rollover lock present.

3.1.2.2 At Unlock

Another variant of this scenarios is if counter B was initially logged in with the same HUID, but locked. Then at step f above the user unlocks counter B rather than logged in to counter B.

FUJ00171905

3.2 Branch Balancing

3.2.1 An Unlocked Counter Is Not Aware Of Branch Rollover

This scenario is not actually a problem because the office branch TP is only held in the data centre. If counter B rolls over the branch and counter A is unlocked, then counter A will still detect the correct branch TP when it accesses the data centre for reports or branch rollover.

3.2.2 A Second Counter Removes The Branch Balancing Lock

3.2.2.1 At Logon

Consider the scenario:

a. An EUM user logs in to counter A.
b. The user presses the Trading Statement button to balance the branch.
c. The branch is locked.
d. The branch balancing process is started.
e. The user locks the counter.
f. The same HUID user logs in to counter B.
g. This unlocks the branch since the user is the same as the locking user.
h. The user rolls over the branch into a new trading period.
i. The user locks or logs out from Counter B.
j. The user unlocks counter A.
k. The user resumes branch balancing.

Investigation shows that this fails because the system detects the branch is not locked.

Note that the failure does not occur until the end of the branch rollover process, and:

i) The counter does not report failure to the clerk, but rather reports successful rollover into the next trading period, even though the rollover actually failed. This has been raised as defect PC0275644.
ii) An invalid branch trading statement is printed prior to the rollover failure.

Note that if a user with a different HUID (even if linked to the same POID) logs in while the first session in the above scenario is locked, they are correctly unable to rollover the branch since the branch rollover lock is present.

3.2.2.2 At Unlock

Another variant of this scenarios is if counter B was initially logged in with the same HUID, but locked. Then at step f above the user unlocks counter B rather than logged in to counter B.

FUJ00171905

3.3 Stock Unit Attachment

This is another variant of the scenario in section 3.1.1.

If the clerk has changed the stock unit that their HUID is attached to on counter B, and then unlocks counter A, counter A is still thinks that the user is attached to the old stock unit, and continues to trade in the old stock unit.

The existing code prevents a user's stock unit attachment being changed if that user is currently logged on, but does not prevent it being changed if the user in question is the user making the change.

3.4 Unlock

As described in section 3.1, 3.2 and 3.3, Unlock can cause problems if the TP, BP or stock unit were changed while the counter was locked by the same HUID logged in at another node.

Even though these issues will be solved, an independent check should be made that the values in use by the counter match those known to the data centre.

3.5 Inactivity Auto Settlement

The same issued described in section 3.4 also applies when the counter times out the lock screen due to inactivity and auto-settles the basket to cash.

3.6 Lock Button

The lock button at position T3 is right next to the Prev button. Prev is a very commonly pressed button, which POL have stated leads to Lock being pressed accidentally. Once pressed, Lock requires the username and password to be entered to undo the mis-press, slowing clerks down.

3.7 Other scenarios

Other scenarios have been considered to see whether they may have problems in similar areas to those above. These scenarios should still be tested with a) concurrent use, and b) EUM locked use.

Where problems have been found that are general concurrency issues which are not related to the EUM locking changes, they have been raised as separate PEAKs (see section 6.1.1).

See section 6 for details.

FUJ00171905

4 Solution Design

4.1 Stock Unit Balancing

4.1.1 An Unlocked Counter Is Not Aware Of Stock Unit Rollover

The problem is described in section 3.1.1.

The requirement ids are [EUM-HBE-SUB-010] and [EUM-HBE-SUB-020].

The code already prevents stock unit balancing being started if a different HUID is logged on elsewhere, even if that other session is locked.

The fix is to prevent stock unit balancing being started if the same EUM HUID is logged on at another node, even if that other session is locked.

Existing High Level Design:

See [DES/APP/HLD/0126] section 3.4.1 step 4.

At the start of stock unit balancing, the existing counter code calls BRDB query GetLoggedOnSessionDetailsForSU. This query looks for sessions associate with the current stock unit, other than the current session, which are not in state 'LOGOUT' or 'INVALIDATE' (so they are ACTIVE, FAILED, or RECOVERING). It also looks for outstanding recovery data associate with the stock unit.

The counter code (BalanceStockUnit.pdl) then sees if any of these sessions belong to another user, and if so displays error message MSG31305 and aborts balancing (step 5).

For background information on user session states see diagram in [DES/APP/HLD/0083] section 7.2.3.4, which has been reproduced and updated in section 13.1 of this CSP.

New High Level Design, for review by Development:

This requires a change to BalanceStockUnit.pdl to display MSG31305 and abort the balancing attempt even if the sessions returned by the GetLoggedOnSessionDetailsForSU belong to the current HUID.

POL have asked to review the text of MSG31305 [EUM-HBE-MES-010], see section 5.1.1.

If a counter was balancing and physically failed, it would leave the stock unit locked and the session in state 'ACTIVE'. This in itself will not prevent the same user logging in and balancing on another counter, because the solution in section 4.1.2.1 allows the active session to be marked as FAILED. Note however, that as per existing business rules, failed sessions must be recovered before balancing can be performed, and so as at present, the failed counter would need to be replaced prior to balancing being able to continue.

This change requires a counter change, and potentially a reference data change.

4.1.2 A Second Counter Removes The SU Balancing Lock

4.1.2.1 At Logon

The problem is described in section 3.1.2.1. The requirement id is [EUM-HBE-SUB-050].

The login code already prevents a different HUID (whether the same POID or not) from logging in while the stock unit is being balanced at another counter, but is locked. However the same HUID (linked to a POID) removes the balancing lock and is allowed to continue the login.

The fix is to check to see if the stock unit is locked by the HUID that is logging in, and that HUID is linked to a POID, and there is an ACTIVE or RECOVERING session present for that HUID on another node. In

FUJ00171905

this case do not unlock the stock unit, but display new message MSGNEW01 (see section 5.1.2) warning that the stock unit is locked for balancing, and to continue then all other sessions for this HUID will be terminated (there should normally only be the one session for the same HUID on another node that started the balance).

Existing High Level Design

The existing login messages exchanged with the BAL are shown in the sequence diagrams in section 13.2.

1. The counter sends the usual SecondLogonInteractionDTO to the BAL.

2. The BAL code performs the stock unit balancing check. This is called from AutheticationFacade authenticate (for Second Logon) and from TrustedLogonServiceHandlerImpl isStockUnitBalancingInProgress. The check is implemented in CheckStockUnitBalanceDAOImpl isStockUnitBalancingInProgress, which delegates the check to isBalancingInProgress.

3. If balancing is in progress and the HUID is the same as the HUID that holds the lock, then isBalancingInProgress removes the stock unit balancing lock. A BalancingInProgressResponseDTO is then returned to the client. The counter then displays MSG00303 "Stock Unit Balancing In Progress", and when the user presses OK the counter logs off with no further interaction to the data centre.

New High Level Design, for review by Development:

The changes to login messages exchanged with the BAL are shown in the sequence diagrams in section 13.8.1.

1. The counter sends the usual SecondLogonInteractionDTO. This must have the service version defined in BSSpecification.xml incremented, so that the BAL can tell this call is from the new counter code.

2. If the SecondLogonInteractionDTO service version is the new version, then isBalancingInProgress must not remove the lock if the HUID matches the locking HUID, and that HUID is linked to a POID and has an active session on another node.

This change will require a call to existing SQL PoidSessionAlreadyExists_v2 via SessionDAOImpl getExistingUserActiveSessions, if userBean.isPoidUser(). If there are any rows returned for the same HUID (i.e. branch_user) then that user has active sessions on another node (the current node's session is already excluded via the current token id).

3. The BAL must then return a SecondLogonResponseDTO, with UserAlreadyLoggedOn set to true (as per the usual case if the user is already logged on). The counter would normally then display MSG04045 Concurrent Login, and then call the BAL ConcurrentLogon service handler with ContinueLoggingOn set to true or false as required.

In order for the counter to display the different message MSGNEW01, an extra flag must be returned in the SecondLogonResponseDTO, sameEUMHUIDIsSUBalancing set to true. The counter would then display the new message with buttons to Continue or Cancel, and then continue with a ConcurrentLogonRequestDTO with ContinueLoggingOn set to true or false as required. Setting ContinueLogginOn to true will terminate all other sessions for this HUID.

As at present with concurrent logon for the same HUID, the stock unit rollover lock remains. If that HUID attempts to perform balancing, that code ignores the lock, but aborts balancing (and removes the lock) until the terminated (FAILED) session on the other node is recovered.

This change is not relevant to SSKs via Trusted Logon, because the SSK HUID is never used to balance a stock unit.

This fix requires a counter, BAL and reference change.

Allowing the user to terminate other sessions and login means that it is possible for the user to continue trading if a counter that the user is balancing physically fails.

FUJ00171905

4.1.2.2 At Unlock

The problem is described in section 3.1.2.2.

This variant concerning counter B being unlocked when A is balancing, rather than B logging in, is prevented by the fix in section 4.1.1 which prevents stock unit balancing being started if the same EUM HUID has another active session.

FUJ00171905

4.2 Branch Balancing

4.2.1 An Unlocked Counter Is Not Aware Of Branch Rollover

As described in section 3.2.1 this is not an issue.

4.2.2 A Second Counter Removes The Branch Balancing Lock

4.2.2.1 At Logon

The problem is described in section 3.2.2.1. The requirement id is [EUM-HBE-BB-010].

The code already prevents a different HUID from balancing the branch if it is already being balanced on another node.

The fix is to add a new check for the case where a user attempts to login, and the branch is locked for balancing by that HUID linked to a POID, and there is an ACTIVE session present for that HUID on another node. In this case display a new message warning MSGNEW02 (see section 5.1.3) that the branch is locked for balancing, and to continue and unlock the branch then all other sessions for this user (HUID) will be terminated.

Existing High level Design

The existing login messages exchanged with the BAL are shown in the sequence diagrams in section 13.2.

1. The counter sends the usual SecondLogonInteractionDTO to the BAL.

2. If the branch is locked, the normal SecondLogonResponseDTO is returned, no matter whether the HUID is the same as that which locked the branch or not. If it is the same, the branch is unlocked.

New High Level Design, for review by Development:

The changes to login messages exchanged with the BAL are shown in the sequence diagrams in section 13.8.2.

1. The counter sends the usual SecondLogonInteractionDTO. This must have the service version defined in BSSpecification.xml incremented, so that the BAL can tell this call is from the new counter code.

2. If the SecondLogonInteractionDTO service version is the new version, then the BAL must check whether the branch is locked for balancing via existing query IsBranchLocked. This will be called from Authetication Facade authenticate (for Second Logon).

3. If the BAL finds that the branch is locked, and the HUID logging in is the same as the HUID that owns the lock, and the HUID is for a POID user, and the HUID has an active session on another node (SQL PoidSessionAlreadyExists_v2 via SessionDAOImpl getExistingUserActiveSessions) then it must return a SecondLogonResponseDTO, with UserAlreadyLoggedOn set to true (as per the usual case if the user is already logged on). The counter would normally then display MSG04045 Concurrent Login, and then call the BAL ConcurrentLogon service handler with ContinueLoggingOn set to true or false as required.

6. In order for the counter to display a different message, an extra flag must be returned in the SecondLogonResponseDTO, sameEUMHUIDIsBranchBalancing set to true. The counter would then display the new message, and continue with a ConcurrentLogonRequestDTO with ContinueLoggingOn set to true or false as required.

As at present with concurrent logon for the same HUID, the branch rollover lock remains. If that HUID attempts to perform branch balancing, that code ignores the lock.

This change will not impact SSKs via Trusted Logon, because the SSK HUID is never used to balance the branch.

