SCHEDULE 2.1

SERVICES DESCRIPTION

Services Description

1 DEFINITIONS

In this Schedule, the following definitions shall apply:

"BACS" means; an electronic system used to make payments directly from one bank account to another.

"FILEACT" means; a secure channel for the transfer of large files of data.

"FIN" means; a message type (MT) that transmits financial information from one financial institution to another.

"SWIFT" means; a messaging network that financial institutions use to securely transmit information and instructions through a standardised system of codes.

2 INTRODUCTION

2.1 Government Banking (GB) is a shared government function which provides critical banking services across central government and for wider public sector customers.

2.2 GB is the money transmission conduit for government departments and the wider public sector and as such represents a vital function for government. It is responsible for holding balances and facilitating banking transaction services to around 700 public sector customers and fully contributes to HM Revenue and Custom’s aim of ensuring money is available to the UK’s public services. Additionally, the services provided by GB help HM Treasury to minimise the cost of government borrowing and supports its cash management. To facilitate HM Treasury goals Government Banking supplies reports on an intraday and next day basis of government department’s receipts and payments currently broken down by transaction type (Bacs, Faster Payments etc.).

2.3 GB became operationally effective in 2010 following the Bank of England’s decision to exit from transactional banking and a HM Treasury review, which recommended that banking services for government and the public sector should be procured from commercial banks.

Government Banking's key objectives:

- Provide timely, accurate reporting to HM Treasury
- Minimise balances in commercial banks
- Provide 'value for money', modern money transmission service across Government
- Be the voice of Government into the payment industry

2.4 HM Treasury is responsible for providing the Debt Management Office (DMO) with long term, medium term and real-time forecasts of government flows. These forecasts provide an essential basis for setting the DMO's execution strategy of cash management operations in the market helping the DMO make better use of opportunities in the financial markets to even out future cash flows by borrowing and lending money for the government as a whole at the best rates.

2.5 HM Treasury run a Cash Management Scheme covering the forecasting of gross departmental cash flow and its outputs are used to inform the forecasts submitted to the DMO. HM Treasury also lead and advise on cross-government cash management policy and work with Government Banking to minimise balances in commercial banks.

2.6 In 2013 GB made the decision to move on from their bespoke, in-house developed system, 'Government Banking Management Application (GBMA)' and to procure a third-party bank sponsored SWIFT bureau service. The existing contract for these services is due to expire in April 2021.

2.7 Instead of bulk files being sent by the banks which were of a cumulative nature (i.e. data from 8am was also reported in the 4pm file), GB intends to move to industry standard SWIFT messages transmitted over the SWIFT Network. The advantage of this system is that it reports on accounts on a movement only basis and does not duplicate data.

The current application has been modified to allow us to create the required outputs and it is our aim to move to a more standardised solution.

This Schedule sets out the intended scope of the Services to be provided by the Supplier and to provide a description of what each Service entails.

3 SERVICES DESCRIPTION

The parties agree that the following clauses do not apply and are specifically excluded from the Services: 3.3.7 sections c) to h), 3.3.20, 3.3.25 -3.3.44, 3.4 – 3.4.8, 3.5 – 3.5.8 (all inclusive). This content may be available at a future date subject to the Change Control procedure.

3.1 Mobilisation –

3.1.1 The Supplier, as the incumbent, is able to access both systems simultaneously, provide live data feeds into both environments (i.e. Live FTR and Test PCM) and manage all aspects of the data and configuration migration between the old and new platforms. Not having to manage an external third party and broker a means of securely managing data transfers into the external providers services will make the overall migration project much less complex.

3.1.2 The Supplier will supply a Test PCM service which will physically become the live platform once the project has sufficiently progressed. Essentially, this will enable the Authority to continue to use this environment post go-live without the need to build and update another environment which would require further testing prior to live use.

3.1.3 For a period to be determined by the Authority (and agreed with the Supplier), the Supplier will offer access and feed data into both PCM and FTR, enabling the Authority to compare inputs and outputs, making the testing and analysis of the new platform much less complicated. The UIs are very similar making it every easier for the Authority to compare old with new

3.2 Operational Services – Requirements

3.2.1 The solution will capture and consolidate data for multiple entities (i.e. The Government Departments bank accounts) and return the information in a format acceptable to HMT and GB. The solution must be banking industry standard, scalable, flexible and easy to maintain.

3.2.2 The application must have any necessary User acceptance Test (UAT) environment to allow the testing of all changes prior to their deployment into the live (Production) environment. The UAT environment must have the ability to populate the environment with live (production) data.

3.2.3 The Authority must have the ability to debit and credit customers' accounts using various file uploads and additionally have the ability to 'zero' customer accounts.

3.2.4 GB currently utilises a SWIFT bureau but is open to alternative methods of connecting to the banks. Only restriction is that currently Bank of England will be SWIFT connection only.

3.2.5 The Authority requires that all feeds / files have an alert mechanism to indicate if a file has been the following.

- Not been received from the supplier banks.
- Been received from the supplier banks and has not been processed.
- Duplicate file has been received.

3.2.6 Timings of the alerts are to be agreed as part of implementation.

- The key output requirements are summarised below:

- All generated reports must be complete (reflect all relevant information made available, for inclusion in the defined report, by the banks via the agreed data transfer channel) and accurate (reflects all agreed data processing rules and adhere to the format defined by the Authority)
- The production of 6 intraday banking activity reports on an agreed schedule and one next day report for HMT using data received from supplier banks.
- Creation of one cash management Files for HMT (to enable them to compare actual movements with those forecast by the Government Departments).

- Creation of journal (internal transfers) files specific to each electronic banking system from Bank of England files (i.e. Bacs Grade 3).
- Creation of journal (internal transfers) files specific to each electronic banking system from HM Treasury files (i.e. Vote Funding, HMT Interest).
- Ability to recreate historical reports of specific files (i.e. cash management files)
- Zeroing customers' and Government Banking accounts.
- Reporting monthly balances of all Government Banking accounts for HMT using an agreed structure.
- Overdraft monitoring (intra and end of day).
- Volumes and values of Government Banking customers.
- Audit reports.
- Reconciliation reports (Euro and Sterling pool's).
- Ability to create ad-hoc reports.
- Management Information reports.
- File / feed monitoring alerts (missing files from data feeds etc.) can be visual or e-mail based.

3.2.7 Hours of Access and Support

- GB must be able to access the system Monday to Friday (except for designated English and Welsh Bank Holidays)
- GB must be able to access the system on a normal Working Day between the hours of 7am – 7pm.
- On business-critical days (i.e. end of financial year, SA peak etc) the Authority may request access to be extended to an agreed time with the ability to run reports.
- The Supplier shall provide a manned service desk to the Authority to the agreed operating hours.
  - normal Working Day operating hours
  - extended support for business-critical days when operating hours will be agreed between the Supplier and the Authority on a case by case basis.
- The application will process all files received within an agreed timeframe (see A4.9).
- Any scheduled maintenance must be outside normal working hours, provide the Authority with a minimum of 10 working days notice and be scheduled with the agreement of the Authority.
- Any Urgent system maintenance to be scheduled with agreement of the Authority.

3.3 Functional Requirements

3.3.1 Payment Functional Requirements

Bacs Grade 3 (reflecting Government Department Bacs Grade 3 payments on to their accounts).

The Supplier must be ready and able to receive a file from the Bank of England (BoE) at 7:30am on a daily basis and use the data within it to create a set of payment messages.

The Supplier must be able to look up the unique Bacs Service User Numbers (SUNs) contained within the file and match them against the relevant customer accounts. Using those SUNs and the related file values associated with them the Supplier shall create electronic instructions that will be sent to the relevant supplier banks by the system users. The message will instruct the bank to pass an internal transfer – debiting the relevant customer's account (to reflect the Bacs G3 payment which is physically being made and settled at the BoE) and crediting a specifically nominated Government Banking owned account. The payment will have a specific value date, i.e. the working day after the date the file is received from the BoE.

Importantly, the debit entry posted to each of the Authority's customer's bank statement must quote the SUN so that the customer can view this on their electronic banking platform (e.g. Bankline) and reconcile the payment.

Every line within the BoE file must create its own payment message. Any unrecognised / unmatched SUNs must still create a payment message, pointing the associated debit value to a nominated Government Banking Bacs G3 Suspense account. The credit would still be directed towards the nominated Government Banking account as stipulated in. A4.1.1.2 of the tender Specification

Any mismatch (exception) as outlined in A.4.1.1.4 of the tender Specification must create an alert for investigation and resolution as the Authority will need to redirect the debit from the Government Banking Bacs G3 Suspense account to the relevant customer's account.

The created internal transfer movements must have a 4 eyes principle authorisation process to allow release to the supplier banks.

The Authority's risk and security team must have an audit function to allow them to view the Government Banking personnel/timings involved in each payment instruction release (bulk or otherwise).

In contingency, should the Supplier be unable to see/process the Bacs Grade 3 file, or the BoE be unable to send it the Supplier shall upload the Bacs Contra report (provided daily to the Authority by the BoE –. This will then allow the process described in A4.1.1.2 of the tender Specification to be followed.

3.3.2 HMT Interest (passing of HMT Interest to Government Department accounts)

The Supplier will be required to upload a file to credit/debit customer accounts, passing the corresponding contra entry to a specifically nominated Government Banking owned account using the same payment message principle outlined in A4.1.1.2 of the tender Specification.

Importantly, the credit / debit entry posted to each of the Authority's customer's bank statement must quote a narrative (e.g. 'HMT Interest') so that the customer can view this on their electronic banking platform and reconcile the receipt / payment.

The application must produce a system alert if a payment message cannot be created, e.g. if an account is closed. The alert will trigger an investigation for the Authority to aid the receipt / payment redirection.

All payments must have a 4 eyes principle authorisation process.

The Authority's Risk and Security team must have an audit function to allow them to view the Government Banking personnel / timings involved in each payment instruction release (bulk or otherwise).**3.3.3 HMT Vote (passing of HMT Voted money to Government Department accounts)**

The Supplier must be able to upload a file to credit customer accounts, passing the corresponding contra entry to a specifically nominated Authority owned account using the same electronic message principle outlined in A4.1.1.2. of the tender Specification.

Importantly, the credit entry posted to each customer's bank statement must quote a narrative (e.g. 'HMT Vote') so that the customer can view this on their electronic banking platform and reconcile the receipt.

The application must be able to create a system alert if an electronic journal message cannot be created, e.g. if an account is closed. The alert will trigger an investigation for the Authority to aid redirection of the internal movement.

The application must be able to create an alert/work item if it detects any potential duplication of payments to an individual account. The alert will trigger an investigation for the Authority and will hold said instructions until investigated.

All payments must have a 4 eyes principle authorisation process.

The Authority's risk and security team should have an audit function to allow them to view the Government Banking personnel / timings involved in each payment instruction release (bulk or otherwise).

3.3.4 Miscellaneous Transfer (Internal transfers)

The Supplier must be able to give the Authority the facility to be able create electronic journal messages (for onward electronic transmission to the associated bank) by either:

a) An uploaded spreadsheet using the following format:

Debit A/c No	Debit A/c Name	Credit A/c No	Credit A/c Name	Payment Date	Amount	Narrative

Or:

b) A manually inputted credit one/debit one process to move money between accounts.

Note:

- The currency of the journal movement must be displayed with an alert should the remitter and beneficiary accounts be in different currencies, i.e. inadvertently resulting in a currency conversion.
- All payments must have a 4 eyes principle authorisation process regardless of input route.
- Journal entries must be restricted to accounts and sort codes registered within the Supplier's system (see Security section).
- The Authority's Risk and Security team should have an audit function to allow them to view the Government Banking personnel / timings involved in each payment instruction release (bulk or otherwise).

3.3.5 Miscellaneous Payments (External)

The solution must be able to create payments that can be made via Faster Payments or Chaps (dependent on FP Limit) using an uploaded spreadsheet with the required details (format to be agreed) or manual entry.

