POL00037819

Internal
Date: August 2020

Version: 2
Author: Shaun Turner

Horizon Multiple Login: Options Paper

1) Background

The original Smart ID technical build only allowed a user to be logged in at one terminal at time. This was driven by the compliance requirements to minimise the risk of users who were not vetted or trained being able to trade on the Horizon system. Completely unfettered multiple login access to the counter would have allowed multiple Horizon logins to be created (linked to the same Smart ID), passed out to other user who have not been vetted and trained, and all of those users would be able to transact on the counter at the same time, limited only by the number of counters in branch.

Prior to the rollout of the Smart ID pilot branches in June/July 2017 it was recognised that this model was too restrictive for multi-counter branches, particularly when related to back office work and Drop & Go transactions. The Restricted Use ID (RUID) was introduced as a temporary stop gap solution to provide flexibility whilst Fujitsu worked on a permanent multiple login solution.

The RUID was a branch level Smart ID issued to all multi-counter branches between which rolled out between July 2017 and August 2018, and was designed to be used for back office reports and Drop and Go transactions. Operational guidance was issued to the Postmaster/Branch Manager to make it clear what was permissible and what was not.

Fujitsu delivered the new Multiple Login functionality into the network during August 2018, which allowed a user to be logged in at multiple Horizon terminals, but with only one active (unlocked) session at a time. The RUID's were then phased out (deactivated) between September and October of 2018.

2) RUID Usage

During the period January to August 2018 before RUIDs were phased out the following summarises the usage in branches.

- In total 3771 RUIDs were issued to multi-counter branches
- Of these 2422 were not used at all (65%). This may seem like a large number, but it needs to be remembered old Horizon IDs were not deactivated until the branch had migrated sufficiently to Smart ID usage, so RUID use would be somewhat suppressed initially.
- For the remaining branches, which did use the RUID, the table below shows that over a quarter of branches (25.86%) used the RUID less than 10% of the days across the monitoring period. Only 21.42% of branches used their RUID over 50% of the days (i.e. every other day), and a tiny 1.22% used the RUID every day. This suggests that demand for the RUID is actually low, though as per point above it should be noted that old Horizon logins were also in use across this period also.

POL00037819

RUID Usage (% of days in use)	% of branches
Less than 10%	25.86%
10 - 19%	14.54%
20 - 29%	13.93%
30 - 39%	13.54%
40 - 49%	10.71%
50 - 59%	7.96%
60 - 69%	6.50%
70 - 79%	3.29%
80 - 89%	2.45%
Above 90%	1.22%

In addition, it should also be noted that as of the November 2019 version of the Configuration Database that **38% of branches have only 1 counter position** and therefore do not require a multiple login solution at all.

3) Audit Findings: Sharing of logins

One of the risks of the constraints which Multiple Login functionality places on counter staff is that it may lead to increased sharing of logins as a way to circumvent the system. Indeed, this is one of the central contentions put forward by the NFSP in discussions about Multiple Login.

Prior to the implementation of Smart ID, one of the compliance checks on an audit was to check the whether there was any sharing of logins. When Smart ID was introduced this check was removed from audits until January 2020 when it was reinstated. Looking at performance before Smart ID (using audit data from 2014/15) and comparing it to the checks between January and March breaks down as follows:

- Pre- Smart ID (c.500 audit results from 2014/15) – 11% of branch audits found evidence of sharing of login credentials
- Post Smart ID (219 audits where a check was done between Jan – Mar 2020) – 12% of branches were found to be sharing login credentials

4) Multiple Login Issues

This section documents the current issues which have been flagged with the Multiple Login functionality. All of the issues that have been raised relate to the operational impediments which result from having Multiple Login control on the counter. Compliance teams are broadly happy with the current solution, whilst accepting that it does not necessarily fix the issue of sharing Smart IDs, it does minimise its application.

POL00037819

4. 1 Inconvenience of Locking/Unlocking

Multiple login functionality slows down quick switching between counters (e.g. Drop and Go and standard counter transactions) by forcing, when a user wishes to switch counter positions, them to lock their current counter and unlock the one they wish to work on by entering their password. This slows the user down impacting the ease with which they can serve customers. It should be noted that security guidelines state that terminals that are not in use should be locked.