FUJ00171905

This fix requires a counter, BAL and reference change.

Allowing the user to terminate their other sessions and login means that it is possible for that user continue to balance the branch if a counter that the user is balancing physically fails.

If the branch is being balanced by a different HUID, this is fine. The existing code will stop that HUID starting to balance the branch concurrently.

4.2.2.2 At Unlock

The problem is described in section 3.2.2.2. A new requirement should be added for this scenario.

This variant concerns counter B being unlocked when A is balancing the branch.

In this scenario we would not want to allow counter B to start balancing the branch. The current code would allow it to do so because it is the same HUID that holds the lock.

The fix is add a new check when Branch Balancing is started to check if the branch is locked for balancing by that HUID linked to a POID, and there is an ACTIVE session present for that HUID on another node. In this case an error message should be displayed and the user returned to the menu.

If the other counter that was performing the balancing had failed, then the user simply has to log on again to a different counter and the fix in section 4.1.1 will terminate that session and allow branch balancing to be started.

Existing High Level Design:

The existing lock branch messages exchanged with the BAL are shown in the sequence diagrams in section 13.3.

See [DES/APP/HLD/0126] section 3.15.1 step 1.

1. At the start of branch balancing, the existing counter code calls the BAL GenericBRDBRetrievalService GetBranchTradingPeriod followed by isBranchLocked. If the branch is locked by a HUID which is different to the current HUID then counter displays message MSG31315 "Cannot balance branch" "The branch is currently being balanced by user, <user>." and aborts balancing.

2. The counter calls BAL LockBranchService to lock the branch for balancing.

3. This service also checks to see if the branch is already locked for balancing, and if the HUID with the lock is not the same as the current HUID then error LOCK_BRANCH__LOCKED is returned, and the counter again displays MSG31315.

4. If the LockBranchService returned success, then the counter proceeds with further checks.

New High Level Design, for review by Development:

The changes to lock branch messages exchanged with the BAL are shown in the sequence diagram in section 13.9.

1. The BAL LockBranchService check needs to be changed to also return error LOCK_BRANCH__LOCKED if the HUID holding the lock is the same HUID as the current HUID, and the current HUID has a POID, and that HUID has an active session on another node.

2. This requires the service handler to call existing BAL query SQL PoidSessionAlreadyExists_v2 via SessionDAOImpl getExistingUserActiveSessions, if userBean.isPoidUser().

This fix requires a BAL change.

FUJ00171905

4.3 Stock Unit Attachment

The problem is described in section 3.3. The requirement id is [EUM-HBE-AUSU-010].

The following fixes were considered:

1. To disallow a user's attached stock unit from being changed if that same HUID has an ACTIVE or RECOVERING session on another node (which would be locked).

   The problem with this is that if the locked counter failed then the user would not be able to unlock the counter to close down the session. Therefore the attached stock unit could not be changed until the counter was replaced and a user logged in (causing the previous user sessions to be tidied up).

2. When attempting to change the attachment, to give a warning message, but allow the user to continue. When unlocking a counter, or on inactivity time-out, if the attached stock unit does not match that currently known to the counter, then give an error and force logout the user.

   The problem with this is that inactivity timeout does not currently interact with the data centre, except to settle the basket. It would not be good to add an extra check on the attached stock unit on every settlement. Instead, a new interaction with the data centre would be needed, and if this failed, or the attached stock unit was found to be incorrect, then the counter would need to force logout in offline mode.

Therefore the actual solution is that when attempting to change the stock unit that a user is attached to, if that user is a POID user, and the attachment being changed is for the current user's HUID, and other ACTIVE or RECOVERING sessions for that user are found, then give a warning message. If the user opts to continue then terminate the other sessions.

Suggested High Level Design, for review by Development:

Note the existing login messages exchanged with the BAL are shown in the sequence diagrams in section 13.6. An updated sequence diagram showing the changes is given in section 13.10.

1. If the attachment being changed is for the current user's HUID, then the counter sets a new flag "sameEUMHUIDSessions" to "Check" in the request DTO "payload".

2. The BAL service handler AttachUserToStockUnitServiceHandler currently performs various checks in StockUnitDAO attachUserToStockUnit. If the checkSameEUMHUIDSessions is set to "Check" it must perform a new check to determine whether there are other ACTIVE or RECOVERING sessions for the current user's HUID on another node. It does this by calling existing SQL PoidSessionAlreadyExists_v2 via SessionDAOImpl getExistingUserActiveSessions (RECOVERING is added to this query via PC0276050). If the query results show that are other sessions for the current user's HUID on another node then return a new error ERROR_KEY_EUM_HUID_HAS_OTHER_SESSIONS.

3. If the counter gets the new error it displays warning message MSGNEW03 (see section 5.1.4) with Continue and Cancel buttons.

4. If the user presses Continue, the service handler is called again, but this time setting the new flag "sameEUMHUIDSessions" to "Terminate". The service handler must then set all ACTIVE or RECOVERING sessions for that HUID on other nodes to status "FAILED".

5. If the user press Cancel the attach user to stock unit user case is cancelled.

This design also applies to the case of unlock finding that a user is concurrently logged on.

This design is backwards compatible with old counters.

This requires a change to use case BAD-123 "Attach User to Stock Unit".

When unlocking the other counter, the existing code will detect that the session has been failed, and give message MSG10009 "System Logout" "You are being logged out (because you have logged on at another counter)" and logoff. POL have asked to review the text of this message.

FUJ00171905

The fix requires a counter, data centre and reference change, and will need SV&I testing.

FUJ00171905

4.4 Unlock

The requirement id is [EUM-HBE-SUB-030].

When a counter is unlocked, a further check should be performed to ensure that the current TP and BP and stock unit are those that the counter has cached in memory. If they are different then a system error should be generated and the counter force logged out without further interaction with the data centre. Any items in the basket will be handled by recovered as usual.

A system error is acceptable because this scenario should never happen when the other changes described in this document are implemented. This check is a failsafe.

High Level Design, for review by Development:

See the Unlock message flow diagrams in section 13.5. Updates flows are shown in section 13.11.

The counter Unlock code calls the BAL service SecondCredentialCheck followed by BAL service UnlockCounterService. However, neither of these responses contains the latest stock unit TP and BP and Stock Unit. The counter should pass to the UnlockCounterService the TP and BP and stock unit (extra fields needed on UnlockCounterRequestDTO), and the service should be changed to call existing query GetBranchStockUnitData (see StockUnitProfileDAO getStockUnitProfile) to determine whether the TP and BP and currently attached stock unit are correct.

If the TP or BP or stock unit are not correct, an error should be returned (in the UnlockCounterResponseDTO) and the counter should give a system error and force logout without interaction with the data centre (see ForcedLogoffBLO in silent, offline mode).

Note that it is not sufficient for the BAL to throw an exception and not return to the counter because this causes the counter to display MSG04047 stating there is a comms failure and just refuse to unlock.

The BAL UnlockCounterService should omit the new check if no TP and BP and stock unit are passed from the counter, and thus be backwards compatible with the existing counter code.

This change requires a counter change and a BAL change.

FUJ00171905

4.5 Inactivity Auto Settlement

The requirement id is [EUM-HBE-SUB-040].

The TP, BP, and SU check described in section 4.4 also needs to be applied if the system times out at the lock screen and attempts to auto-settle because one or more items are in the basket.

In this case a system error should be generated, but no message should be output (contrary to the requirement) because the counter is most likely to not have a user present at the point of inactivity timeout.

High Level Design for review by Development: See the Inactivity Auto Settlement message flow diagrams in section 13.7. Updates flows are shown in section 13.12. When the counter times out the lock screen due to inactivity, it does not call the BAL SecondCredentialCheck or UnlockCounterService, but simply calls the settlement service to settle any non-empty basket to cash. In this case, prior to calling the settlement service, the counter should call the query specified in section 4.4 via the GenericBRDBRetrievalService to get the latest TP and BP and stock unit, and check they are correct.

This change requires a counter change.

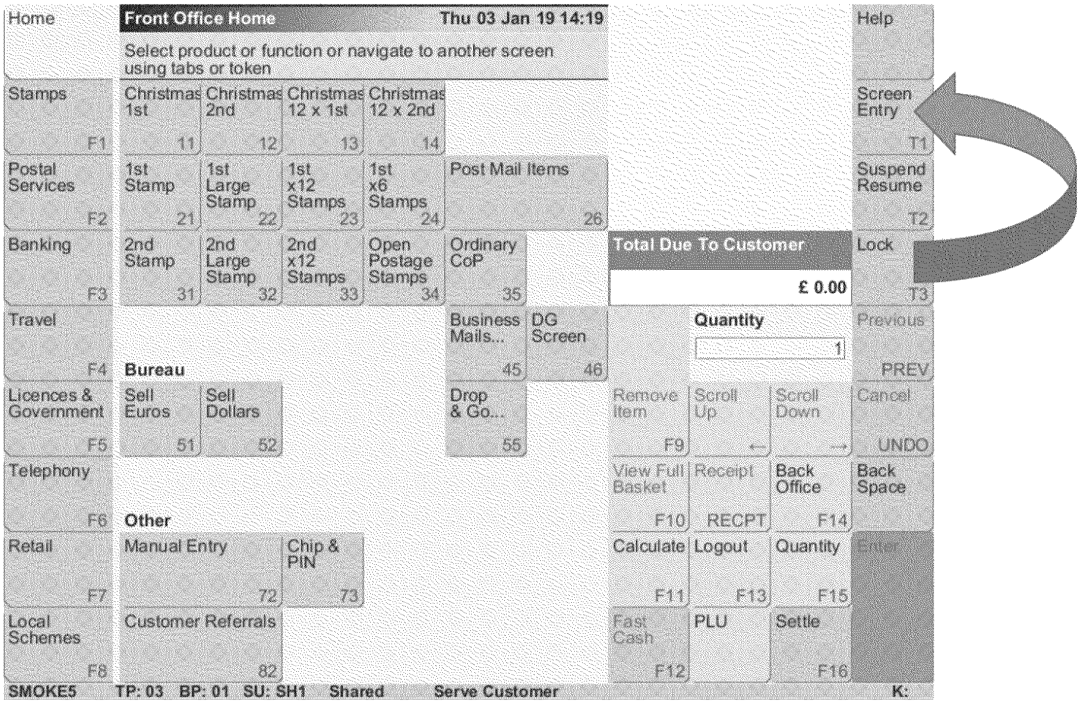
FUJ00171905

4.6 Lock Button

The problem is described in section 3.6.

Requirement EUM-HBE-MLB-010 requests the "Lock" button on the counter right hand bar to move from position T3 to T1, i.e. that is it swapped with the Screen Entry button.

Accidentally pressing Screen Entry is quick to correct by simply pressing Screen Entry again.



Suggested High Level Design, for review by Development: This requires a minor change to CommandBarUIE.java.

4.7 Other scenarios

The other scenarios listed in section 3.7 do not require design change. The PEAKs raised during the analysis of the scenarios (see section 6) will be fixed using the normal incident handling process.

FUJ00171905

5 Reference Data

5.1 Message Def

Note that any changes to existing messages will go live "big bang" when the reference data is released, and so will impact existing counters as well as new counters. If necessary, a reference data rule could be introduced to make this conditional on the counter code version.

5.1.1 MSG31305

POL have expressed a desire to review and potentially change the text of MSG31305.

The current message has title "Unrecovered Sessions" and text "The stock unit, %StockUnit%, cannot rollover. This may be because the stock unit is attached to a user who is still logged on or whose session has not yet been recovered.".

5.1.2 MSGNEW01

This new message is output when a user logs on and the system finds that the stock unit is locked for balancing by that HUID, and that HUID has one or more active (locked) sessions on another node.