Due to sort code lock these payments will require an additional senior authorisation to allow payments to be made, e.g. a six eyes principal based on the system control rules.

3.3.6 Zeroing (reducing/increasing selected balances to 'nil')

The Supplier must be able to zero, i.e. reducing/increasing balance to nil, specific accounts on a Daily or Monthly schedule, i.e. by creating payment request(s) for onward electronic transmission to any of the supplier banks using the closing cleared balance from the day before or current cleared balance data.

There are 2 scenarios here:

- Clearing high value Authority accounts to nil against an alternative but specified Government Banking account; and
- Clearing customer balances to nil against an agreed customer account. The intent here is for the customer to see the funds 'move' from one account to the other to aid good cash management principals. The set of internal transfer payments would be sent to the supplier banks electronically and require the same authorisation rules as any other payment.

3.3.7 Euro Negative Interest (debiting Government Departments accounts with interest based on their Euro balances)

a) The solution must be able to store the end of day cleared balance data for all Euro accounts.

b) The Supplier must be able to collate the customers' balance data (balances at weekends and bank holidays must be captured) and present an output showing each of them as a monthly total.

c) The Supplier must then be able to calculate the interest payable by the customer. (Based on a variable percentage of the total balances held throughout the month).

d) The Authority user must be able to apply the percentage rate chargeable as this can fluctuate and the application must be able to use multiple rates in working out if rate changed mid-month.

e) The Supplier must present the output as a transfer payment file debiting the relevant Authority customer and passing the corresponding contra entry to a specifically nominated Authority owned account using the same electronic message principle outlined in A4.1.1.2 of the Specification

f) Currently, interest charges are not collected where the resulting value is low. The Supplier must be able to strip out transfers from the payment file that fall below a set limit.

g) The Authority user must be allowed to set the limit that payments are not collected at.

h) All payments must have a 4 eyes principle authorisation process.

3.3.8 Bank of England Requirements

The Bank of England have asked to explore the possibility of sending all payment instructions to them using the SWIFT network. Some of these services are currently provided to us by the Bank of England and some are manual processes.

The solution must have the ability to send MT103 messages via SWIFT to BoE instructing them to make movements on our Drawing account as follows:

1. Funding to the commercial Banks (Sterling and Euro)
2. Internal Movements from Drawing account to HMRC & HMT accounts held at the BoE.
3. External Movements from Drawing account to Citibank (EC1)
4. FX instructions (Beneficiary account information for FX instructions are not held in the application.)

The ability to receive and process intraday and end of day messages from the BoE (MT900 and MT910, MT940)

The ability to take the intraday notification's (MT900, MT910) and create movements / reconciliation checks based on a clearly defined rule set.

The ability to upload Balance data extracted from our banking supplier's Electronic Banking Systems to check and create any funding requirements.

All payments must have a minimum of 4 eyes principle authorisation process.

3.3.9 File Processing

All end of day statement files received before 03:00 will be processed and loaded by 05:00. All end of day statement files received thereafter, will be processed and loaded onto the GRACE platform within 30 minutes of them being made available by the Supplier.

All intraday statement files received before 03:00 will be loaded by 05:00. All intraday statement files received thereafter will be loaded within 20 minutes of them being published by the data Supplier.

All BACS Grade 3 files will be loaded within 15 minutes of them being made available by the Supplier.

All Advanced BACS files will be loaded within 15 minutes of them being made available by the Supplier.

Alerts to be generated for late or missing files and flagged to user and logged for us in MI requirements.

The ability to reprocess replayed files on authorisation ensuring that there are no duplicates records.

3.3.10 HMT Reporting Functional Requirements

Intraday 'Swing' Reports

The solution must be able to create transactional based reports on a required schedule (see below) using defined account structures and rules. The relevant Authority user must be able to request a spot report.

Report Schedule to HMT (Time the report must be with HMT) on each working day is as follows:

- 09:15 Produce by 9:10
- 12:15 Produce by 12:10
- 14:00 Produce by 13:55
- 14:55 Produce by 14:50
- 16:15 Produce by 16:10
- 17:20 Produce by 17:15
- 23:45 Produce by 23:45

- Output is available to the Authority and HM Treasury.
- Output must be able to be e-mailed directly to HM Treasury in contingency.

Minimum information in output is as follows:

- A/c No.,
- Controlling Department,
- Total same day external payments (Chaps, Faster Payments, etc.)
- Total same day external receipts (Chaps, Faster Payments, etc.)
- Total Bacs Payments
- Total Bacs Receipts
- Total Residual Payments (excluding Sterling to Sterling transfers)
- Total Residual Receipts (excluding Sterling to Sterling transfers)
- "Previous Day" – Combined overnight balance outside the Exchequer
- Net flow (overnight plus credit/debits sum of other columns)

3.3.11 Next Day 'Swing' Report

The solution must be able to create a next day report which reports all Bacs items clearing on the following working day. This information is supplied by the banks (see below) by 10.30am. The relevant Authority user must be able to request the generation of a spot SWING report outside of the agreed schedule.

Report Schedule to HM Treasury (Time the report must be with HM Treasury) on each working day is:

- 11:00 Produce by 10:30
- Output is available to Government Banking and HM Treasury.
- Output must be able to be e-mailed directly to HM Treasury in contingency.

Data inputs into the report are as follows:

- Bacs Grade 3 file from Bank of England;
- Next Day Bacs from NatWest;
- Next Day Bacs from Barclays.

Minimum information in output is as follows:

- A/c No.
- Controlling Department;
- Bacs Credits in;
- Bacs Out (non-Bacs Grade 3)
- Bacs Grade 3 (payments out).

3.3.12 Cash Management – Daily File

The Supplier must be able to create a daily output that allows HM Treasury to run their Cash Management scheme that reports for the previous working day and breaks down payments / receipts by payment channels (e.g. transactional data for the file value date 1st June is produced on the 2nd June). All Accounts will be reported separately.

Minimum information in the output is as follows:

- A/c No.;
- Controlling Department;
- Opening cleared balance;
- End of day Cleared Balance;
- Total same day external payments (Chaps, Faster Payments);
- Total same day receipts (Chaps, Faster Payments);
- Total Bacs Grade 3 payments;
- Total Bacs Debits (Non grade 3 Bacs);
- Total Bacs Credits;

- Total Internal Receipts (excluding high value journals – i.e. transfers to Government Departments from Government Banking's High Value Journal Account);
- Total Internal Payments (excluding high value journals – i.e. transfers from Government Departments to Government Banking's High Value Journal Account).

Data Inputs

- End of Day statements.

Outputs

- Create a file using the above headings (see Appendix G for format) available for transmissions to HMT by 10am.

Contingency

- The Supplier must be able to run a report for a specific date outside the normal window of previous working day, i.e. backdated to an earlier day should there prove to be an interrupted flow to data.
- A report will also be scheduled to run at 23:45 as a backup.
- Output must be able to be e-mailed directly to HM Treasury in contingency.

3.3.13 Cash Management – Monthly File

The Supplier must be able to create a monthly report using the Cash Management – daily files building an output that is required at the latest on the 5th working day of each month.

Minimum information in output is as follows:

- A/c No.;
- Controlling Department;
- Open Balance;
- End of day Balance;
- Total same day external payments (Chaps, Faster Payments);
- Total same day receipts (Chaps, Faster Payments);
- Total Bacs Grade 3 payments;
- Total Bacs Debits (Non grade 3 Bacs);
- Total Bacs Credits;
- Total Internal Receipts (excluding high value journals);
- Total Internal Payments (excluding high value journals).
-

Repeated for each working day.

Data Inputs

- Daily Cash Management files for chosen month.

Outputs

- Create a report using the above headings available for transmissions to HMT by no later than the fifth working day.
- Output must be able to be e-mailed directly to HM Treasury in contingency.

3.3.14 End of Month Balance Report and Reconciliation

The Supplier must be able to report the cleared end of day balance for each account and populate on a daily working basis using an agreed account structure. The resulting file output is required by the third working day of the following month in a specific format.

Minimum information in output is as follows:

- A/c No (or lead account where the accounts are grouped within a hierarchy).
- End of day Cleared Balance.
- This is repeated for every working day of the month (weekends and Bank Holidays are excluded).

Outputs

- Create a file using the above headings (see Appendix I for format) must be transmitted to HMT by the third working day.

File Reconciliation

- The Authority is required to reconcile the Government Departments' last working day's balances against the value of the money held within the Exchequer and demonstrate this to HMT. The solution must provide a function that allows the Authority to reconcile these figures. The solution must allow for manual input of an HMT balance by the Authority. The application must also allow for additional balancing entries including funds left outside the Exchequer and produce an output that can be viewed / exported to HM Treasury.

- The End of Month report must report all cleared account balances throughout the month irrespective of whether the account is closed mid-month.

- If an account is closed the Authority must be able to enter a redirection account for any interest / charges that the Authority would have to credit / debit after the closure date.

- The Authority must be able to link (group) customer accounts using a hierarchy structure and have visibility of these links when accessing the account information

- The Authority must be able to view and filter customers' open and closed accounts within the customer information screens.

3.3.14 Late payments.

The Authority require a report that identifies payments (Chaps, Faster Payments) over £100K made after a specific cut off time e.g. 3pm., this report must be available by 8am the following day.

Internal movements are to be excluded from this report except on payments t hat move out of the pool. (I.e. Internal transfers that we only see one side of the transaction)

3.3.14 Future HMT requirements (Future Requirement)

The Authority will need in the future, integration of the RESTful API that allows data to passed through to an external database held by HMT.

3.3.15 Government Banking Functional Requirements

Reference Data

The application must allow the Authority to hold static data for our customers. The Authority groups its customers using a Unique Identifier.

- UID (Unique Identifier)
- Customer Name
- Account No.
- Sort codes
- Currency
- Interest bearing account indicator
- Vote account indicator
- Service User Numbers (SUN) – note: we must be able to link Bacs SUNs to our customer accounts to allow for the look up process involved in the Bacs G3 payment process (A4.1.1.2)
- Controlling Department
- Relationship Manager

The application must be able to show the account structure of any account selected.

3.3.16 Government Banking Reporting Functionality

Interrogation - the system user must be able to access the application and interrogate the data held within it. The user must be allowed to define what information is presented in the output report all of which should be exportable.

Report scheduling - The application must be able to create and run automatable reports. Example (user sets up a large report to run overnight)

Report Creation – The application must allow an authorised user to create reports on the entire data held with the application and output them in various format's (Dashboard, CSV, PDF etc.)

Overdraft Monitoring - Using the End of Day cleared balances the system must be able to create balance reports as follows:

- The Supplier must provide a report that lists 'all' account balances by 8am and a contingency report at 23:45.
- The Supplier must provide a separate report showing an overdrawn account 'group' i.e. created by an account hierarchy by 8am and a contingency report at 23:45.
- The Supplier must produce an alert where a flagged 'Vote' account is overdrawn.

Grose Limit - Must be able to monitor/report on the Grose Limit (GL) for all of the banks. Gross Limit is calculated using all of the accounts that are in a negative position for each currency.

- Each bank has different limits so the Authority must be able to set limits for each bank as required.
- Alerts created using the End of Day balances if the Grose Limit is breached.

Chaps made under Faster Payment limit - When Government Departments make payments by Chaps that are under the Faster Payment limit, they incur additional costs as this is a more expensive payment method.

- The Supplier must be able to report on all Chaps payments made below the Faster Payments limit.
- The Supplier must allow the User to create the date range of the report.
- The Supplier must allow the Authority the ability to set/change the Faster Payment limit as it may change from its current £250,000 limit.
- The Supplier must allow for the output to be filtered by various key fields (i.e. By Controlling Department, UID and Relationship Manager)

Note – the End of Day balance data will contain the information from which this report can be created.