4.2 Back Office Administration Impeded

One of the limitations of the Fujitsu solution is that a terminal cannot be locked when displaying a 'transient message', the most common examples of which are when the terminal is printing a report or when it is awaiting customer input on the pinpad. The printing of reports and the fact that the user has to wait for the transient message to clear before they can lock the terminal has been raised as an issue, due to the fact that the user has to wait for the 'transient' printing message to clear from the screen so they can lock the terminal. This is cited at a particular issue with busy end of day printing of reports for cut off whilst trying to serve customers on another counter.

4.3 Receipts & Payments Misbalances – FIXED Sept 2019

Multiple login functionality allowed a user with the same Horizon ID (e.g. ABCD01) to be logged in at more than one terminal providing only one of the sessions was active (unlocked). Fujitsu identified in cases where a SU or Office Balance was initiated in those circumstances then it could cause receipts and payments misbalances in the branch which had to be corrected by a Transaction Corrections.

These issues were fixed by the Horizon release in September/October 2019, which put in place further controls on multiple logins related to Stock Unit and Branch Balancing and changing Stock Units.

4.4 Session Terminations

Multiple logins increases the chance of Horizon sessions being inadvertently terminated. In most cases this will be due to a use logging in (or unlocking a session) without locking their other session(s). Screen messages do give the option to abort the login (or unlocking) or continue and terminate any other active sessions.

The above scenario does place constraints on the user (one active session at a time), but does represent the system operating as per the requirements given to Fujitsu. There are two more obtuse cases which can cause session terminations:

POL00037819

- The user has moved branches and their Smart ID is still being used (in breach of contract) in their old branch. Due to the fact multiple login controls operate across the Network, not within just one branch, a user with an active session will be logged out when someone logs in at the same time using their Smart ID in another branch. These cases are few and far between (5 per year) and the solution is to give the user a temporary ID and deactivate their ID whilst the issue is resolved with the offending branch.
- Users logging in and kicking out an existing locked session. This is a scenario flagged recently by the NFSP and occurs where User 1 is logged in on 2 terminals, one locked session (Terminal 1) and one active session (Terminal 2). If User 2 comes to Terminal 1 and seeing it locked decides to log in themselves anyway, this not only kicks User 1 off Terminal 1, but because Horizon has to effectively unlock that session in the background, it terminates User 1's active session as well. The issue is compounded by the fact that User 1 will not be aware their active session has been terminated until the counter tries to contact the data centre, which is normally on the settling of a basket (a real pain if you have been doing Drop and Go). Provisional Fujitsu analysis suggests between 45-50 occurrences of this type of scenario per week, although not all of these were where transactions were in the basket on the active session.

It should be noted when there are session terminations, whatever the cause of them, any transactions in the basket are subject to standards Horizon recovery processes when the next user logs in to that terminal. Furthermore, such recovery processes predate the introduction of multiple login functionality and cover scenarios

4.6 Additional Issues Put Forward By NFSP

Bulk transactions like Drop & Go and bulk car tax issuing for garages are highlighted as examples of where the constraints of the system become restrictive or more prone to error. These are often done by one individual switching between the bulk transactions and customers coming to the counter. The necessitates locking and unlocking on a frequent basis and if mishandled can lead to inadvertently triggering a forced logout on one of the terminals (e.g. if the user forgets to lock one terminal, or if another user logs them out as per Section 4.4)

Outreach terminals are similar to the scenario highlighted above, where in cases that the outreach business is concluded the Horizon terminal is brought back to the core to perform back office functions (dispatch, balancing) a user will need to be potentially switching between the outreach terminal and serving customers on the core branch counter.