The new message is similar to the existing EUM concurrent logon message MSG04002. The bold text below shows the difference to this message.

Title	Text	Buttons
User Already Logged In **and is Balancing a Stock Unit**	You are currently logged in at another counter position **which is balancing a stock unit**. If you login here, your original session will terminate and you will be forced to logout when you return to the original terminal. This may also invoke Recovery actions. Press Continue to login or press Cancel.	Continue, Cancel

5.1.3 MSGNEW02

This new message is output when a user logs on and the system finds that the branch unit is locked for balancing by that HUID, and that HUID has one or more active (locked) sessions on another node.

The new message is similar to the existing EUM concurrent logon message MSG04002. The bold text below shows the difference to this message.

Title	Text	Buttons
User Already Logged In **and is Balancing the Branch**	You are currently logged in at another counter position **which is balancing the branch**. If you login here, your original session will terminate and you will be forced to logout when you return to the original terminal. This may also invoke Recovery	Continue, Cancel

FUJ00171905

	actions. Press Continue to login or press Cancel.	

5.1.4 MSGNEW03

This new message is output when a user attempts to attach their own attachment to a stock unit and the system finds that their HUID has one or more active (locked) sessions on another node.

Title	Text	Buttons
User Already Logged In	You are currently logged in at another counter position. If you change the attachment, your original session will terminate and you will be forced to logout when you return to the original terminal. This may also invoke Recovery actions. Press Continue to change the attachment or press Cancel.	Continue, Cancel

FUJ00171905

6 Testing

Testing must cover the following:

1. Testing the old counter with the new BAL, and ensuring there is no regression due to these changes.

   The areas that this regression testing needs to focus on are:

   Branch Balancing and Stock Unit Balancing Regression Testing

   Existing balancing functionality [EUM-HBE-GEN-010]

   A user can continue trading if the counter they are balancing on fails [EUM-HBE-SUB-060], [EUM-HBE-BB-020]

   Stock unit attachment

   EUM Regression Testing

   Existing EUM concurrent logon and locking functionality [EUM-HBE-GEN-020]

   Trusted Logon Regression Testing

   SSKs can successfully logon

   SSKs cannot logon if a stock unit is balancing

2. Testing new counter with the new BAL to cover the changed functionality described in section 4.
3. Testing new counter with the new BAL to check for regression.

   The same areas as in point 1 above require focused regression testing.

4. Testing the counter, looking for other concurrency issues.

   The list of regression test areas has been agreed with Post Office Limited [EUM-HBE-GEN-010]. These areas are:

   Modify User

   Change password [EUM-HBE-MU-010]

   Change role [EUM-HBE-MU-020]

   Change account disabled status [EUM-HBE-MU-030]

   Change user must change password status [EUM-HBE-MU-040]

   Delete User [EUM-HBE-MU-050]

   Delete Stock Unit [EUM-HBE-MU-060]

   Cut Off Report [EUM-HBE-MU-070]

   Declarations [EUM-HBE-DEC-010]

   Transfers [EUM-HBE-TRA-010]

   Remittances [EUM-HBE-REM-010]

   Inactive Stock Unit Rollover [EUM-HBE-ISU-010]

   Transaction Corrections [EUM-HBE-TCO-010]

   Transaction Acknowledgements [EUM-HBE-TAC-010]

   "Off script" testing aimed at finding other concurrent issues

Also note that the scenarios described in [REQ/CUS/BRS/3693] should be tested.

6.1.1 Related defects

FUJ00171905

The following defects have been identified during the investigation and design phase.

There will follow the normal incident management process to determine whether they need to be fixed, and if so in what release they should be fixed.

If fixes are required, and not already released, they should be considered for including in this release since they are in the area of concurrency.

PEAK Reference	Priority	Title
PC0276050	C	Concurrent login checks are bypassed if a counter is in Recovery
PC0275906	D	Attach user to stock unit omits logged on user name if check fails in data centre
PC0275902	D	Concurrent Cheques Listing could cause duplicate cheque rem out
PC0275893	D	Concurrent processing of pouch delivery leads to doubling the Rem In
PC0275890	D	Cash Variance Screen Misleading
PC0275644	C	Counter does not detect branch rollover failure

6.1.2 Development Testing

Development units are responsible for thoroughly unit testing all the new functionality developed. They should also run through regression testing as described above.

6.1.3 CIT Testing

CIT is responsible for performing integration testing of the Counter, BAL, HBS RTS and BRDB. It should test the new functionality and regression testing as described above.

6.1.4 SV&I Fujitsu Testing

CIT is responsible for performing functional testing of the overall solution. It should test the new functionality and regression testing as described above.

6.1.5 ATOS Testing

ATOS is typically responsible for performing UAT on behalf of Post Office Limited.

6.1.6 LST Testing

LST is responsible for final testing of final release packages prior to live deployment.

FUJ00171905

7 Fujitsu Deliverables

This table lists the Fujitsu deliverables and associated teams.

Team	Component	Documentation
Counter/BAL	Counter	To be identified by Dev
Counter/BAL	BAL	To be identified by Dev
Architecture		Use Cases

FUJ00171905

8 Service Introduction & Migration Strategy

Since these changes are fixes to the existing functionality, and not new functionality, and in order to reduce testing costs, the counter changes will be activated as the counter code rolls out, and *not* controlled by a reference data non-core link.

Test costs would be much greater if the new counter code had to cater for both old and new code paths.

The data centre changes must be backwards compatible with the old counter.

Performance will not be significantly impacted by these changes.

9 Summary of Assumptions and Outstanding Issues

There are no outstanding issues.

Assumption Number	Assumption Description	Cross reference into solution description

These assumptions are likely to be invalid in future versions of HNG-T that generate other transaction types. At that point, additional checks could be introduced if required.

FUJ00171905

10 External Requirements Traceability Matrix

These requirements are taken from [REQ/CUS/BRS/3693].

Tag/Id	Name	Version	Priority	Description	Acceptance criteria	Method	CSP Section
EUM-HBE-GEN-010	Zero degradation of existing functionality	0.1	M	Solution enhancements should not negatively impact any existing Horizon functionality relating to balancing.	Regression Test transaction scenarios to ensure changes do not have a negative impact. All issues identified shall be documented and flagged to Post Office. Note: List of regression tests to be agreed between Fujitsu and Post Office during detailed design phase.	TST	Testing: 6
EUM-HBE-GEN-020	Concurrent Logon	0.1	M	A singleton Horizon User ID or different Horizon User ID (but linked to same POID) shall be able to logon at one or more counters providing the previous counter(s) is locked and there is only one active session at a time.	EUM Concurrent Login functionality is unaffected by solution change. Example Tests. 1) HUID01 logged on at both Nodes 1&2 simultaneously but only one session is active at a time. 2) HUID01 & HUID02 (both linked to the same Smart ID) logged in at Nodes 1 & 2 respectively but only one session is active at a time. Any items present in the basket should be retained (subject to 60 min Horizon timeout rule).	TST	Testing: 6
EUM-HBE-SUB-010	Prevent stock unit balancing starting if the same HUID is logged on elsewhere	0.1	M	The solution shall prevent stock unit balancing being started if the same HUID is logged on elsewhere, even if that other session is locked.	The User shall be presented with a Horizon message and prevented from balancing if the same HUID is logged on in the network.	TST	Solution: 4.1.1
EUM-HBE-SUB-020	Balance Report check for other User sessions.	0.1	M	When the "Balance Report" button is pressed, Horizon shall check for other user sessions associated with the stock unit that are in the ACTIVE, FAILED, or RECOVERING state, including the current user's sessions, irrespective of whether the sessions are locked.	A User attempting a balance report whilst other sessions associated with the Stock Unit are in any of the ACTIVE, FAILED and RECOVERING status's (regardless of the session lock) shall be presented with MSG31305.	TST	Solution: 4.1.1

FUJ00171905

				If any are found then Horizon shall present the User with the existing message MSG31305 "Unrecovered Sessions" and abort the stock unit balancing attempt. Note: Potential rewording of MSG31305 shall be undertaken during the detailed design phase.	A User attempting a balance report whilst no other sessions are associated with the Stock Unit are in any of the ACTIVE, FAILED and RECOVERING statuses shall be follow the Balance Report transaction journey.		
EUM-HBE-SUB-030	Counter check for Trading Period, Branch Period & Stock Unit deltas.	0.1	M	When a User Unlocks a counter, Horizon shall check if the current Trading Period, Branch Period and attached stock unit are those that the counter has cached in memory. If they are different, then Horizon shall present the User with an Error Message and the counter shall be force logged out, with any active customer session handled through existing recovery processes	On unlocking, the counter will check that the TP, BP and Stock Unit match those held in the data centre. If the attributes match, the User shall proceed with standard transaction journey. If a discrepancy is identified, the User shall be presented with a message and force logged out. Note: message content shall be agreed between Fujitsu and Post Office during the detailed design phase.	TST	Solution: 4.4
EUM-HBE-SUB-040	Abandon Auto Settlement	0.1	M	In the event of auto settlement (after 60 mins of inactivity at the counter), if an item resides in the basket, Horizon shall first check if the current Trading Period, Branch Period and attached stock unit are those that the counter has cached in memory. If they are different, then Horizon shall abort auto settlement and present the User with an Error Message and the counter shall be force logged out.	On initiating auto settlement routine, the counter will check that the TP, BP and Stock Unit match those held in the data centre. If the attributes match, the auto settlement routine shall proceed as normal (settle basket to cash) transaction journey. If a discrepancy is identified, the User shall be presented with a message and force logged out. Note: message content shall be agreed between Fujitsu and Post Office during the detailed design phase.	TST	Solution: 4.5
EUM-HBE-SUB-050	Prevent a HUID logging on to Horizon if the same HUID is balancing the same stock unit on another counter or Terminate other Active sessions	0.1	M	When any HUID attempts to log on, Horizon shall check if the HUID is already logged on to an active session on another Node & the stock unit is locked for balancing. The User is presented with the option of continuing logon, but any active sessions linked to the HUID shall be terminated to remove risk of Stock Unit misalignment.	If the HUID is logged on at another node in an ACTIVE state & the stock unit is locked, the User shall be presented with a message to advise the Stock Unit is locked for balancing. Horizon shall present the User with the option of: a) Cancelling Logon b) Continuing Logon Journey – this shall result in the stock Unit being unlocked & any other sessions terminating. Note 1: More than 1 session may be terminated as per b)	TST	Solution: 4.1.2.1