Provision of volumetric data of our transactions.

The solution must be able to interrogate and filter the End of Day statements over a given period using multiple filters.

- I.e. payment channel, Controlling Department etc.
- The output must be exportable from the application.

The solution must capture overnight balances left in commercial bank for use in End of Month Reconciliation.

3.3.17 Reconciliation

Daily Sterling Reconciliation

The Authority is required to confirm that all of the monies held in the supplier banks match the balances held by the Bank of England and HM Treasury at end of business of the previous day. Reconciliation is done the next working day and works on the end of day balances of the previous working day.

The application must reconcile all the balances held in Authority accounts against the balances held at the Bank of England and what HM Treasury believes the balances to be via their "ways and means" calculation. This reconciliation must be done the next working day for the previous day's balance.

The application must capture the following balances and include a specific formula to show that the figures reconcile:

i. Bank of England cash account figure;
ii. Bank of England drawing account figure;
iii. HMT Exchequer ("Ways and Means") figure;
iv. Balances of Authority control accounts in all supplier banks;
v. Balances of all Authority journal accounts in all supplier banks.

(Note: i), ii) and iii) will need to be manually entered by the Authority as we do not have data feeding into the application relating to these figures. iv) and v) will take the figures from the End of Day balance information)

- The application must allow Authority users to add and remove accounts that form part of the reconciliation.
- The application must allow Authority users to see a historical view of the reconciliation.
- The application must allow functionality that allows Authority users to manually key balancing items plus the facility to enter an explanatory narrative
- The application must ensure that any manual adjustments to the balances displayed or manually keyed balancing items require 4 eyes principle authorisation by Authority users.

3.3.18 Daily Euro Reconciliation

The Authority is required to showon a daily basis that all of the balances held in the supplier banks match the figures held by the Bank of England at end of business, the previous day. Reconciliation is done the next working day and works on the end of day balances for the previous working day.

The application must reconcile all the balances held in Authority accounts against the balances held at the Bank of England. This reconciliation is done on the next working day and is for the previous day's balance. The report is to be broken down into working days of the month.

The application must capture the following:

i. Capture Bank of England Euro Holding A/c.
ii. Capture balances of Authority Control accounts in all supplier banks.
iii. Capture balances of all Authority Journal accounts in all supplier banks.

(Note:) i. will need to be manually entered by the Authority as we do not have data feeding into the application relating to these figures. ii) and iii) will take the figures from the End of Day balance information)

- The application must allow Authority users to add and remove accounts that form part of the output.
- The application must allow Authority users to see a historical view of the reconciliation.
- The application must allow functionality that allows Authority users to manually key balancing items plus the facility to enter an explanatory narrative
- The application must ensure that any manual adjustments to the balances displayed or manually keyed balancing items require 4 eyes principle authorisation by Authority users.

3.3.19 Potential Future Requirement for HMRC Data & Reports

HMRC are reviewing the potential to use GRACE as their reporting tool during the term of the contract. They currently have this ability through a separate service and are exploring the possibility of using the GRACE system to meet their current and future needs.

Data volumes are detailed in (Glossary & Volume data)

The solution must be able to create transactional based reports on a required schedule (see below. The relevant HMRC user (as defined by the role controls – See A11) must be able to request a spot report

Report Schedule to HMT (Time the report must be with HMT) on each working day is as follows:

- 09:15
- 12:30
- 14:00
- 15:00
- 16:20
- Output is available to HMRC and HM Treasury.
- Output must be able to be e-mailed directly to HM Treasury in contingency.

Application must create a reconciliation report of sweeps to Bank of England. Report must be received by HMT by 18:00

The application must allow HMRC users import / upload a payment form / file.

The application must allow HMRC to monitor their position and create a report for HMT requesting funding. Report is only produced at 12:30 or 14:00.

3.3.20 Single Sign On

HMRC have initiated several programmes of work, to plan, build, test and deploy services, applications, and data to Hyperscale Cloud environments. Security and compliance are amongst the key concerns HMRC have in relation to moving services, applications, and data to Hyperscale Cloud environments.

As a result of this programme, HMRC would prefer that each HMRC user should have one set of credentials which allows them to authenticate to the internal directory, and all subsequent access to applications should be authorised using that authentication process.

This idea of having a single set of credentials which are used to authorise a user to multiple services and applications. Single Sign-On (SSO), is fully described at Appendix A of the Specification.

The solution must be compatible with a Single Sign On approach.

3.3.21 Additional Security Functions

The application must be able to split user functionality by role to maintain separation

of duties (e.g. payment administrators must not be able to set up accounts) and to ensure that users can only access data and functions they require to do their job.

All role changes, rule changes, account structures changes and payments must have a minimum 4 eyes principle authorisation process.

All role changes, rule changes, account structures changes and payments must be fully auditable.

The application must be able to 'lock-down' sort-codes for the bank accounts held within it (i.e. there is currently a defined range of sort-codes). Changes to the 'lock-down' list should be maintainable by the Authority security role.

Connection to application must only come from defined IP addresses.

Supplier personnel who are administrators must be cleared to Security Clearance (SC level)

3.3.22 Management Information Requirements

The Management Information Requirements needed to allow us to monitor the service are as follows.

MI on file receipt and processing

- Provide real time MI information on the file processing (time file is received from bank to time processed) per feed.
- Provide a summarised MI of the previous months file processing stats by the 10th working day. See KPI
- Provide real time MI information on the file volumes (size / messages) – reflecting the charge bands.
- Provide a summarised report of the previous months file volumes (size / message) stats by 10th working day.
- The ability to self-configure reports to interrogate file processing data.

Reports

- Provide real time MI on the timing of the swing reports creation cross referenced with last file times per feed.
- Provided a monthly report of the swing timing of report creation and the files times by the 10th working day
- Provide real time MI on the timings of all other reports that use end of day statement data cross referenced with file timings.
- Provided a monthly report on the timings of all other reports that use end of day statements by the 10th working day.
- The ability to self-configure reports to interrogate file processing data.

3.3.23 Operational Date, Implementation & Data Migration

The Supplier must provide a replacement application of Financial Reporting Transaction tool (FTR) with an Operational Date on or before 28/02/2022. For the avoidance of doubt this means that;

a) the new application must be fully tested, implemented and operational;

b) the system must be ready to provide the captured and consolidated data for multiple entities and return the information in an acceptable format as described in the specification to GBS and HMT on or before the Operational Date

Any delay in achieving the Operational Date on the part of the Contractor will result in a reduction to the overall contract price equivalent to any week (including any part week) period for which the system is inaccessible

To ensure that the Operational Date is met the Contractor must provide an implementation plan which will confirm how the Operational Date will be achieved

The Contractor will not be required to facilitate the migration of any data from the existing system as part of the implementation process.

3.3.24 Hours of Access and Support

- The Authority must be able to access the system Monday to Friday (except for designated English and Welsh Bank Holidays)
- The Authority must be able to access the system on a normal Working Day between the hours of 7am – 7pm.
- On business-critical days (i.e. end of financial year, SA peak etc) the Authority may request access to be extended to an agreed time with the ability to run reports.
- The supplier shall provide a manned service desk to the Authority to the agreed operating hours.
    - normal Working Day operating hours
    - extended support for business-critical days when operating hours will be agreed between the Supplier and the Authority on a case by case basis.

    - The application will process all files received within an agreed timeframe

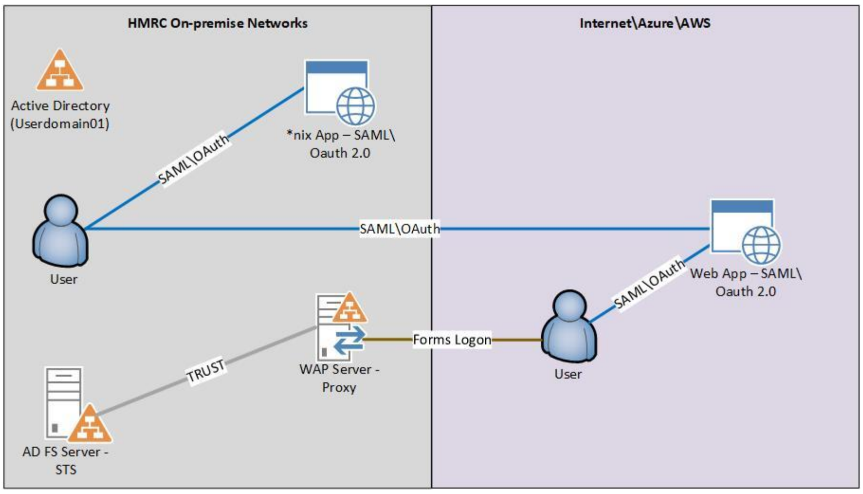
    - Any scheduled maintenance should be outside of normal working hours and provide the Authority with a minimum of 10 working days notice.

    - Any Urgent system maintenance to be scheduled with agreement of the customer.

3.3.25 Security Requirements –

Security Token Services

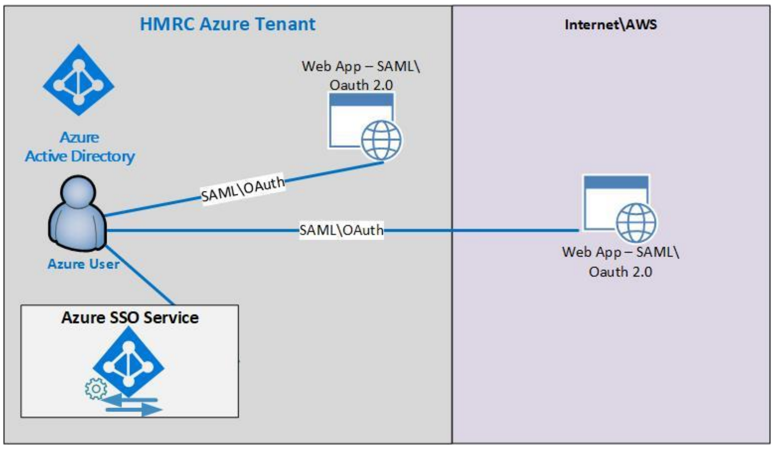
Another name for an SSO service, is a Security Token Service (STS). HMRC have an internal on-premise STS based on Active Directory Federation Services (AD FS). This service is integrated with the internal Userdomain01 AD domain and allows HMRC users to be authorised to web applications and services both on the internal network and on the internet.



In the diagram above, the internal network hosts both the AD FS systems and proxy systems called Web Application Proxy (WAP) servers which allow the SSO service to be reached from the Internet. In reality, the WAP servers are hosted in a perimeter network with firewalls isolating them from the internal network.

An internal user will connect directly to the AD FS servers on the internal network to retrieve a security token in order to access services both internally and on the Internet if required. A HMRC user on the internet will be passed a suitable token via the WAP servers once they have successfully authenticated against the AD. The resulting tokens can be in a format specific to the application the user wishes to access, being either SAML 2.0 or OAuth 2.0.

The security token formats are discussed in detail in the following section of this document.



HMRC have also created their own Microsoft Azure cloud tenant, which is used primarily to allow users of Office 365 to have a cloud presence. In order to allow this, HMRC operate a service called Azure AD Connect on an internal server, that synchronises users and groups from the internal AD to Azure AD. This Azure AD includes an Identity Federation service called Azure SSO. See section 2.7.3 to understand how Azure AD Connect is utilised.

HMRC users authenticate to the Azure AD when they access either their OneDrive or any of the Office 365 applications. When the HMRC user goes to a web application which is integrated with Azure SSO, the service will generate a security token and pass it to the user to allow them to authorise to the application. The web application does not have to be hosted in Microsoft Azure and can be hosted at any third-party service provider or cloud provider. It simply needs to be accessible from the Internet.