POL00037819

4.6 Impact of Multiple Login Issues

Now that the issue of receipts and payments misbalances (see Section 3.2) has been fixed, there should be no financial impacts in branch related to multiple logins. The principle impact is therefore as follows:

- Operational inconvenience – the unlocking/locking time and issue with back office 'transient' messages can be seen to stymie full efficient operation at the counter.
- Mistrust of the system – Session terminations, especially from the second issue (user 2 logging in over a locked session of user 1), can create a mistrust of the Horizon system no more so than when the session terminates with transactions in the basket. Although any such transactions would be subject to standard recovery processes and would not be lost, the context of the GLO means terminated sessions could be exploited as a way of explaining branch losses.
- Sharing/Recycling of Smart IDs – The main claim from the NFSP is that the controls around multiple logins are too rigid and will force branches to look for ways around the controls, namely the sharing and recycling of Smart IDs. The opportunity for the recycling of Smart IDs is certainly large given the churn in the network, with the Dormant Smart ID process deactivating around 800-100 accounts per month which have not been used for 90+ days.

5) Multiple Login Options

This section lays out, at a high level, the various options on multiple logins considering some of the issues highlighted above. All costs and delivery timescales are indicative based on previous work of a similar nature. Note: All the costs below are development and ongoing staff costs,

5.1 Fundamental Technical Change (Fujitsu Solution)

Cost: £300k **Delivery:** 9 – 12 months dependent on release slot

Delivering a comprehensive solution which addresses all the issues above will require Fujitsu development of the Horizon solution and therefore considerable development, testing and deployment costs.

The ideal solution would have the following requirements:

- A single additional login which can be enabled on a branch by branch basis via reference data.
- The login can be associated with one Smart ID at a time via a revised User Management Horizon screen.
- The additional login would apply the training controls based on the Smart ID it is linked to.

POL00037819

- The additional login will not be subject to Multiple Login controls so it can be logged in with and active whilst the user has one active session on their Smart ID.
- The additional login should have access to all back office functions and Drop and Go, with the facility to add additional capability via reference data if required.

Pros	Cons
✓ Addresses issues concerned by having a login which is not constrained by multiple login controls ✓ Can be restricted by branch so it is only deployed in branches with a proven need ✓ Provides traceability of transactions by mapping the additional login to a Smart ID ✓ Fine grained control over what transactions are possible ✓ Maintains integrity of training controls ✓ No Accenture development required ✓ No additional resource required to manage new administration and monitoring processes	× Expensive and will be difficult to get business case signed off × Allows an unvetted user to access the system, albeit constrained to doing the permissible transaction types × Complex solution for an issue which is not universal to all branches × Limited shelf life if existing Horizon is replaced in the next 2-3 years. × Would require the addition of new reference data structures if the facility to control by branch and control the transactions is in the requirements

5.2 Reinstate Restricted Use ID (RUID)

Cost: £15k per annum staff costs **Delivery:** 1 month

This solution would reinstate the use of the RUID in a more tightly controlled way than previously. The RUID usage statistics in Section 2 of the document suggest that not all multi-counter branches would require a RUID, so they should only be issued based on a criteria assessment.

There are two potential variants of this approach that could be considered:

1. Back office administration functions only – This accepts that the current multiple login functionality is acceptable for multi-counter transactional work (e.g. Drop & Go), but provides an additional login to be used for back office facilitating easier end of day cut off processes, preparing remittances, completing cash declarations etc.
2. Back office administration and Drop & Go – This is the same as the original RUID on which it would be permissible to do Drop & Go and back office administration.

The issues with this approach remain the same, in that the RUID cannot be locked down to certain transactions (this could be achieved to some extent by Accenture development – see Section 4.3 below) and therefore would require a monitoring and intervention regime. The costs listed above are the ongoing staff

POL00037819

costs needed both from a data analysis and intervention/administration perspective.