FUJ00171905

					Note 2: message content shall be agreed between Fujitsu and Post Office during the detailed design phase.		
EUM-HBE-SUB-060	Continue Trading if a counter in the progress of Stock Unit Balancing fails	0.1	M	The solution shall allow the User to continue trading at another node (in a multi counter branch) if a counter being balanced physically fails.	If the counter being balanced physically fails, the User can trade at a different counter with the same HUID. Test scenario for Stock Unit Balancing activities.	TST	Testing: 6
EUM-HBE-BB-010	Prevent a HUID logging on to Horizon if the same HUID is balancing Branch on another counter or Terminate other Active sessions	0.1	M	When a HUID attempts to log on, Horizon shall check if the HUID is already logged on to an active session on another Node & the Branch is locked for Balancing. The User is presented with the option of continuing logon, but any active sessions linked to the same HUID shall be terminated.	If the HUID is logged on at another node in an ACTIVE state & Branch is locked for balancing, the User shall be presented with a message to advise the branch is locked for balancing. Horizon shall present the User with the option of: c) Cancelling Logon d) Continuing Logon Journey – this shall result in the Branch being unlocked & any other sessions terminating. Note: message content shall be agreed between Fujitsu and Post Office during the detailed design phase.	TST	Solution: 4.2.2.1
EUM-HBE-BB-020	Continue Trading if a counter in the progress of Branch Balancing fails	0.1	M	The solution shall allow the User to continue trading at another node (in a multi counter branch) if a branch being balanced physically fails.	If the counter being balanced physically fails, the User can trade at a different counter with the same HUID. Test scenario for Branch Balancing activities.	TST	Testing: 6
EUM-HBE-AUSU-010	Prevent Trading on a Stock Unit that has been changed at another Counter by the same HUID	0.1	M	Where a HUID is logged on at 2 counters simultaneously, when the active HUID attempts to change a Stock Unit, Horizon shall check if the HUID is already attached to the Stock Unit (on a different Node) in ACTIVE or RECOVERING states. If True, Horizon shall present the User with a message and the option of cancelling the action or continuing the change. If the User proceeds with the change, Upon unlocking any of the other sessions, the User shall be presented with an error message and the terminal shall be force logged off.	If the HUID is logged on at another node in an ACTIVE or RECOVERING state, the User making the Stock Unit change shall be presented with a message to advise other User (s) are associated to the Stock Unit being changed. Horizon shall present the User with the option of: a) Cancelling the action b) Continuing Action If the User selects b) Continue, any other sessions associated to the Stock Unit shall be terminated and presented with an Error Message upon attempting to log back in on that session. Once the User acknowledges the message (clicking Okay), the terminal shall be	TST	Solution: 4.3

FUJ00171905

					Force Logged Off. Note: message content shall be agreed between Fujitsu and Post Office during the detailed design phase.		
EUM-HBE-MU-010	Changing a User's Password	0.1	M	The solution shall not change existing system behavior towards User Password change activities, regardless of being logged on at more than one counter at a time. e.g. Changing Own Password, Forced Password Change, Changing another Users Password.	Incumbent system behavior should be confirmed following solution change. i.e regression tests for existing Horizon password change rules.	TST	Testing: 6
EUM-HBE-MU-020	Changing a User's Role	0.1	M	The solution shall not change existing system behavior towards Changing a User's Role activities, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e regression tests should confirm Horizon prevents changing a User's role if it is logged in.	TST	Testing: 6
EUM-HBE-MU-030	Changing a User's Disabled Status	0.1	M	The solution shall not change existing system behavior towards Changing a User's (e, g, active/disabled)Status, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e regression tests should confirm Horizon allows a user to be disabled, or enabled, no matter whether that user is logged in or not, or whether they are the current user, so long as they have the correct permission. A user can still lock and unlock the counter even if their account is disabled, but they cannot login as a new session.	TST	Testing: 6
EUM-HBE-MU-040	Changing a User's Unlock Account Status	0.1	M	The solution shall not change existing system behavior towards Changing a User's Unlock Account Status, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm Horizon allows a user to unlock a locked user account, no matter whether that locked user account is logged in or not. It not possible for the same user to unlock their account, because they could not be logged in to do so.	TST	Testing: 6

FUJ00171905

					With EUM locking, a user cannot unlock a counter if their user account has become locked by that same HUID attempting to login on another counter and giving an incorrect password three times. The user account would need to be unlocked by another user.		
EUM-HBE-MU-050	Deleting a User	0.1	M	The solution shall not change existing system behavior towards Deleting a User, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm Horizon prevents a user being deleted if that user is logged in, no matter whether it is the same user or a different user that is attempting to perform the deletion.	TST	Testing: 6
EUM-HBE-MU-060	Deleting a Stock Unit	0.1	M	The solution shall not change existing system behavior towards Deleting a Stock Unit, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e regression tests should confirm Horizon prevents a stock unit from being deleted if any user is attached to that stock unit, no matter whether it is the attached user or a different user that is attempting to perform the deletion.	TST	Testing: 6
EUM-HBE-MU-070	Reporting & Cut Offs	0.1	M	The solution shall not change existing system behavior towards Reporting and Cut Offs, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter allows multiple users to view reports concurrently, and handles the case of attempting to cut off reports concurrently. The first cut off chronologically will succeed, but the second will display error message MSG00524 "Already Cut Off".	TST	Testing: 6
EUM-HBE-MES-010	MSG31305 Text Review	0.1	M	As Post Office, if MSG31305 “Unrecovered Sessions” is re-utilised, I want to revise the wording	Agreed text shall fit the Message Box height & width constraints.	TST	Solution: 5.1.1

FUJ00171905

				to reduce ambiguity and promote accuracy for all impacted scenarios where the message appears. Note: MSG31305 should be uplifted to advise users to contact NBSC if a terminal has crashed.	Message content shall be agreed between Fujitsu and Post Office during the detailed design phase.		
EUM-HBE-MLB-010	Move Lock Button screen location	0.1	C	As Post Office, I want to move the "As Is" position of the Lock button away from the "PREV" button to near top of screen near "help button": T1 button position to T3 button position.	Horizon displays the Lock Button in Position T1 regardless of the screen which the User on. The Screen Entry button which used to be at positon T1 is now at position T3.	TST	Solution: 4.6
EUM-HBE-IFT-010	Inflight Transactions	0.1	M	The solution shall ensure that a cut off report triggered from one terminal shall not have a detrimental impact on an inflight transaction or basket on another locked terminal.	Statement of Fact	SOF	n/a
EUM-HBE-REP-010	Event Reporting	0.1	S	Any new events identified during the Design Phase shall be reportable enhancements to existing HORice and ARQ reports. Depending on the detailed analysis, this may include enablement of reporting via Credence. It is assumed this shall require uplift of the Horizon to Credence AIS.	Detailed reporting enhancements shall be outlined during the detailed design phase, signed off by Post Office and added as an appendix.	SOF	n/a
EUM-HBE-DEC-010	Declarations	0.1	M	The solution shall not change existing system behaviour towards Declarations, regardless of being logged on at more than one counter at a time. Note: Declarations is taken to mean all forms currently available on Horizon (cash, stock, foreign currency etc)	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users inputting/updating declarations and messaging is appropriate	TST	Testing: 6
EUM-HBE-TRA-010	Transfers	0.1	M	The solution shall not change existing system behavior towards Transfers, regardless of being logged on at more than one counter at a time. Note: Transfers encompasses both Transfer In and Out	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users completing transfers and messaging is appropriate	TST	Testing: 6
EUM-HBE-REM-010	Remittances	0.1	M	The solution shall not change existing system behaviour towards Remittances, regardless of being logged on at more than one counter at a time. Note: Remittances encompasses both Transfer In	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users completing remittances	TST	Testing: 6

FUJ00171905

				and Out	and messaging is appropriate		
EUM-HBE-ISU-010	Inactive Stock Unit Rollover	0.1	M	The solution shall not change existing system behavior towards Inactive SU rollover, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users completing Inactive SU rollovers and messaging is appropriate	TST	Testing: 6
EUM-HBE-TCO-010	Transaction Corrections	0.1	M	The solution shall not change existing system behavior towards Transaction Corrections, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users processing Transaction Corrections and messaging is appropriate	TST	Testing: 6
EUM-HBE-TAC-010	Transaction Acknowledgements	0.1	M	The solution shall not change existing system behavior towards Transaction Acknowledgements, regardless of being logged on at more than one counter at a time.	Incumbent system behavior should be confirmed following solution change. i.e. regression tests should confirm the counter maintains the integrity of users processing Transaction Acknowledgements and messaging is appropriate	TST	Testing: 6

FUJ00171905

11 Internal Requirements Traceability Matrix

This section lists the internal requirements and provides cross references to the where in the solution the requirement will be met. The internal requirements are presented in sets as defined by the current POA team which defined the requirements.

11.1 GDPR Requirements

There are no explicit GDPR requirements.

The changes made do not impact the GDPR position of the counter or data centre.

11.2 Third Line Support

The table below lists the requirements defined by the SSC for third line support.

Requirement Number	Requirement	Response
GENERAL		
TLS_GEN_001	If the design for the support of the system depends upon tools, these must be formally delivered to the relevant support team. (Development tools are not available to live support teams unless they are productised and formally delivered.)	No additional tooling is needed for support.
LOGGING		
TLS_LOG_001	The solution design and the individual component designs must aim to ensure that sufficient information is available about the processing and data begin processed to diagnose problems during live operation. **This MUST be designed with GDPR and Data Privacy in mind, obfuscating sensitive data wherever possible at the point of logging**	The existing counter and BAL error handling and reporting strategies are used.
TLS_LOG_002	For data flows that are part of a transaction, it should be possible to associate the logging of that data in each application within the system that manipulates the data. **This MUST be designed with GDPR and Data Privacy in mind, obfuscating sensitive data wherever possible at the point of logging**	The existing counter and BAL error handling and reporting strategies are used.
TLS_LOG_003	If a COTS product is being used, guidance must be documented for reading the log files generated by the product and relating the logged information to the Horizon system. Configuration should be applied to comply with GDPR	N/A. There are no changes to the COTS products for this project.

FUJ00171905

TLS_LOG_004	If there are security restrictions on who may read the support logs these must be documented in the support guide.	N/A No changes to who can read support logs.
TLS_LOG_005	The Design must explicitly state that log files (and their containers) allow read access to support users.	N/A No new log files generated.
TLS_LOG_006	The syntax and semantics of the data in the log files must be documented. The syntax definition should include a definition of: • the field separators (if any) • the record separators (if any) • the character set used	N/A No changes to the existing log file formats.
TLS_LOG_007	It should be possible to automatically parse the log files and identify record separators using simple short scripts.	N/A No changes to the existing log file formats.
TLS_LOG_008	The solution should ensure that all logs are switched at least daily. One of the switches should be at a fixed time each day; The preferred time is 00:00:00.	N/A No new log files produced.
TLS_LOG_009	There should be no 'lazy' writes. Each record should be flushed immediately.	N/A No changes to the log writing code.
TLS_LOG_010	The log filename path and pattern must be documented. The filename must include the date that the file was created.	N/A No changes to the existing log file formats.
CONTRACTUAL COMPLIANCE		
TLS_CON_001	The solution must enable the operational support teams to measure the attributes of the system performance covered by contractual limits and operational level agreements.	N/A No changes to the existing measurement techniques.
SYSTEM MANAGEMENT		
TLS_MGT_011	The solution must include processes for house keeping log files to ensure that disks do not fill up.	N/A No new log files produced
TLS_MGT_012	From experience additional information is written to the logs that is too verbose to be written to the events, such as stack traces. Thus, application log files are a primary source of information used by support staff when diagnosing problems. Due to the amount of time it takes for a customer to raise an incident for	N/A No change to log file retention periods.

FUJ00171905

	investigation it has been found that 1 month is the minimum that the SSC would like for the log files to be retained. So, at least one month of logs must be retained, more if the logs are low volume. The solution must support at least 1 month log data.	
SYSTEM MAINTENANCE		
SYS_MNT_001	The design of each component of the system must allow for upgrade of that component to a later version without breaking operational level agreements.	N/A No change.
MIGRATION		
ARC_MIG_001	The design of changes to the system should aim to minimise the constraints imposed on migration for the order in which he changes are deployed. For example, if an interface is changed between two components, the design should aim to allow the two components to be deployed in either order.	The normal deployment of BAL changes prior to counter changes is required. See section 8.

FUJ00171905

12 Summary of Dependencies

The following dependencies exist on organisations other than Fujitsu:

ATOS:

- Reference data changes. See section 5.
- UAT. See section 6.

Computacenter:

- HNG-A Counter Release, Rollout, and ability to back out or quickly fix forward if any live issues are identified.