Strategy Note: *HMRC CTO current guidance is that Azure SSO is used for all new integrations. Azure SSO can produce tokens that can be used by both new and legacy web applications, so in most instances this should be possible. The HMRC AD FS service is currently having relying applications and services moved off it in preparation for decommissioning. Therefore, it can no longer be considered an option for SSO integration.*

Security Tokens

Security tokens are also known as Authorisation Tokens and are the means by which a user is authorised to an application or service. In order to authorise the user must be redirected to a Security Token Service (STS) which is able to authenticate the requesting user against a directory service such as Active Directory (AD).

Both AD FS and Azure SSO act as an STS that they can generate tokens containing information about a user, which can be used by the consuming application or service to authorise the user for access.

The tokens will also have a digital signature attached to them which allows the consuming application or service to validate the origin of the token and the integrity of the token. This is an important check will must be performed to allow the consuming application to “trust” the information contained in the token.

There are two primary token types in use today, SAML 2.0 and OAuth 2.0. Both AD FS and Azure SSO can produce both types of token, but only Azure SSO supports OpenID Connect (OIDC)\OAuth 2.0 integrations. This is the most up-to-date Modern Authentication protocol and is the preferred choice for new integrations.

Also, the OAuth 2.0 functionality in the version of AD FS that HMRC are using on-premise (ADFS 3.0) does not support the full range of functions that are available from Azure SSO.

For clarity throughout the rest of the document the term authorisation token will be used when discussing a feature or technology which could apply to either SAML 2.0 or OAuth 2.0 tokens. Protocol specific discussions will call out either SAML 2.0 or OAuth 2.0 when appropriate.

Claims and Assertions

The technical names for the items of information about a user that are included in authorisation tokens are claims or assertions. They are referred to as claims as they are claims made by one party (the Identity Provider) about another party (the user), which are trusted by the application or service, as proof of the users right to access the service. Any system which uses information contained in authorisation tokens to authorise users is also called an Assertion Consuming Service (ACS), so you may hear that term used when discussing the contents of authorisation tokens.

Claims or attributes included in authorisation tokens can include:

- Given Name
- surname
- Display Name
- Email Address
- Role information

Some applications only require a single Name Identifier value in the authorisation token, whilst others will require additional values, perhaps to indicate a department or business unit. Each application will have different requirements in terms of the claims that allow a successful integration. Any integration will involve discussions with the vendor about the claims required by their application. The OAuth 2.0 RFC defines a fixed set of claims in the access token, so there may be times when SAML 2.0 is a better choice as it allows more flexibility in terms of claims that can be included in the SAML token.

Integration Note: Role claim values sent in OAuth 2.0 tokens or SAML 2.0 tokens produced by Azure SSO cannot contain spaces in them. This is a restriction of Azure SSO

Name Identifier Values

One value contained in the security token will be particularly important to the consuming application or service. This is the Name Identifier (NameID) and it represents the users’ identity in the application. It is effectively the users' logon name when they access the application and it is important because it **must not change**.

For several possible reasons, users' may need to change their names. When they do, values such as their surname, email address and display name will have to change as well. This makes these user attributes a poor choice for the NameID, as the application cannot deduce that this is still the same user. A value used as a NameID should be a static value which will not change throughout the lifetime of the users account in the directory. A&I guidance is that the users' PID should be used as their NameID as it will not change throughout the life of the user account. If a project should elect to use another value which may be subject to change, then the application will need to be coded to deal with this situation and prevent SSO issues and account duplications.

Sometimes an application will define an immutable value or source anchor, which is a Unique ID (UID) which is contained in the source directory and is also contained and stored in the application identity store. Each time a user presents an authorisation token, it will contain this value, and this is used to link the user with their identity store account. As it is a non-name value, if the users name changes for any reason, the link between the user' account in their home directory and the user account in the application will remain intact.

Integration Note: The users PID should be used as the immutable value in authorisation tokens. This value is derived from an attribute called "user.onpremisessamaccountname" and is **NOT** included by default in either SAML 2.0 tokens or OAuth 2.0 tokens.

SAML Tokens

Security Assertion Mark-Up Language (SAML) is both a token format and a standard for SSO. SAML tokens can contain information about the user requesting access such as their name, email address or organisation. It is possible to include any value which is stored in the HMRC AD as a claim\assertion in a SAML token. The Azure SSO is capable of producing SAML tokens, but the information in Azure AD is a subset of that in the internal AD.

Bearer Tokens

The Open Authorisation version 2.0 protocol produces tokens which are formatted using Java Script Object Notation (JSON) rather than SAML. These tokens are referred to in this document as "bearer tokens", to distinguish them from SAML tokens. The Azure SSO service can only produce tokens which contain claims stored in Azure AD.

Web applications and services which use authorisation tokens to authorise users to them are called "consuming services" in the rest of this document.

Strategy Note: *HMRC CTO current guidance is that OAuth 2.0 bearer tokens be used when users are authorising to web application and services. This is of course, dependent on the web application supporting the use of OpenID Connect\OAuth 2.0 protocols. Where a project identifies that use of OpenID Connect\OAuth 2.0 is* *not supported then SAML 2.0 tokens generated by Azure SSO are a valid alternative.*

Sources of Attributes\Claims

HMRC operate a number of directory services across the estate which are integrated with the Forefront Identity Management (FIM) tool. This is used to allow each directory to “master” certain attributes and synchronise those attributes to the other directories if there is a business need.

Azure AD contains information about HMRC users and groups which is synchronised from the internal AD using the AD Connect service. Azure AD only contains a subset of the information about users and groups as some of the attributes related to them are not relevant in Azure AD. Azure AD does NOT contain information stored in any directory service other than the HMRC Active Directory.

Therefore, it should be realised that Azure SSO can only produce SAML 2.0 or OAuth 2.0 tokens that contain information that is stored in the Azure AD.

Protocol Options

Protocol support is one of the primary differentiators between the HMRC internal network and Azure AD.

Two different protocol types are discussed in the following sections:

- Directory Access protocols
- Authentication\Authorisation protocols

LDAP\LDAPS

The standard means of querying\updating information stored in directory services on the internal network is the Lightweight Directory Access Protocol (LDAP) and its secure variant LDAPS.

This protocol is often used in tandem with a service account to allow applications to populate their local databases with information from stores such as Active Directory (AD). Azure AD does not support the use of LDAP to perform queries against it. An Application Programming Interface (API) called the Graph API is now the standard method to retrieving information from Azure AD.

REST\HTTP

Representative State Transfer (REST) is an architectural style for building distributed systems based on hypermedia. REST is independent of any underlying protocol and is not necessarily tied to HTTP. However, most common REST implementations use HTTP as the application protocol.

REST\HTTP is the standard way of querying the Azure APIs and can be used in the same way that an LDAP query would have been used read\write to the Azure Graph API. Modern cloud applications should have the ability to query the Graph API to populate their local identity stores or to update information about user roles. This will be discussed further later in the document.

Kerberos

Kerberos will only work on the internal networks and only where both the Authority and the service\server is able to communicate with one of the Userdomain01 domain controller systems. This means that Kerberos is not suitable for integrating cloud-hosted applications and services.

There is a detailed discussion of Kerberos in section 3.3.1.1.

WS-Federation

WS-Federation is a legacy SSO protocol which has been around for many years. It should only be used to integrate applications when none of the other protocols are supported.

Security Assertion Mark-up Language (SAML)

SAML is an industry standard application which is supported by many web applications and services. However, certain limitations in its implementation mean that it is no longer considered as the strategic protocol for HMRC. With the advent of newer browser attacks, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF), SAML has become vulnerable to token theft or redirection. On the vast majority of SAML integrations, the SAML token is returned to the browser and the redirect to the consuming application happens within the same browser session. This means that browsers are now considered to be “unsafe environments” for passing security tokens and another method should be used. OpenID Connect\OAuth 2.0 removes some of these vulnerabilities. Therefore, SAML should only be used where OpenID Connect\OAuth 2.0 is not supported by the consuming application.

OpenID Connect\Open Authorisation v2.0 (OAuth 2.0)

Open ID Connect\OAuth 2.0 is now the industry standard for SSO integrations and is the strategic choice for all new external application integrations on the HMRC estate. Where it is supported by the application it should be used to support SSO integration.

3.3.26 Protocol Support

Azure SSO Service

The following authentication and authorisation protocols are supported by Azure SSO

- Security Assertion Mark-up Language (SAML)
- Open Authorisation v2.0 (OAuth 2.0)
- OpenID Connect

Strategy Note: The CTO guidance on protocols is that new consuming applications should use either SAML 2.0 or OpenID Connect. The strategic protocol is OpenID Connect, with SAML authorised for use only where the external application or service does not support the newer protocol.

User Provisioning\Deprovisioning

Many web applications will maintain a local identity store which contains information about users who access it. This identity store is used to maintain details such as the users name, their email address and personalisation information such as the users' homepage and any preferences that they have selected whilst using the application. The identity store may also contain details of the permissions that the user has once authorised to access the application by the SSO process.

HMRC have a policy that wherever possible, user provisioning and deprovisioning should be automated and be capable of integrating with the Service Request System (SRS). Therefore, ideally, any application being integrated will be capable of using SCIM as this will be the strategic solution going forward. Section 2.7.4 gives an overview of SCIM.

How this identity store is managed is dependent on the web application being integrated. The following section will discuss typical scenarios

Manual Identity Store Management

Older web applications can require a support resource to manually manage the application identity store. This support resource can be an individual or a team, dependent on the scale of the application and the number of users. A web management portal is made available so that a support team can create, delete and update user accounts as required. Often an API will be exposed, such as the Microsoft Graph API, which allow scripting to be used to perform account management, including bulk creation and deletions.

Use of a manual process can lead to additional operational costs. Manual management processes also do not work very well with other automated service allocation processes, often causing issues with user access due to delays in following the manual process. Manual management should only be used where there are no automation options available.

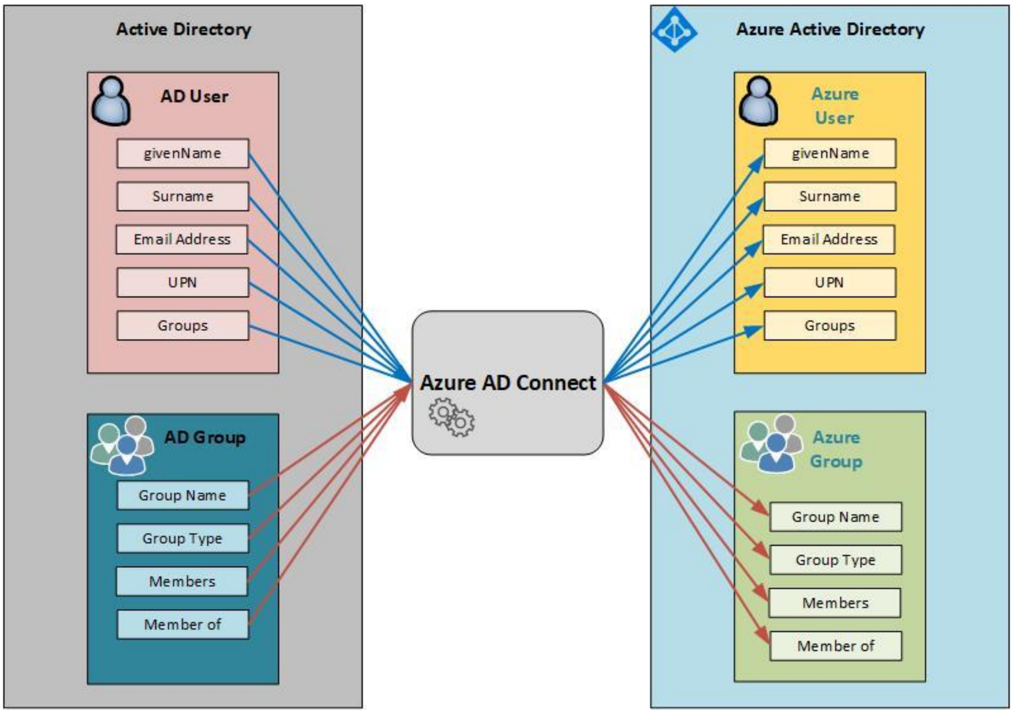
Dynamic (Just-in-Time) Account Creation

Some web applications are written in such a way that information in the security tokens presented by users can be utilised to create and update a user account. The application will create the user account when the user first connects and presents a valid security token and will populate the various items of information about the user using the assertions in the token. On subsequent accesses the security token content is compared with the users account in the web application and will be updated if any of the assertions has changed. Account deletion then becomes a process of monitoring accounts which have not been accessed for a specific amount of time, and then deleting them if they are no longer required. This process can also be scripted if requires by the enterprise.