A monitoring regime would need to be set up to include the following controls on RUID usage:

1. Warnings where the RUID is used for 'unauthorised' transactions and ultimately deactivation. Depending on how strict the regime, it could be something like a 3 strikes process where the RUID is deactivated on the 3rd offence. This would allow a couple of mistakes where the branch inadvertently serves on the RUID.
2. Temporary deactivation of the RUID in cases where not everyone in the branch has passed the core trainings (AML, Info Security, and, if the RUID can be used for Drop & Go, Mails and Prohibited & Restricted). This would reduce (but not remove) the risk of having a user who has not passed the training using the RUID

Pros	Cons
✓ Minimal cost and time to set up as utilises existing technical solution ✓ Familiar solution for those branches that used RUID previously ✓ RUID can be activated only in branches with a proven need and based on business criteria (Area Manager sign off could be a requirement)	× Loosens compliance, as even with the controls in place, an unvetted user could access the counter using the RUID × Regulated financial services and insurance products could be transacted on the RUID where the FS and Insurance tests are passed (mitigated by option 4.3 below). Sanctions for misuse can only be applied after the fact. × Ongoing costs in Branch Standards in monitoring and administering RUID misuse × RUIDs can be used by anyone and therefore transactional traceability would be broken

5.3 Minor Technical Change (Accenture Solution)

Cost: Option A: £30-40k & 10k per annum staff costs **Delivery:** 3 – 6 months

Option B: £60-70k **Delivery:** 3 – 6 months

Option A - Basic

POL00037819

This option is supplementary to option 4.2, so presupposes that RUIDs have been reissued, but it does provide some additional control around Financial Services. As noted above, one of the issues with RUIDs is that if someone passes the Financial Services and Insurance test on the RUID, it can then be used to transact regulated financial products. Given the RUID cannot be tied to an individual, any regulated products transacted on it would be a cause of concern, but especially financial services.

This solution would mean Accenture changing the Smart ID solution so that Post Office could select which training updates they wish to have applied to the RUID training record. If the RUID was only used for back office administration functions, the only training that would be permitted on the RUID training record would be AML and Information Security, whereas if the RUID was used for back office and Drop & Go, then updates for Mails and Prohibited & Restricted would also flow through to the RUID.

This solution would need to be used in conjunction with 4.2 above and therefore these pros and cons are additional.

Pros	Cons
✓ Provides a better control around regulated products than just the vanilla RUID solution (Section 4.2 above). The products which count as 'regulated' can be controlled through reference data providing some future flexibility ✓ Technical changes are contained within the Accenture environment reducing development costs compared to option 4.1 ✓ Slight reduction in monitoring costs due to ability to block certain regulated products entirely	× Does not remove the need entirely for monitoring given some banking transactions are not considered 'regulated' products

Option B – Enhanced

This option would need to supplementary to option 4.2 **and** would build on top of the functionality in option A above. The benefit it has over Option A is that, whereas Option A allows lock down of selected regulated products it can only do so for those products linked to an existing curricula. This option would allow lockdown of a wider list of products.

It would achieve this by introducing a new curricula and Product Group. The Product Group would be linked to the products that the business wants to deem out of scope for the RUID but not covered by existing curricula. For Smart IDs marked as a RUID, the curricula would be set by default to be incomplete or will not be sent to Horizon, meaning the user will never have access to those linked products.

POL00037819

All other non-RUID Smart IDs will get the curricula by default and each time an update to training is sent, the new curricula will be sent to Horizon with a fixed expiry date (e.g. 31/12/9999). This means for them the products would be always be available by default.

This solution would need to be used in conjunction with 4.2 above and therefore these pros and cons are additional.

Pros	Cons
✓ Allows control of more products than just those linked to existing curricula. This is the principle advantage over Option A ✓ Removes the need for monitoring of RUID usage	× Adds a further level of complexity into the reference data. × Complicated implementation to ensure that users do not get locked out × Lack technical coherence as it is essentially 'fudging' the existing system × Has technical risks in that if this new curricula was ever invalidated in the data it could lock out

5.4 Accept Existing Solution

Cost: N/A **Delivery:** N/A

The existing solution has issues but it arguably still represents the best compromise position between compliance on one hand the branch operations on the other. All the solutions proposed inevitably loosen controls and give greater opportunities for unvetted users to operate on the counter than now and from a risk perspective, compliance teams within the Post Office may not be prepared to sign off on the proposals.