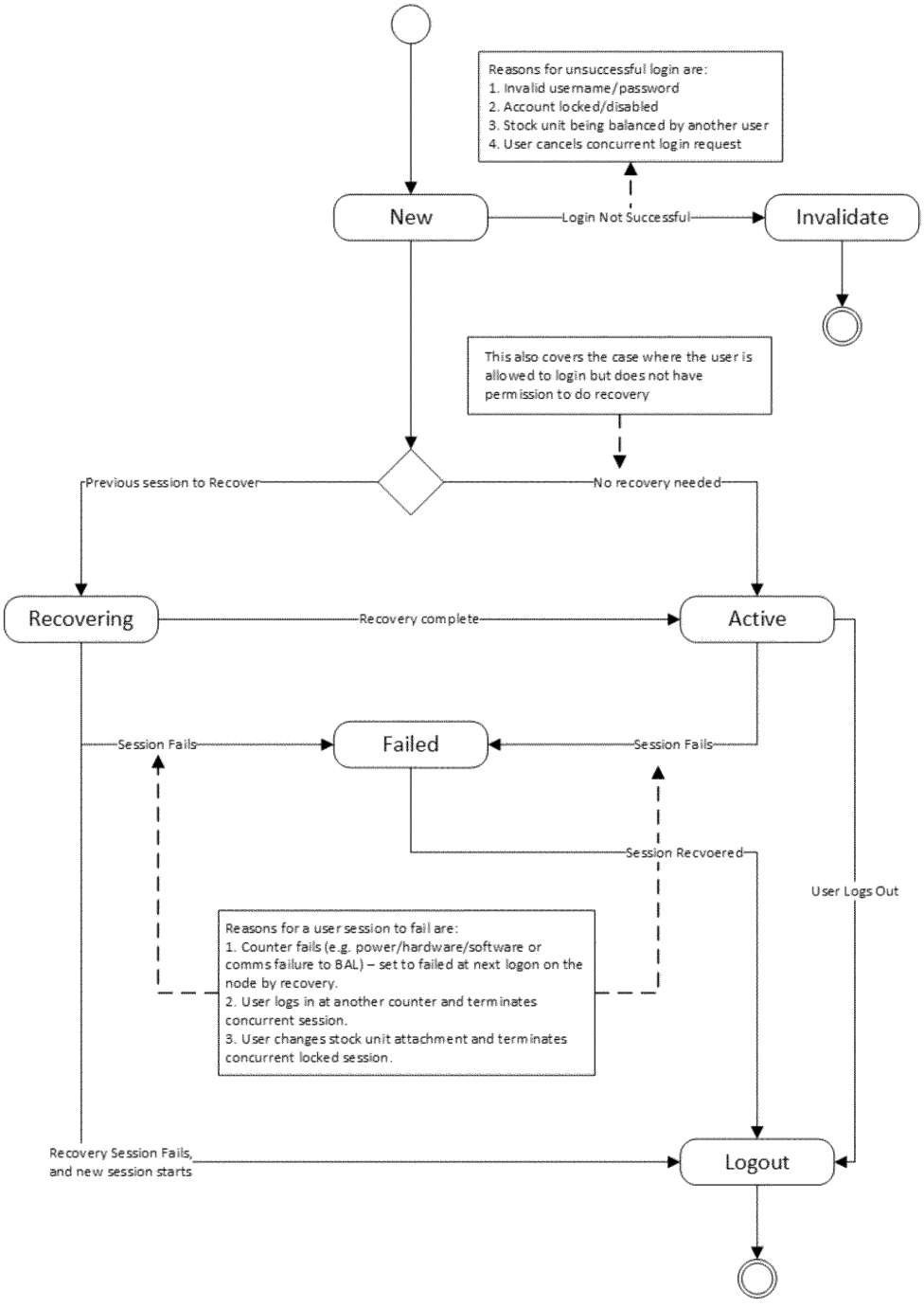
Post Office Limited

- Timely requirements clarification, as required.
- Release Acceptance and Authorisation

FUJ00171905

13 Appendices

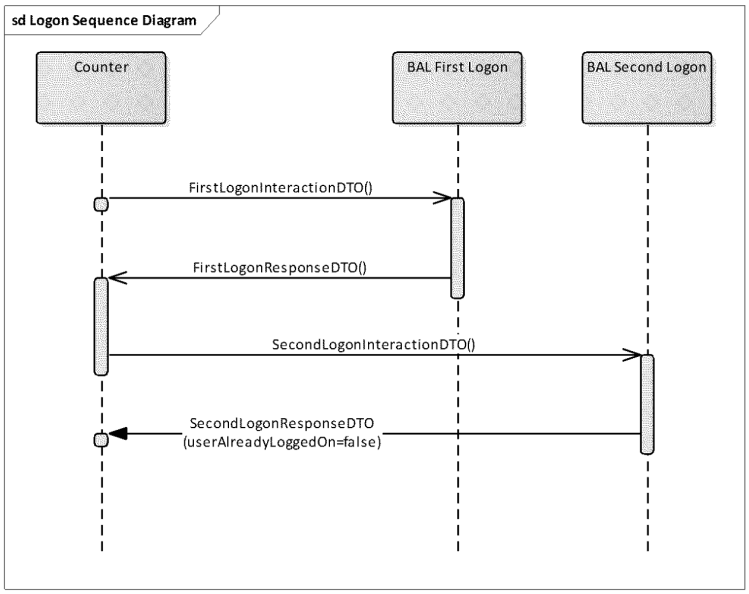
13.1 User Session States and Transitions