Synchronisation Tools

Some web application vendors have created tooling which allow user and group information from an enterprise directory service such as Microsoft Active Directory (AD) to be synchronised with their application identity stores. Google offer a tool called Google Cloud Directory Sync (GCDS) which runs on an internal server and periodically synchronises internal directory information with the Google Cloud (G-Cloud). The Microsoft offering is a server-based tool called Azure AD Connect (AADC) which performs the same role. Tools such as this tend to only be made available by the bigger Cloud Service Providers (CSPs), as they are expensive to develop and maintain, and require support services to maintain the product throughout its' lifecycle.

HMRC use the Azure AD Connect tool to keep their Azure AD domain in synchronisation with the on-premise Userdomain01 AD domain. AD user accounts and groups are synchronised every 30 minutes.



Azure AD Connect

It should be noted that not all user attributes from the HMRC internal directory are synchronised to Azure AD. Therefore, if your application requires a specific attribute from the internal AD to be included in the Azure AD which is not already synchronised, you should engage with A&I or CDG about the process to have the attribute included.

Directory Query Tools

Some applications would historically use an LDAP query authenticated via a service account to get information about their user bases from the internal AD. This will not work against the Azure AD as it does not support LDAP. It should be possible to modify the application to use RESTful HTTP calls sent to the Azure Graph API and using a cloud service account for authentication and authorisation. The Microsoft Azure websites contain a number of developer references that give examples of how this can be achieved.

SCIM 2.0

The System for Cross-domain Identity Management (SCIM) is an open source standard which allows web application and service identity stores to be maintained automatically. Application Programming Interfaces (APIs) are published by the application, that can be used to automate the creation, update and deletion of user identity information. More and more modern web applications and services support SCIM version 2 (SCIM 2.0) and wherever technical possible this should be used to remove the requirement to manage the application identity stores manually.

The following link give an overview of SCIM and how Azure can use it to provision user identities into applications:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/use-scim-to-provision-users-and-groups

3.3.27 Application Role Allocation

It is a longstanding requirement from HMRC that any application or web service which will integrate with SSO should have the ability to externalise its' user roles so that they can be controlled using the Service Request System (SRS).

What this means is that it should be possible for the application to identify or modify the users' role within the application by reading the value of an assertion included in the authorisation token from the STS.

Service Request System – An Overview

The HMRC Service Request System (SRS) is an enterprise integration tool which allows users to be allocated access to applications and services. There is a business workflow layer in SRS which means that, for some applications, there is an approval process and a manager or supervisor must approve the request before a role is assigned.

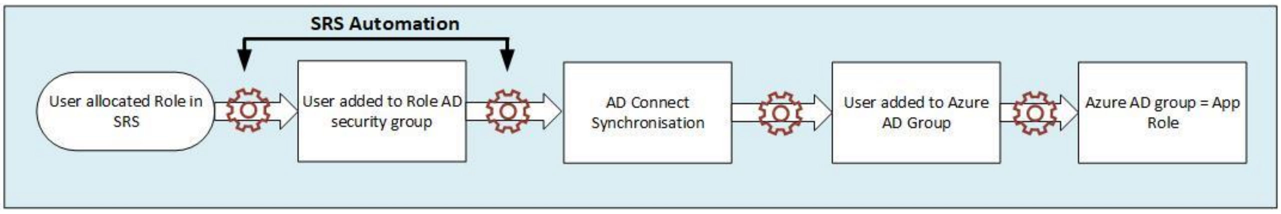
Once a role is assigned, this can trigger a number of processes in the background. These processes can include:

- Allocating the user to an AD security group to assign permissions to the application or service
- Assigning a license to the user if the application or service requires one
- Informing support teams that manual processes need to be initiated to complete a user allocation if required.
- Triggering the delivery of application software to the user desktop if required
- Adding a shortcut onto the users' desktop or into their My Services console to allow access to the application

Dependent on the role being assigned, some or all of the above actions may or may not be required.

Role Allocation Flow – An Example

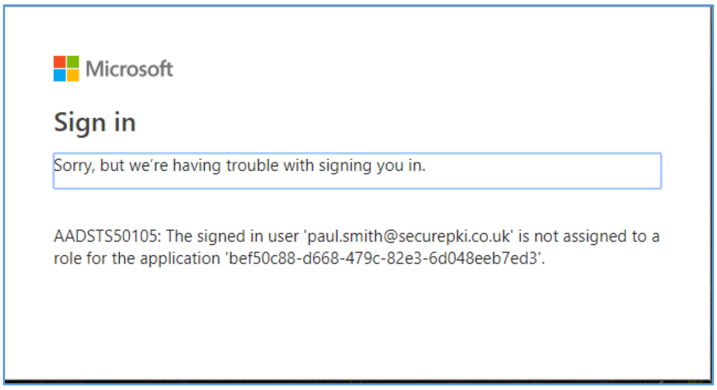
Using the example of how role information will be communicated to an application where Azure SSO is used as the STS, the following diagram shows the process flow:


SRS Automation
User allocated Role in SRS
User added to Role AD security group
AD Connect Synchronisation
User added to Azure AD Group
Azure AD group = App Role

In the above diagram, the user is allocated a role in SRS via the standard business processes and approvals. The role allocation will typically include an AD security group membership, which the users' account in AD will be added to. The Azure AD Connect synchronisation tool will now add the users' Azure account to the Azure group that is mapped to the internal AD group. This Azure AD group can be mapped to a role in the application and a value can be sent in the SAML\OAuth 2.0 token which represents that role. The application code can then infer the correct user role and assign it to the user. The code should be written in such a way that the role value is read each time a token is presented by the user. This allows a user to have their role changed and for the application to pick this up the next time the user authorises to the application. If it is possible for a user to have more than one role, then the developers will need to code their application so that it can handle this situation and arrive at the correct permissions level for the user based on a combination of their roles.

User and Group Assignment

There is an assumption that all HMRC users will have a synchronised account in Azure AD and therefore be able to authorise to it. At the time of writing, all HMRC end user accounts are synchronised to Azure AD by the AD Connect tool. Access to individual applications in Azure is mediated by Azure groups and application roles. If a user is not in a group which is permitted access to the application, they will see an error if they try and access it.



Sign in

Sorry, but we're having trouble with signing you in.

AADSTS50105: The signed in user 'paul.smith@securepki.co.uk' is not assigned to a role for the application 'bef50c88-d668-479c-82e3-6d048eeb7ed3'.

The image above shows the error displayed when a user is not allowed to access an application in Azure.

Azure uses a mechanism called User and Groups assignment to control user access to applications.

Adding an Azure group to the User and Groups assignment section can be used for two possible functions:

1. Mapping a role configuration to an Azure group
2. Acting as an access control to the application itself

If the application being integrated requires a "role claim" (see section 2.8.2) to be included in the authorisation token, then the User and Groups assignment section can be configured to map a group to a role.

If the application to be integrated does not require a "role claim" in the authorisation tokens, then the User and Groups assignment section acts as a simple access control mechanism. If the requesting user is not in one of the groups assigned to the application registration, then will receive the error shown above.

Note that in the unlikely instance that the application users are not allocated to the application via an SRS Role (this is fast becoming mandatory), then a dynamic group called **EMS-DYN-All-HMRC-SYNCED-STAFF** will be assigned to the application registration. This will restrict user access to the application to only HMRC staff who are synchronised from the internal AD domain.

Security Note: Disabling User and Group Assignment, while possible is not considered security best practice. Therefore, it would only be allowed once a thorough security review has been undertaken to understand the risks that this would introduce.

Conditional Access

Azure also implement a technology called Conditional Access, which allows additional restrictions to be imposed on users of an application.

These can include:

- Enforce the use of MFA for all users or just for certain user types (admins).
- Permit or deny access based on user location
- Permit or deny access based on the device being used
- Permit or deny access based on the Authority application being used (eg. Allow PC and iPhone, but deny Android)

Conditional Access is applied using policies, and these policies can be applied either globally for all users of Azure AD, or directly to an application so that only its' users are affected.

Projects should speak to CTO about what policies are being applied globally and assess whether their application requires its own policies to restrict how users access it.

When implementing a project which has applications in it which are used to perform admin functions, then Conditional Access should be applied to these applications so that all users are forced to authenticated with MFA.

Projects should contact the CDIO Architecture and Innovation team for information on what criteria would require the use of Conditional Access.

3.3.28 Application URLs – DNS Considerations

In the Pattern specific sections later in this document, there is a discussion of the various URLs that Authoritys will need to resolve. The actual application URL will be different for each implementation, but the following is a brief discussion of how these URLs should be configured.

HMRC long term strategy is that many of its internal applications will be exposed to the internet so that they can be accessed from HMRC-owned Authority devices, such as the iPhones supplied to many mobile workers. While some applications would never be exposed to the internet, HMRC want the ability to do so should business requirements dictate that it is required.

Due to this, the decision has been made to deprecate the use of internal-only namespaces such as "apps.hmrci", in favour of a namespace which can be resolved on both the internal network and the public internet.

This requirement means that all future applications deployed into Cloud-hosted environments should use the ".corp.hmrc.gov.uk" DNS namespace. This will allow the applications to be resolved both internally within the HMRC network and externally on the public Internet if required.

Due to the new possibility that DNS names will be made available on the public internet, it is important to consider the naming standards for new services and applications.

Historically, HMRC application and service URLs have included things like product names, environment names and sometimes software component names. From a service management point-of-view, this approach makes sense. You can look in the address bar and immediately see which environment you are working with and understand the products in use. However, if these names are exposed in public DNS, they immediately give clues to potential attackers of where to look to find vulnerabilities and security holes to exploit.

Even including the environment name (dev, pre-prod, test, production) discloses information as attackers know that test and pre-prod environments tend to use weaker security controls and password standards than production. By exploiting these less secure environments, an attacker can learn more about the production environment and potentially identify a means to attack it and gain access to the information it processes.

Therefore, the following guidelines should be adhered to when creating DNS names for applications and services:

- Avoid the use of product names in URLs
- Avoid the use of environment names in URLs
- Avoid the use of component names in URLs

Security Note: DNS names that contain information about the internal infrastructure of a solution will be highlighted by any PEN testing undertaken on the service. Mitigation after the fact would include having to rework your URLs and the certificates used to protect them. Choose your DNS names carefully to avoid delay and expense later in your project.

3.3.29 Federation Metadata – An Automation Opportunity

Configuring an application to communicate with a Federation Service can involve the configuration of several parameters, in both the web application management console and the federation service management console. Arriving at the correct values for these parameters and exchanging this information manually, via email messages and attachments for instance, can lead to mistakes being made. Any such mistakes will often lead to issues during the implementation, and increased implementation costs to identify where the errors lie.