Branch voices, like the NFSP, would argue that the restrictions of the current system just means that people find hidden ways to circumvent the system anyway by sharing and recycling Smart IDs. It is very difficult to evaluate these arguments statistically, as the very nature of the method means it is invisible in any Horizon management information that can be extracted.

It is also not possible to fully evaluate to what extent the implementation of a RUID type solution would reduce one problem (sharing of IDs) to increase another (unvetted users being put on the counter). The best that can be done is to look at some data sources which may be indicative of ID sharing.

Prior to Smart ID and up to part way through the Smart ID rollout (August 2018), Field Advisors checked on audits whether any of the staff in the branch were not vetted. For the period from 2013 to 2018, 7.5% of audits found there were 1 or more unvetted users working on the counter, in the first 8 months of 2018 (after which Field Advisors no longer checked), this has dropped to 1%. Smart ID was rolling out over that period and the data capture exercise was ensuring everyone was vetted. (**Note:** I have requested this check be added back into audits and will be monitoring from January 2020 onwards).

POL00037819

A second way of trying to judge ID sharing/unvetted users is to compare the name input in Horizon when a user takes a compliance test and that which is held on record for them in the Smart ID system. This of course does not take account any user who might falsify the name to match that against the Smart ID and, on the flip side, those users who misspell their name, transpose their forename and surname or use a diminutive version of their name.

Those constraints aside, all things being equal you would expect the mismatches to be more prominent in multi-counter branches Smart ID constraints are causing issues, but this is not the case, with single counter positions showing a 7.7% level of mismatch and multi-counter branches showing 7.3%.

This means, albeit based on an imperfect data set, that there is no strong evidence that ID sharing/unvetted significantly correlates with multi counter operation. When audit data starts to come in from January 2020, it will then be possible to analyse with a more robust data set.

Finally on the existing solution, for the issue described in Section 3.4 of a second user logging on to a first users locked session thereby terminating the first users active session, this can be mitigated to an extent by improved screen messaging through the BAU Atos reference data change process.

Pros	Cons
✓ No additional cost ✓ Approved by compliance and security teams with Post Office. ✓ Avoids additional complexity in an already complex solution ✓ Avoids building on technology which may ultimately be replaced (Horizon replacement) ✓ Improved screen messaging mitigates the issue of a second user logging in described in Section 3.4	× Does not fix any of the issues noted in Section 3 and therefore may result in branches finding workaround (i.e. sharing IDs)

6) Next Steps

The following should be the next steps:

- Update existing Horizon screen messages to try and mitigate the issue of a user logging in to a locked session of another user. This can be done through existing BAU processes.
- Further analysis of data from January 2020 of audit returns to ascertain the real level of shared IDs/unvetted users and compare between single counter multi-counter branches.
- Socialise the options with colleagues in compliance and security to ascertain the appetite for making a change and establishing potential risks.

POL00037819

- Options which require technical changes will need a business case to be raised and be subject to standard project governance.

POL00037819

Summary of Options

Ref	Description	Est. Cost (£k)	Est. Delivery Timescale	Summary
4.1	***Fundamental Technical Change (Fujitsu Solution)*** Fujitsu introduction of branch level ID which can be linked to a single existing user and with access to products and functions configurable	300	9 – 12 months	Complicated and expensive but gives a solution which could be configured to meet branch and compliance requirements. Current business climate makes it unlikely a business case would be signed off
4.2	***Reinstate Restricted Use ID*** Controlled reintroduction of RUID in branches with proven need and monitoring regime to prevent misuse	15 per annum	1 month	
4.3a	***Minor Technical Change (Accenture Solution)*** This is a more compliant version of 4.2 but has to be paired with that option (i.e. cannot be delivered in isolation). The additional benefit of this option is it would enable to blocking of certain regulated products entirely	10 per annum +30-40 one off	3 – 6 months	
4.3b	***Minor Technical Change (Enhanced Accenture Solution)***	10 per annum +60-70 one off	3 – 6 months	
4.4	***Accept Existing Solution*** Accept existing solution with its known limitations. Improve on screen messaging to mitigate the issue of a second user logging out the first (section 3.4)	0	N/A	

POL00037819