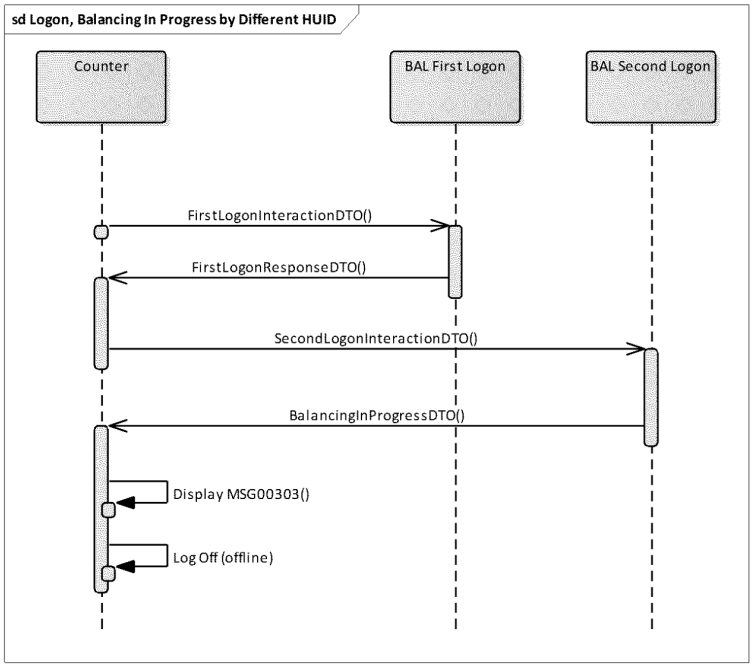
FUJ00171905

13.2 Existing Data Centre Interactions For Logon

13.2.1 Logon

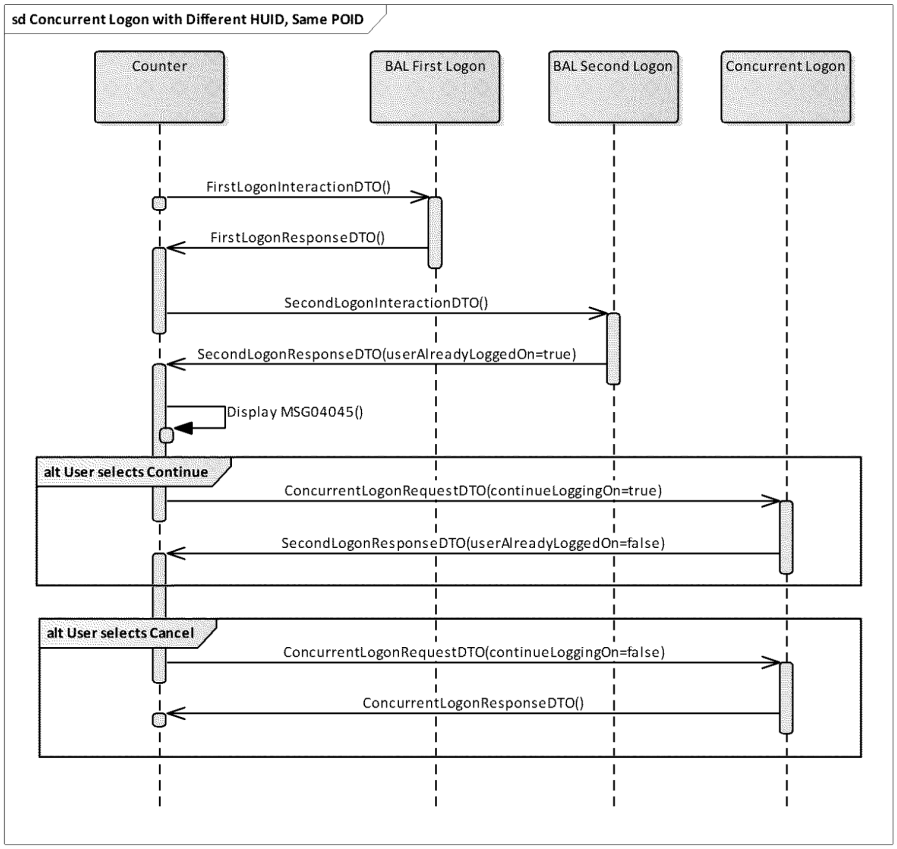


13.2.2 Logon but SU Locked



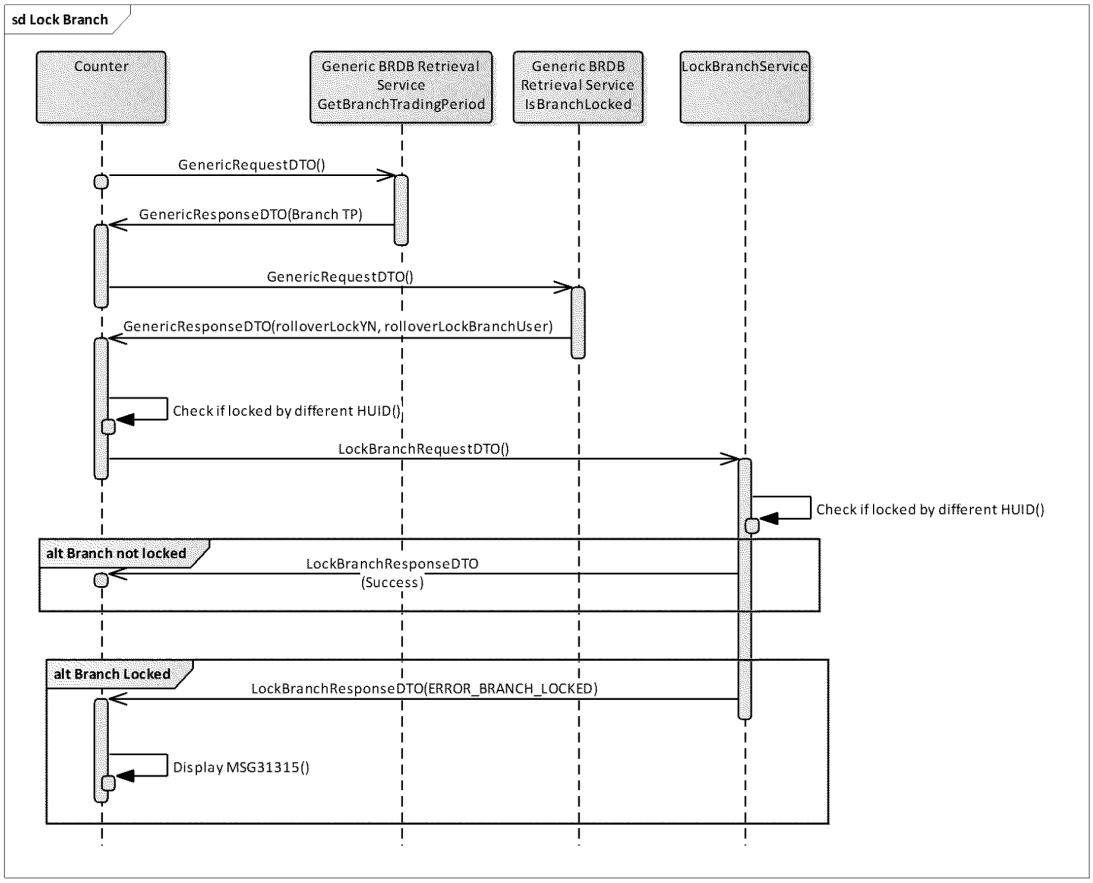
13.2.3 Concurrent Logon

FUJ00171905



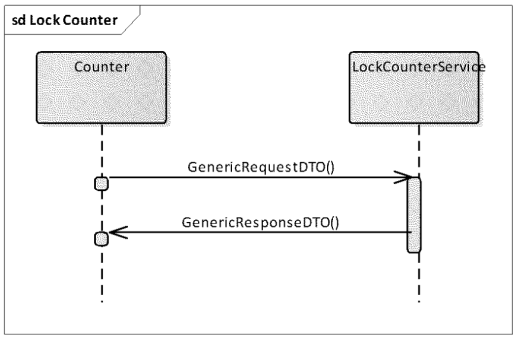
FUJ00171905

13.3 Existing Data Centre Interactions For Lock Branch



FUJ00171905

13.4 Existing Data Centre Interactions For Lock Counter

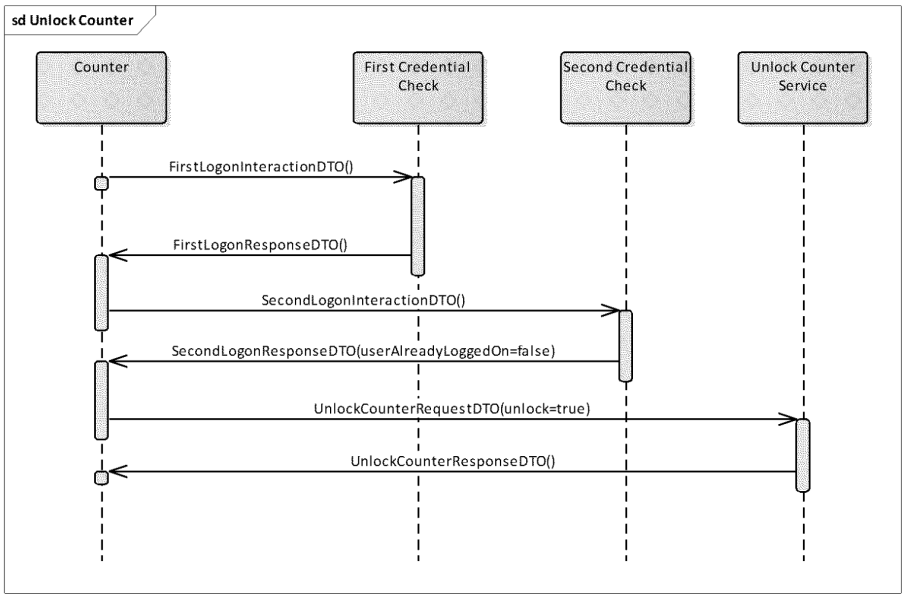


FUJ00171905

13.5 Existing Data Centre Interactions For Unlock Counter

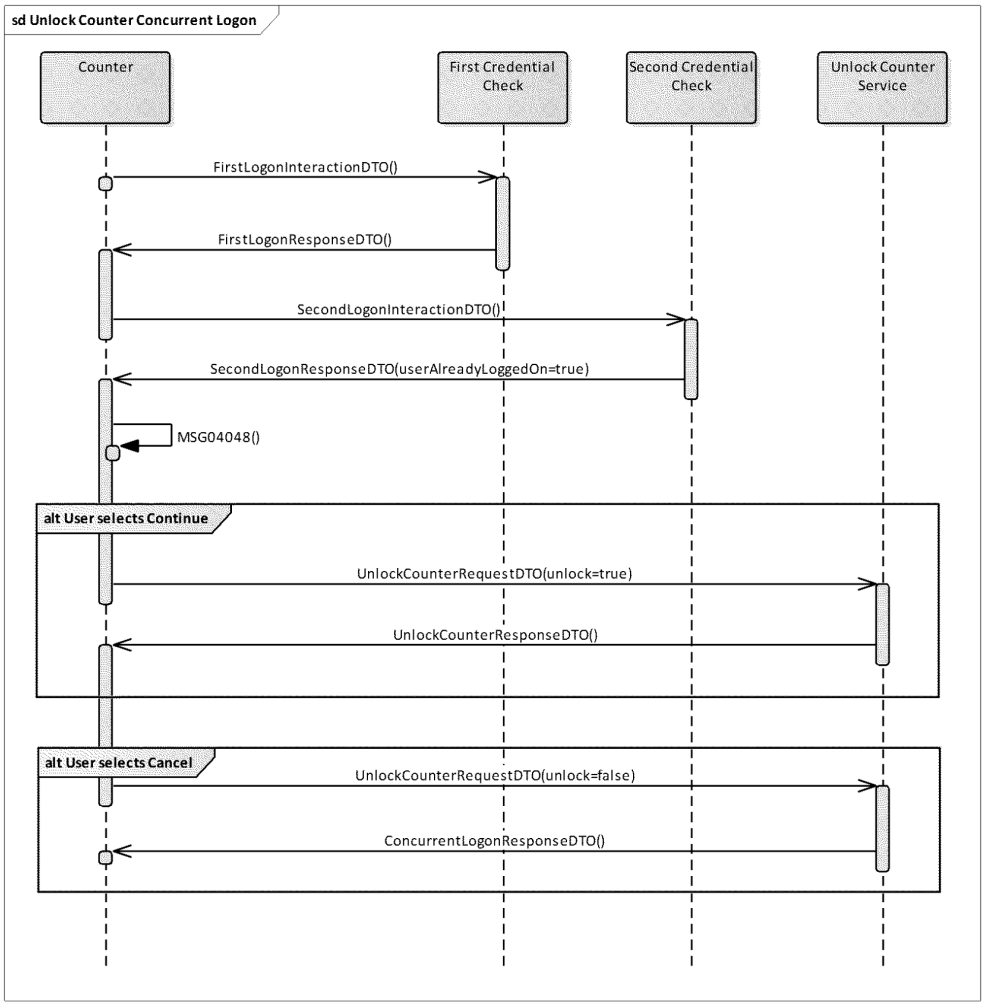
These flows are not changed by this project, but the UnlockCounterRequestDTO will pass additional fields holding the current TP, BP and stock unit (see section 4.4).