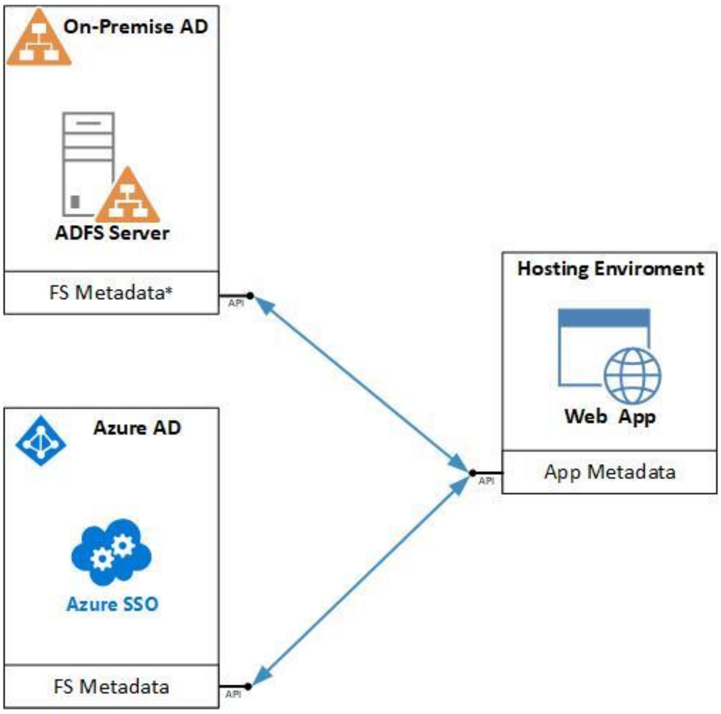
There is also the issue of change management. Federation Services sign the authorisation tokens they produce using a digital certificate called the Token Signing Certificate (TSC). This certificate is only valid for a set time and then it must be replaced. Replacing the certificate involves updating it in the federation service and then communicating to all applications receiving the tokens that they need to use the new certificate to check the signature on the tokens. If the application does not have the correct TSC, then it will be unable to validate the tokens that it receives and the SSO process will fail. Federation Services and applications will sometimes need to change some of the URLs which are used to reach them. How can these changes be identified and addressed in an automated fashion? The answer is federation metadata.

Many federation services and applications publish an XML file containing details of the information needed to communicate with them, along with copies of the public half of the digital certificates associated with them. This XML file is exposed via a HTTPS URL which will allow interested parties to access the information they require to integrate with the application or federation service.

A federation metadata file created and published by an application, will be different to one published by a federation service, because they have different requirements.

An application Federation Metadata file will contain items such as the attributes that the application needs to identify the user, as well as a digital certificate if the application wants to receive encrypted tokens. It will also contain the identifier that will used to allow the federation service to establish which application the user needs a token for.

A federation service metadata file will contain information such as the address that Authoritys need to be redirected to, the URL that the resulting token should be transferred back to, as well as the public half of the TSC which will be used to sign the tokens from the service.



**FS = Federation Service*

The content of the federation metadata file changes whenever a change is made to the application or federation service which publishes it. Therefore, if the file is retrieved periodically by the other end of the federation, it can be used to keep the two configured correctly and able to communicate. The information contained in the federation metadata files does not represent a security issue. The application and the federation service still need to be configured by administrators to retrieve the files and configure themselves using it.

There is an argument that using Federation metadata files will result in unapproved changes to the application or federation service. While it is true that this will be the case, if either the application or federation service performs an update without communicating it correctly beforehand, a service outage will result. The two parties involved in the Federated Trust need to agree which scenario represents the greatest risk to live service.

Both the HMRC AD FS service and the Azure SSO service expose federation metadata via the following URLS:

Federation Service	**Metadata URL**
Azure SSO Service	https://login.microsoftonline.com/<Tenant_ID>/federationmetadata/2007-06/federationmetadata.xml
On-Premise AD FS service	https://fs.hmrc.gov.uk/federationmetadata/2007-06/federationmetadata.xml

3.3.30 OpenID Connect\OAuth 2.0 Token Flows

OpenID Connect and OAuth 2.0 is the preferred SSO protocol for use with applications integrating with the HMRC Azure SSO service. The protocol is extensible and has been written to support a number of scenarios dependent on the Authority and communications available between the Authority application and the web application being integrated.

3.3.31 OAuth 2.0 Specific Terminology

The OAuth 2.0 protocol has its' own set of terminology, some of which will be used in this document:

3.3.32 Resource Owner

The Resource Owner is the user whose information is being requested. The user must perform authentication in order to authorise the application to request their data.

3.3.33 Authority Application

The Authority, in the context of OpenID Connection (OIDC) is the application that needs to access information about the resource owner.

3.3.34 Authorization Server

The authorisation server is the system which can grant access to the users' data. In this scenario, the authorisation server is the Azure AD and its' authorisation API.

3.3.35 Resource Server

This is the system or directory which contains the data about the user which the Authority needs to access. In this scenario, this would be the Microsoft "Graph" API.

3.3.36 Authorisation Grant

This is the code which allows the Authority to access the information on the resource server. This authorisation grant is issued by the authorisation server once authentication has been completed.

3.3.37 Scope

This is the information in the authorisation grant code which limits the information that the Authority can access about the resource owner.

3.3.38 Redirect URI

The Redirect Universal Resource Identifier (URI) is the address in the communication flow that the Authority is redirected to when the authorisation grant has been issued. This can also be known as the "call back" address.

3.3.39 Front Channel Communications

The front channel is the term to describe communications which happen via the browser and redirects. This channel is considered to be less secure as it exposes some secure data to the browser. If the browser has been compromised in any way, then this secure data could be exposed to an attacker.

3.3.40 Back Channel Communications

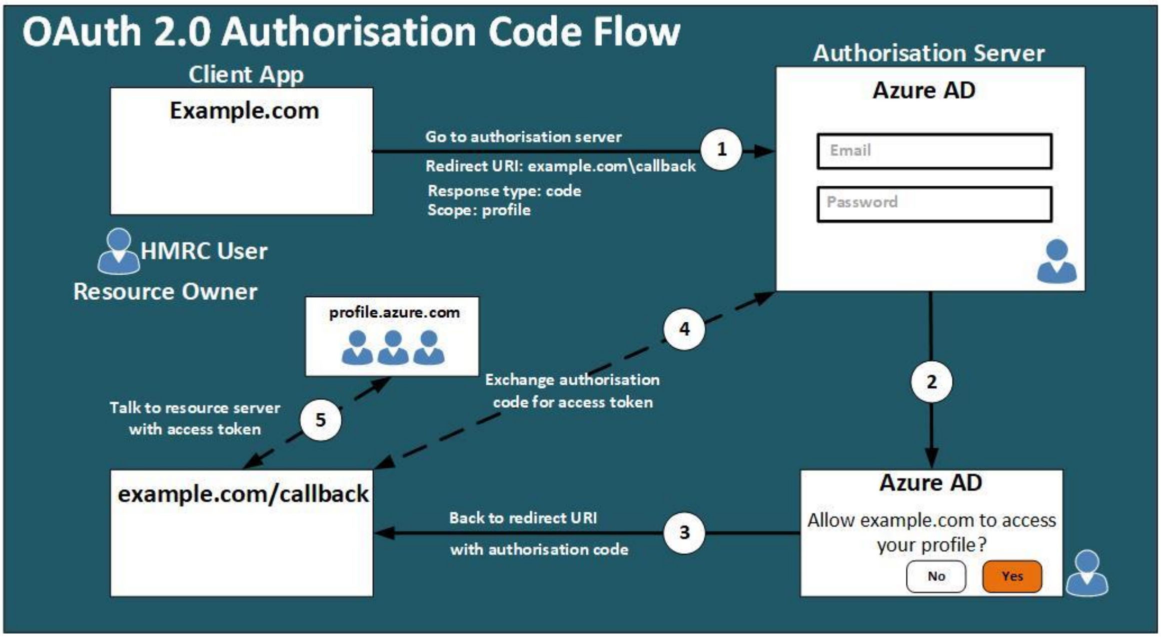
Back channel communication is communication which happens directly between the Authority application and the authorisation service, which in this case would be Azure AD.

3.3.41 Access\Bearer Token

The access or bearer token is returned to the Authority application once the authorisation code has been submitted. The information in the access token is dependent on the scope that was requested and authorised by the user.

OAuth 2.0 Authorisation Code Flow

Whilst OAuth 2.0 supports a couple of token flows, only the Authorisation Code flow is supported by HMRC. The steps of the Authorisation Code flow are shown in the diagram below:



The communication steps for this flow are discussed below:

1. In this scenario, the HMRC user is the resource owner, as they “own” the data which is to be accessed. The user connects to the Authority application with their browser and is redirected to the authorisation API. The API must authenticate the user and redirects them to the authentication service, in this case, Azure AD. The user supplies their logon credentials.
2. The user is presented with a dialog warning that they are about to give access to their data to the requesting application. The user must respond to this message to allow an authorisation code to be issued. This warning message is disabled in the HMRC Azure tenant as users are not allowed to authorise access to data in the Azure domain.
3. The user is issued with an authorisation code and it redirected back to the Authority application.

The above communications all happen in the users’ browser and are designated as “front-channel” communications.

4. The Authority application now connects directly to the token API Azure SSO and presents the authorisation token issued to the resource owner.
5. Once validated, the Authority application is issued with an access\bearer token which it uses to authorise the user.

The process is now complete, and the user can access and use the Authority application. The token flow is preferred as the access token containing the user information is never exposed in the users’ browser. This “back-channel” communication is considered more secure as it reduces the possibility of the token being stolen or compromised. Due to the increased use of cross-site scripting and other browser attacks, exposing the token in the browser is now considered to be less secure than letting the Authority application retrieve it directly.

3.3.42 OAuth 2.0 Authority Secrets

Now that we have reviewed the OAuth 2.0 Authorisation Code flow, we can discuss how the call to the token endpoint is protected. In step 4 of the flow above, the Authority application makes a call to the token endpoint API and presents the authorisation code. In order to allow the token API to authenticate the Authority application, a pre-shared key should have been established between them. This means that the token endpoint can validate the request before it issues an access token. This prevents a malicious actor from intercepting the authorisation code and requesting an access token from the API.

This pre-shared value is generated in Azure AD once the application has been registered.

In keeping with good security practice, the key material should be set to expire after an amount of time. The options in the configuration console are:

- One year
- Two years
- Never expires

Clearly, when this key expires it will need to be renewed and a renewal process will need to be followed. This will involve generating a new key and then communicating that to the application support team to allow it to be configured to use it. This process will need to be documented by a project and included in part of their handover to LIVE service.

The recommended lifetime for this key is two years, which will reduce the renewal frequency. Any project wishing to implement a key which does not expire, should get agreement from HMRC Security that this is permitted, and it should be registered as a risk in any project documentation.

Security Note: Rotating the Authority secret is vital to maintaining the overall security of the application registration. The requirement to renew the Authority secret introduces a degree of Live service risk, as failure to renew it will result in a service outage. It is VITAL that projects document the renewal process for their application and highlight the need to renew the Authority secret to the application support team as part of the handover into Live.

Application Server Communication – IMPORTANT

The back-channel communication requirement for the above OAuth 2.0 flow requires that the application servers be able to connect directly to the Azure Token Endpoint API on the Internet. For this to complete successfully, the following configuration items need to be in place:

1. The server must be configured with a valid proxy configuration to reach the Intemet
2. The server must be able to authenticate to the proxy or be in a by-pass list to avoid having to authenticate
3. The server should have the root Certification Authority (CA) certificate for the proxy server in order to be able to set up a communications session. This certificate must be in a location where it is “trusted” by the application.

Below is an explanation of some of the above with details of how this would work for the HMRC Production environment.

The proxy service is supplied by two arrays of McAfee Web Gateway devices, one in SDC01 and one in SDC02. These arrays are addressed internally by two IP addresses:

- 10.41.63.134
- 10.41.199.134

The server can load balance across the proxy arrays by resolving "gsi-proxy.gss.hmrci" via DNS. This will return the two IP addresses above in a round-robin fashion to the server. The proxy connection port is 9090/TCP.