13.5.1 Normal Unlock



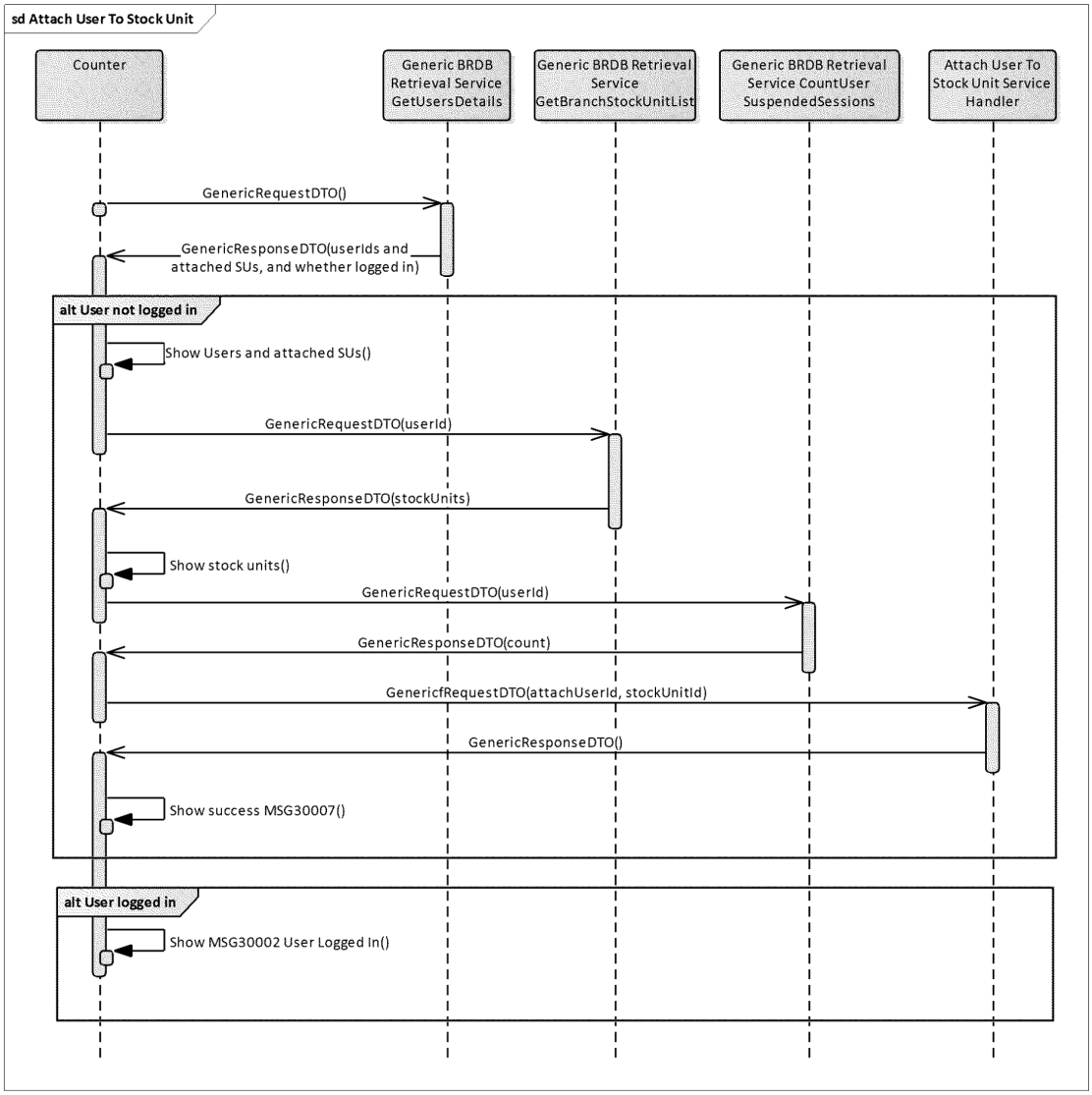
FUJ00171905

13.5.2 Unlock, Concurrent Session



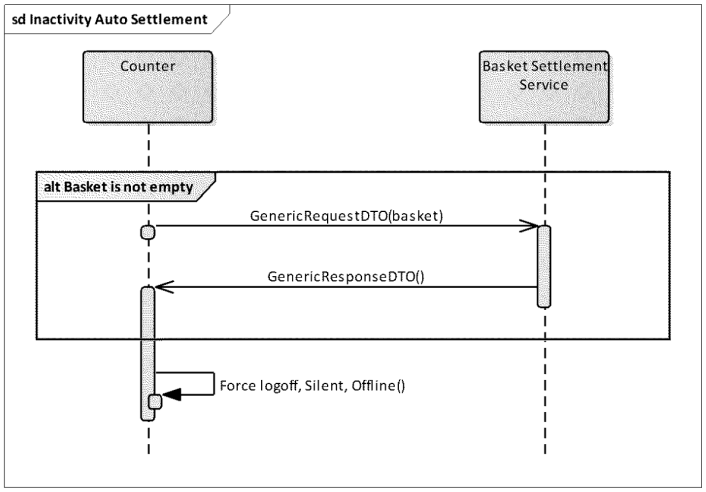
FUJ00171905

13.6 Existing Data Centre Interactions For Stock Unit Attachment



FUJ00171905

13.7 Existing Data Centre Interactions For Inactivity Auto Settlement

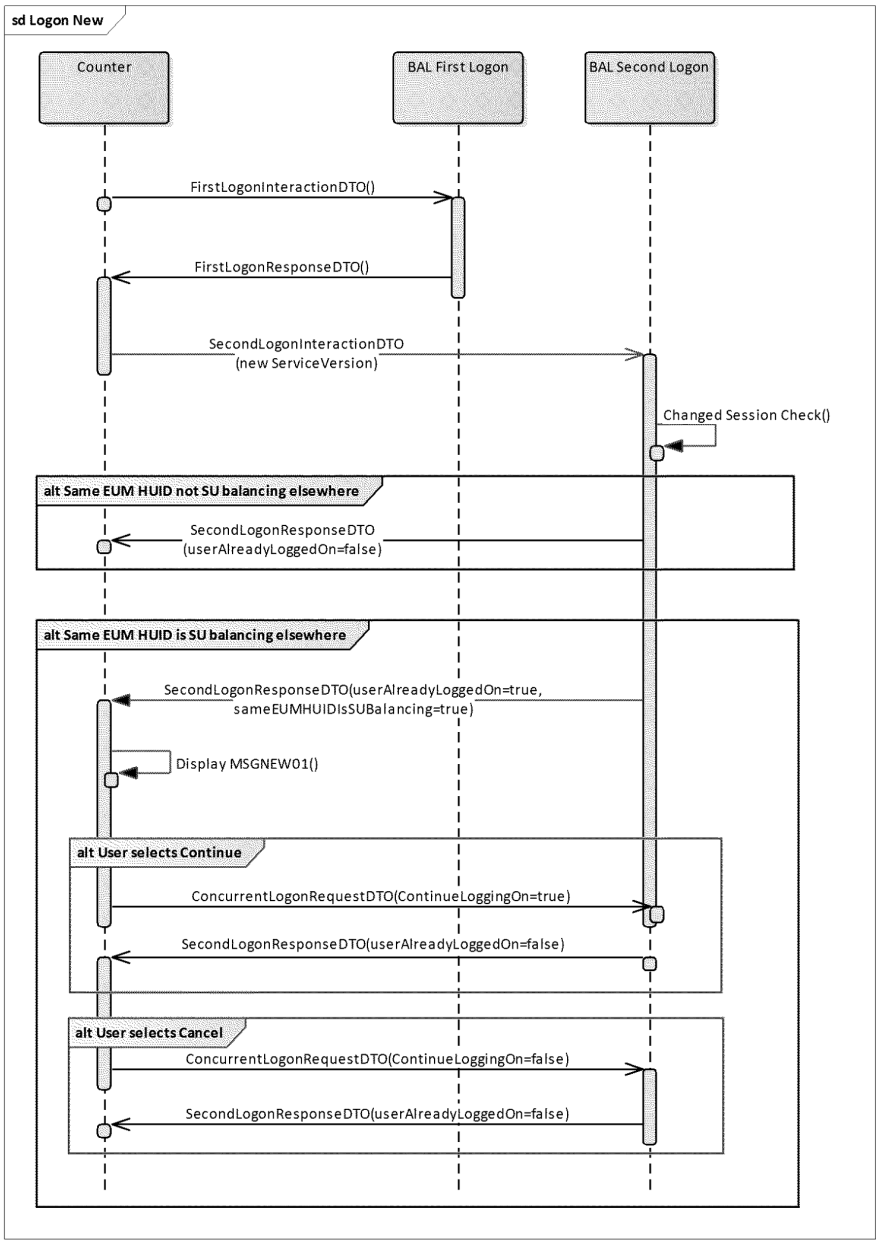


FUJ00171905

13.8 New Data Centre Interactions For Logon

13.8.1 New Stock Unit Balancing check

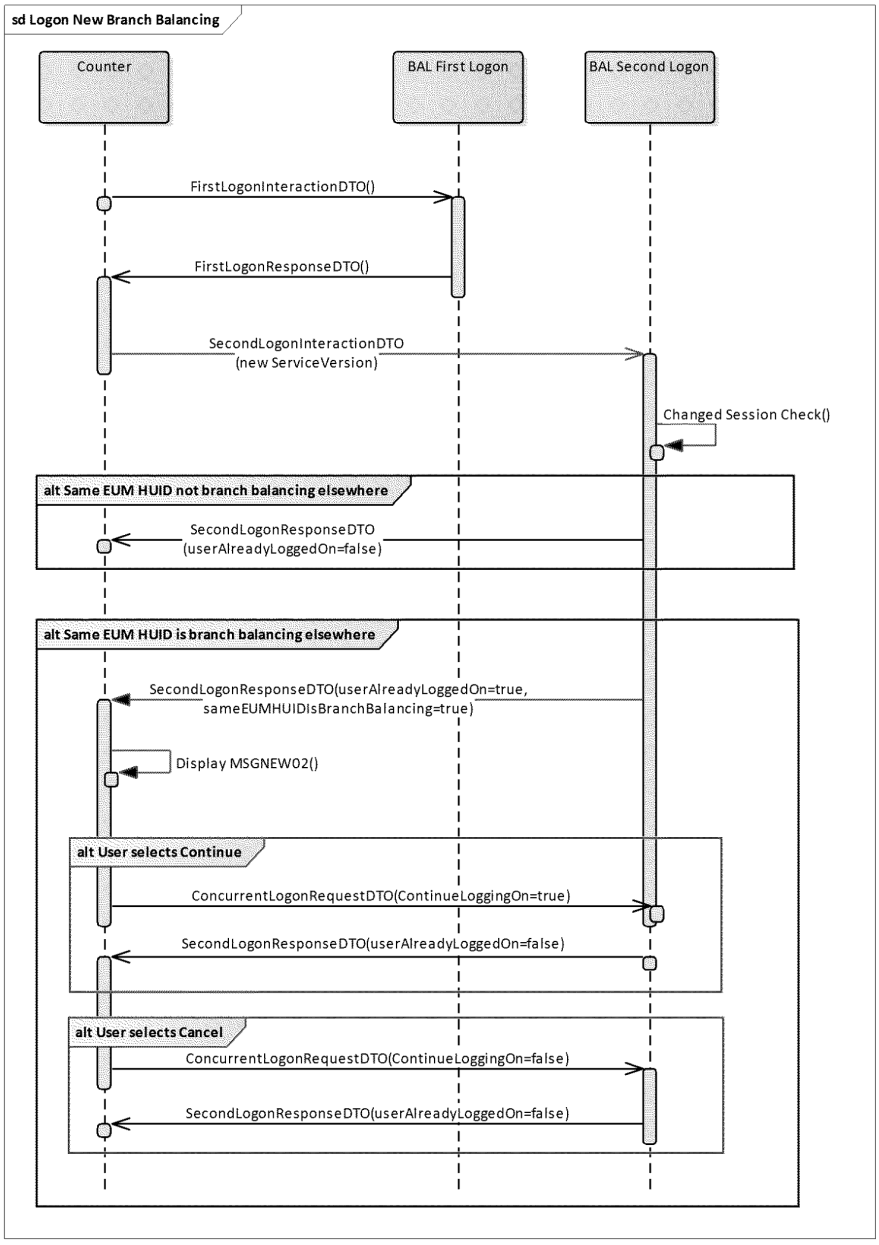
This diagram shows the changed interactions (in red) when the system detects that the same EUM HUID is balancing the stock unit on another node. See section 4.1.2.1.



FUJ00171905

13.8.2 New Branch Balancing check

This diagram shows the changed interactions (in red) when the system detects that the same EUM HUID is balancing the branch on another node. See section 4.2.2.1.

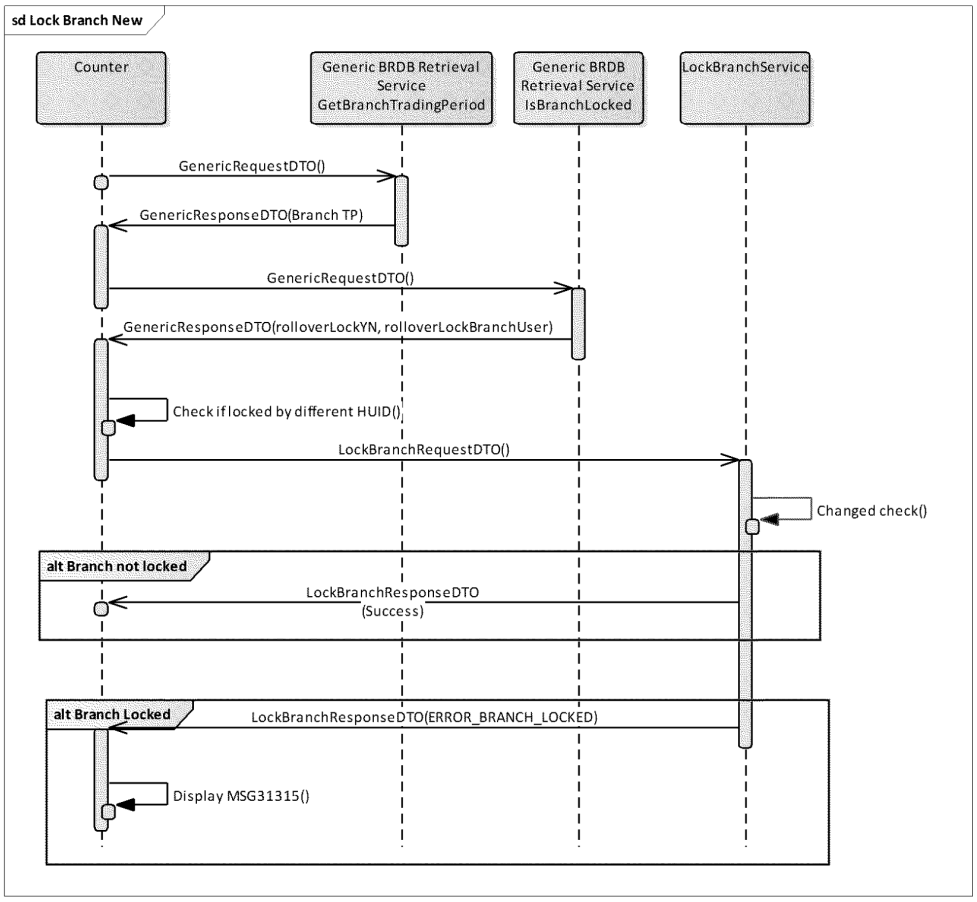


FUJ00171905

13.9 New Data Centre Interactions for Lock Branch

13.9.1 New Lock Branch Check

This diagram shows the changed interactions (in red) for the new lock branch check. See section 4.2.2.2.