Authentication to the proxy service is typically done using a Userdomain01 service account which has been placed into an AD security group which has access to the Internet. There is also an option to request that your server IP addresses bypass authentication. This will need to be reviewed and agreed by security as it does remove some of the security controls that can be applied to the server traffic.

The HMRC proxy service is configured to perform SSL inspection of the traffic which flows through it for the "login.microsoftonline.com" domain name. This cannot currently be bypassed as other projects require that inspection be enabled. Therefore, the proxy is performing an intentional "man-in-the-middle" operation to inspect the traffic. The connection to the server will be established using a certificate which has been generated and signed by the proxy server using the onboard root certification authority. Therefore, your servers will need to trust this certificate in order to create a HTTPS connection outbound.

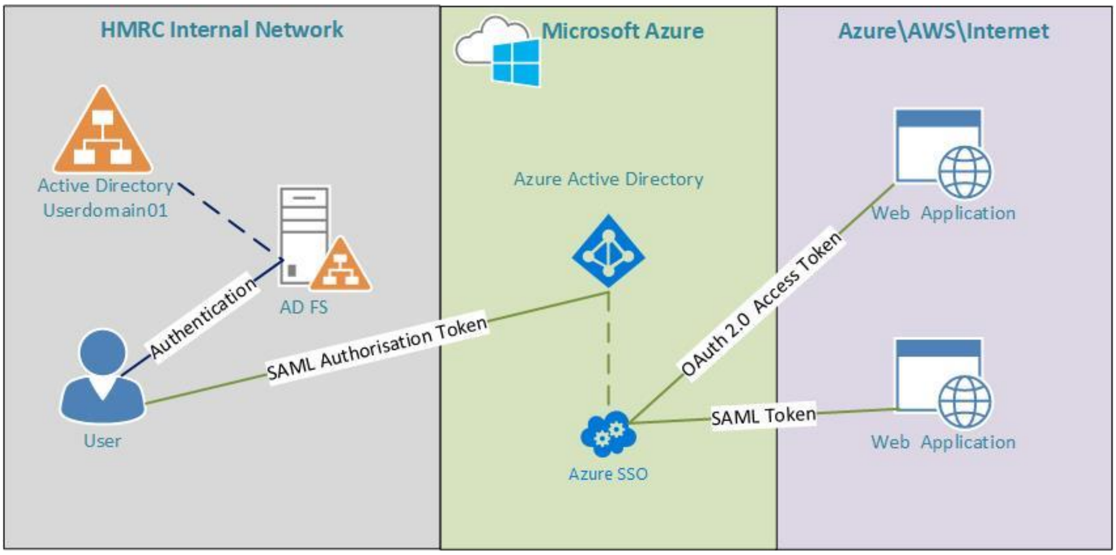
The application engineers will establish the file location for the certificate file so that it can be installed for the application.

Note that this certificate will be available in the "trusted root certification authority" store of any HMRC workstation that has Internet access. The certificate name is HMRC_ASPIRE_CA.

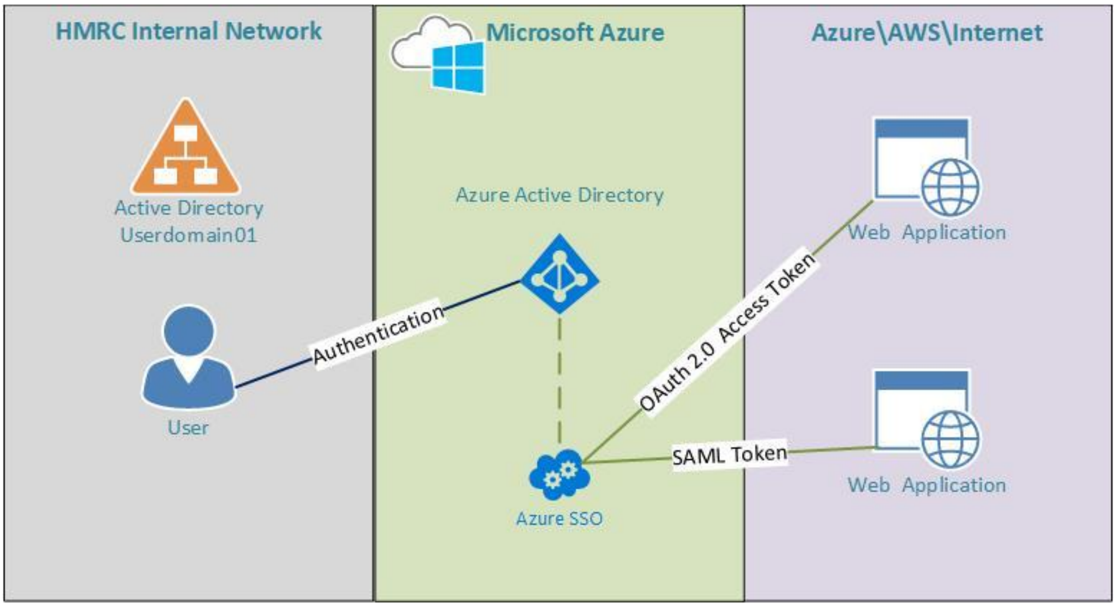
3.3.43 Current Environment Requires a Hybrid SSO

At the time of writing, HMRC users are authorised to Azure SSO via a federation with the on-premise AD FS-based service. This means that all users accessing Azure SSO as a service first authorise with Azure AD. The user is authenticated against the internal AD by the AD FS service using their logon credentials and is then authorised to Azure AD via a SAML token.

The diagram below illustrates this process:



The strategic goal for HMRC is to have all users authenticating directly with Azure AD and not with the HMRC internal AD. When this happens, the use of AD FS will be deprecated, and the following state will be reached:



Until this state is reached, the authentication to the internal AD and the authorisation steps to Azure SSO can be ignored by projects integrating with SSO. They should have no effect on being able to integrate the target application or service. However, they should be kept in mind when considering things like communications requirements.

Note in the diagrams above that Azure SSO can generate both SAML tokens and OAuth 2.0 Access tokens. The integration process is different for these two token types, so they are detailed in separate sections below.

The following sections will detail the high-level processes that should be followed to perform an SSO integration using the HMRC instance of Azure SSO.

3.3.44 Application Permissions to Azure APIs

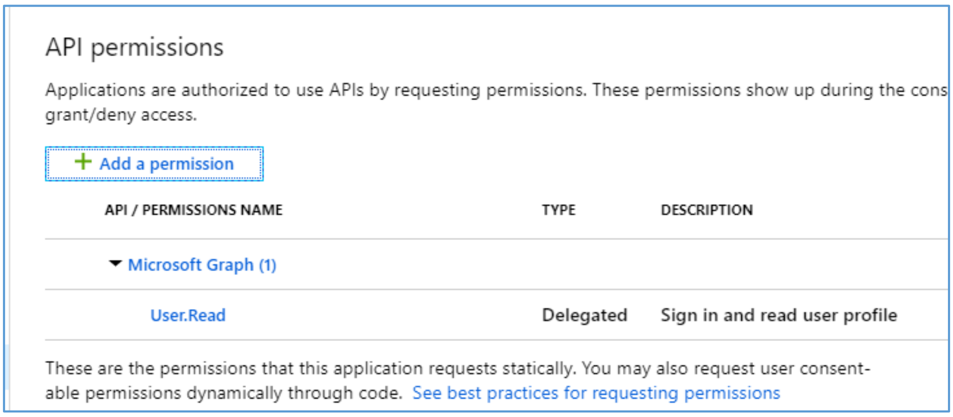
Microsoft Azure exposes a number of Application Programming Interfaces (APIs) which can be used by applications to read\write\amend information. These APIs can also be used to expose functionality, such as the ability to send an email on behalf of the user who is signed into the application.

When a project is deploying a new application, which will require access to these APIs, then certain restrictions will need to be considered when designing the solution:

- API Permissions are NOT enabled by default
- Only delegated permissions will be approved by HMRC Security
- Use of Application Permissions will NOT be allowed due to security concerns
- All permissions requested will need to be reviewed and signed-off by HMRC Security

API permissions are NOT enabled by default

When an application registration is created in the HMRC Azure AD, the only default permissions allocated to the application is user.read for the Microsoft Graph API:



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the cons grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION
▾ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

The Microsoft Graph API is the main API which allows access to information in the Azure Active Directory (AAD). This permission is required to allow the requesting user to log in and to supply information about their identity to the application.

No other API permissions will be available by default and must be requested.

There are two permissions scopes for APIs:

- Delegated Permissions
- Application Permissions

Delegated Permissions

Delegated permissions mean that requests to the API are made in the security context of the user who has previously been authorised to the application. This means that Azure sees these requests as coming from the user and can control access to resources based on the users' identity. If the user does not have permissions to certain data, or to perform certain operations within an application, then the existing security controls will prevent this access. The application can access resources and perform actions, but only those that the user has permissions to anyway.

Application Permissions

Application permissions allow the application to access APIs using a Authority secret value without any identity context. Due to this, restrictions on operations or data that can be accessed cannot be applied. Also, to compound the security concerns, no audit logs are produced for the access as there is no identity to log against.

This is the reason that Application Permissions are not currently permitted on the HMRC Azure Tenant.

Security Sign-Off

> Requesting additional API permissions, be it to Graph, SharePoint or any of the other applications, will have to be signed off by security before CDG will enable them. This is to prevent an application from being assigned wide-ranging permissions to HMRC data which do not adhere to the least privilege security principle.
>
> Your CDG\Capgemini contact will be able to advise and what is and is not typically allowed and if additional permissions are considered critical, the HMRC security will be briefed and asked for their judgement on the risks to data involved.

3.4 SSO INTEGRATION PATTERNS

3.4.1 Generic Integration Information

Before we move on to specific configuration steps that should be followed for the different SSO services provided by HMRC, we will summarise some of the strategy guidance we have had so far:

- Wherever possible, the Azure SSO service should be the choice of integration service.
- The OpenID Connect\OAuth 2.0 protocols should be used to integrate the solution. SAML can be used if this is not supported.
- SAML and Access tokens should only contain the information required to authorise the user and identify their role

3.4.2 Azure Gallery Applications

Microsoft have worked with vendors to create out-of-the-box integrations for hundreds of popular applications and services. Before you begin an integration, check on the Microsoft Azure website to confirm if there is a pre-configured integration template for your target app.

To check if there is currently a gallery application created for your target application, check on this website:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps

It should be noted that these gallery applications only create the basic application registration with no SSO settings configured. They also do not cover the integration of externalised roles for the target application. Therefore, they are of very limited use when attempting to integrate an application with Azure SSO.

3.4.3 User Experience - IMPORTANT

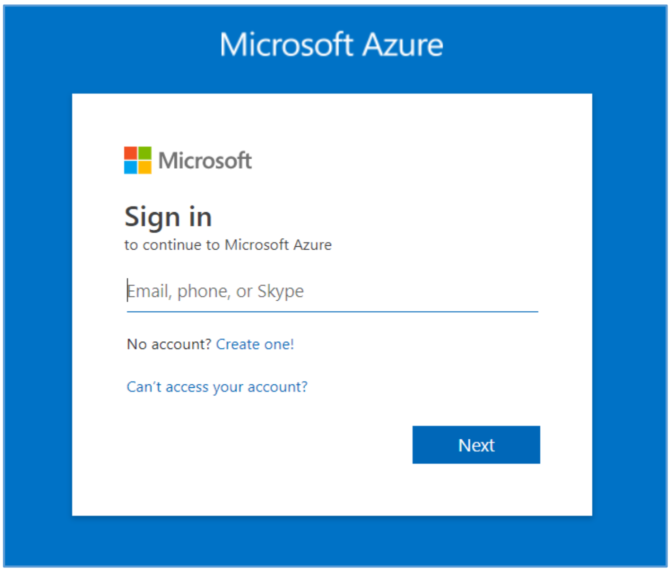
When logging into services or applications protected by Azure AD and Azure SSO integration, users will have one of two possible experiences.