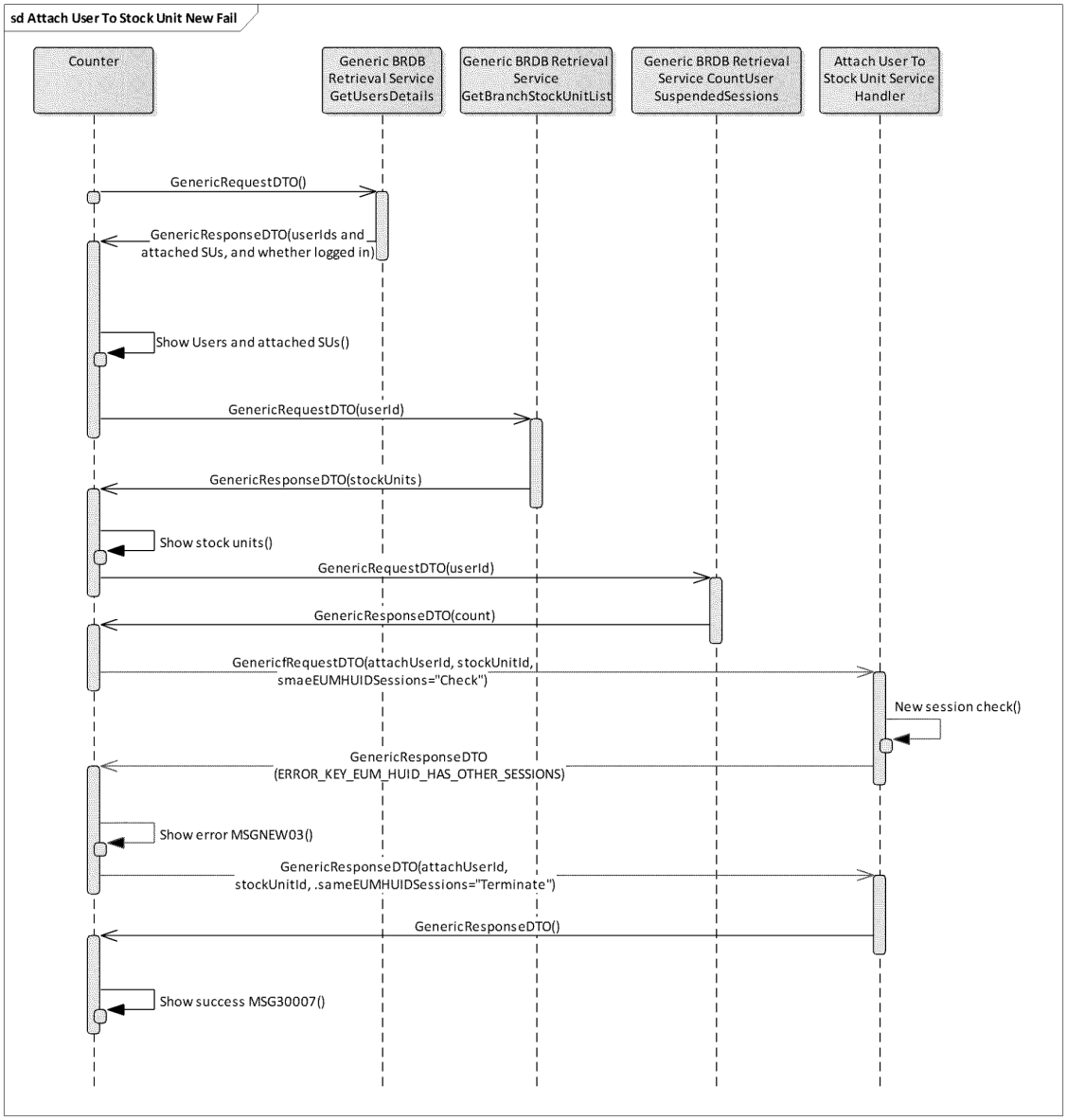


FUJ00171905

13.10 New Data Centre Interactions for Stock Unit Attachment

13.10.1 New Stock Unit Attachment Check

This diagram shows the changed interactions (in red) when the system detects that the same EUM HUID is logged in on another node. See section 4.3.

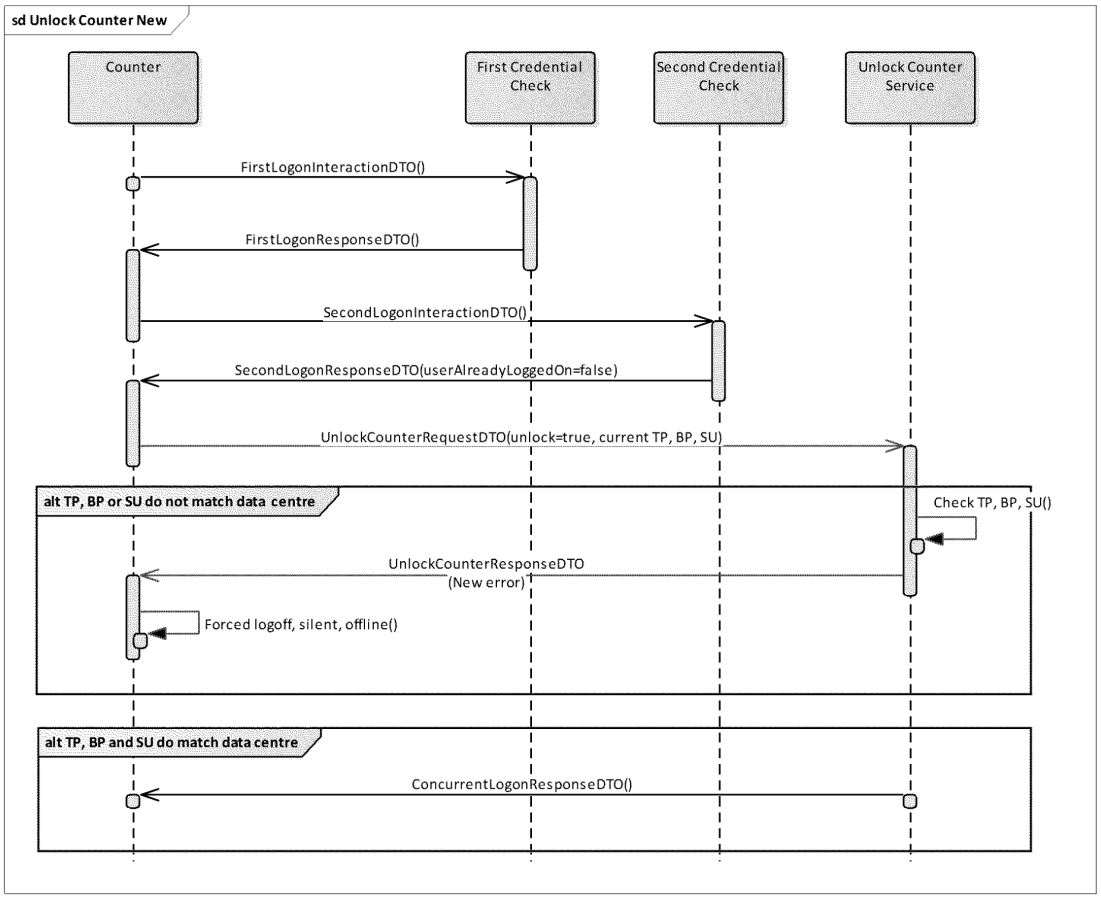


FUJ00171905

13.11 New Data Centre Interactions For Unlock Counter

13.11.1 New Unlock TP, BP and SU Check

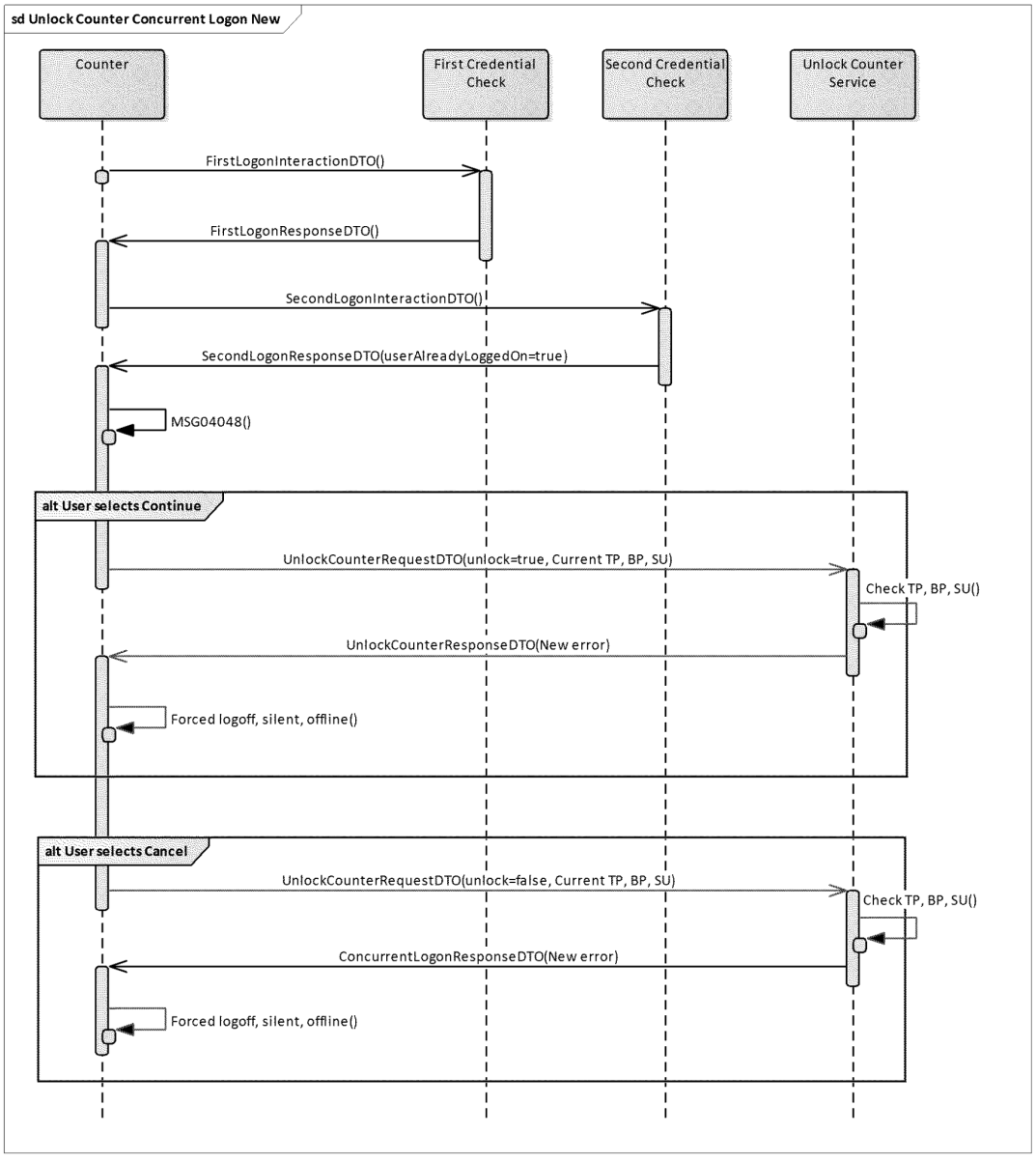
This diagram shows the changed interactions (in red) when the counter attempts to unlock, and supplies the current TP, BP and SU for checking. See section 4.3.



FUJ00171905

13.11.2 New Unlock Concurrent Session TP, BP and SU Check

This diagram shows the changed interactions (in red) when the counter attempts to unlock, finds that a session is concurrently logged on, and supplies the current TP, BP and SU for checking. See section 4.4.



FUJ00171905

13.12 New Data Centre Interactions For Inactivity Auto Settlement

13.12.1 New TP, BP and SU check

This diagram shows the changed interactions (in red) when the counter attempts to automatically settle a basket to cash due to inactivity timeout. See section 4.5.