For clarity, I will refer to these two user experiences as the legacy and the integrated experience.

The Legacy Login Experience

When users first invoke an application protected by Azure SSO and using OAuth 2.0, the application will redirect them to Azure for authentication.

The users will, on first login be presented with the following dialog box:



Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

Email, phone, or Skype

No account? Create one!

Can't access your account?

As this is the first time that the user has accessed the application, the dialog box will be unpopulated.

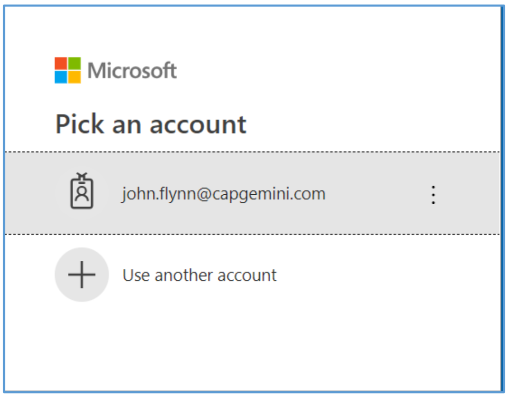
HMRC users will need to enter their Office 365\Azure login name in order to proceed.

The format for this login name is <emailprefix>@hmrc.gov.uk

While this does look a lot like a HMRC user address, it is not and has a different suffix after the @.

Once the username has been entered, the user will click Next and this will initiate the login process to Azure.

On subsequent logins to the application, irrespective of whether the user is accessing an application protected by SAML or OAuth 2.0, the user will see the “Account Picker” screen each time they access the application for the first time each day:



Microsoft

Pick an account

john.flynn@capgemini.com

The above experience is being superseded by the introduction of a number of enhancements to the way that Azure AD and Authoritys are integrated. This includes the making Authority devices "domain joined" so that they are used as an authentication factor, as well as the introduction of a browser plug-in which removes the need to see these dialogs from Azure.

The Integrated Login Experience

This experience will be transparent to the users and no dialogs will be presented as part of the login.

At the time of writing, the experience that the user will see is shown in the table below.

Authority Operating System	Browser Variant	Experience
Windows 10	Microsoft Edge	Integrated
Windows 10	Microsoft Intemet Explorer	Integrated
Windows 10	Google Chrome*	Legacy
Windows 10	Firefox	Legacy
Windows 7	Google Chrome*	Integrated
Windows 7	Other	Legacy

* A browser plug-in is currently being deployed which will remove the prompts from the Chrome browser and make it integrated.

3.4.4 Management Documentation

Every SSO integration will be reliant on an item of encryption material in order to validate the tokens and communications that will be utilised during the sign-on process. For a SAML integration, this is a digital certificate called the SAML Signing Certificate (SSC).

This certificate is generated automatically when an application is registered in Azure SSO and have a validity period of 3 years. If this certificate should expire then SSO will fail for all users of the specific application. It is up to the project delivering the application into Live service to ensure that suitable documentation is written to allow the certificate to be renewed, and to detail how this new certificate can be applied to the application.

Security Note: Certificates expiring in Live production lead to service outages which cannot be allowed to happen!

For an OAuth 2.0 integration there are two items of encryption material which need to be maintained: the Authority secret that is used to authorise the Authority application to the token API and the certificate used to sign the bearer tokens.

The application servers will make a connection to the Microsoft Token Endpoint using a Authority secret value which is generated for the specific application. This Authority secret value has a two-year validity period. and will need to be replaced before it expires.

The OAuth 2.0 tokens themselves will be signed using a certificate which is part of the federation metadata for the domain. This certificate will also need to be updated before it expires.

3.4.5 Vendor\Developer Communication

Any successful SSO integration is reliant on a good channel of communication being set up between the project and the vendor\developer of the application which is to be integrated. Up to a point, all SSO integrations are the same, but ultimately the application or service will have specific requirements in terms of the protocols is can support and the information about the user which should be included in the SAML\Access token supplied by the STS.

The following list are typical questions that a project may need to ask the application vendors or developers. Each application will be different, with differing levels of vendor documentation and vendor knowledge around SSO. Some of the questions below may not be relevant to your integration, but they should help as a guide:

- Does your organisation publish an SSO integration guide for the target application?
- Which SSO protocols does your application support?
- What attributes need to be included in the SAML\Access token to authorise the user to the application?
- Can your application consume\publish Federation Metadata?
- What value will represent the Name Identifier for the application users?
- Does your application use Role Based Access Control (RBAC)?
- If it does, can the user role be derived from a value in the SAML\Access token?
- If your application supports OpenID Connect, will it support the Authorisation Token Flow?
- Does your application use an identity store to hold information about users?
- If it does, how is that identity store maintained?
- Does your application expose a console to allow HMRC to perform management of the application?
- Are the SSO integration configuration components exposed through this console?

- In the event of issues with the SSO service to your application, what escalation routes are available?

Clearly, due to the nature of some of these questions, it is vital that the application vendor\developer have a technical resource on-hand to discuss this and assist the project will their integration. Project Managers should ensure that such a resource is available from an early stage in the project, so that the integration approach can be agreed before time and resource have been spent on an approach that will not work.

3.4.6 Project Actions

Establish the following information with the application vendor\developer:

- Protocol that will be used to integrate
- The number of users likely to require access to the application
- Information about the users which will be included in the security token
- Application URL that users will connect to with their browser
- Reply URL for the Token to be returned to
- The roles that the application exposes and the values in the authorisation tokens that will represent those roles

SRS Integration:

- Engage with the **Roles and Access** team to have the requisite SRS Roles created
- Ensure that the SRS Roles have AD security groups associated with them
- Populate the SRS roles with service users

Azure SSO Configuration (CDG):

- Create an Application Registration (App Reg) within the Azure AD Management Console
- Define the application roles in the application manifest
- Map the roles to Azure AD groups
- Generate the Authority secret for the application
- Pass the Authority secret to the web application support team

3.4.7 Current Engagement Process

The process for engagement for an SSO integration, at the time of writing is as follows:

The project must raise a CR and send it to the CDG Front Door team to request assistance with an SSO integration. The impact returned by CDG for this work will currently include time for a Capgemini resource (either the author or one of his colleagues), to engage with the project to provide consultation on the best approach to integrating their application.

Once the design has been agreed, then a Technical Note (TEN) will be created which will include details of the solution for SSO along with instructions that CDG can follow to create the application registration required to allow SSO to function.

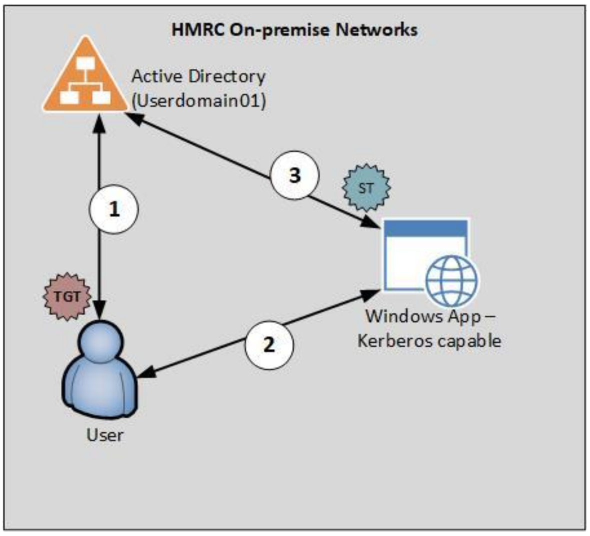
3.4.8 Integration Pattern Options

When integrating with the SSO services provided by HMRC, you have the following choices in order of preference:

Kerberos

Kerberos is a form of Single Sign-On, but it has limitations which make it an unsuitable choice for authenticating and authorising domain members to external applications. Microsoft use Kerberos v5 in their Active Directory implementation, and it relies on both the Authority device and the server(s) hosting the application being member systems in the AD domain.

The steps required for a Kerberos authentication and subsequent authorisation are as follows:



1. During the authentication process, the Authority will contact a domain controller and provide credentials to the domain. Once the user is authenticated, they are issued with a token called a Ticket Granting Ticket (TGT).
2. When the user wishes to authorise to an application they will connect to the server and be redirected to a domain controller. They will present their TGT (this is valid for 8 hours by default) and will be issued a Service Ticket (ST) for the server hosting the application.
3. The Authority will now present this ST to the server hosting the application. The server will check the service ticket is valid and then allow access based on authorisation information contained in the service ticket.

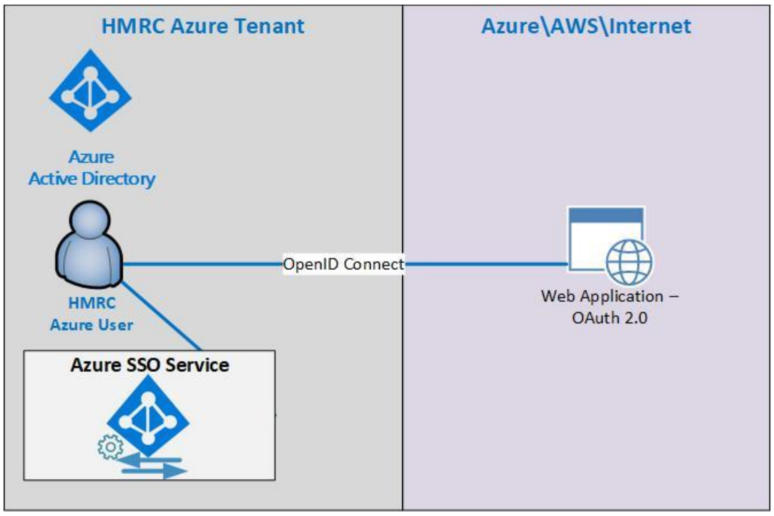
The above is a slightly simplified version of how Kerberos works, but it is intended to illustrate the restrictions that Kerberos has:

- Both the Authority and the server or servers hosting the application must have a pre-existing trust relationship with the domain. They must be members of the same domain or members of different domains which have a trust relationship established.
- Both the Authority and the server must be able to communicate with the domain controllers for the domain or domains to perform authentication and authorisation

This limitation means that Kerberos is only suitable for use on internal networks as you would never expose your domain controllers to the internet directly. Kerberos is also not useful where the server or service hosting the application is not running the Microsoft Windows operating system. Various methods can be used to allow a non-Windows system to participate in a Kerberos-based domain, but none of these are particularly robust and all are difficult to implement and manage.

Azure SSO\OpenID Connect

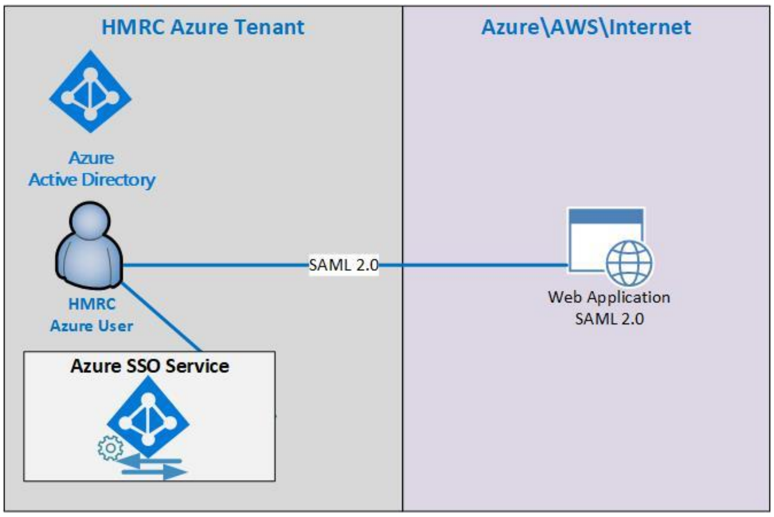
This option is the strategic option which should be used whenever possible by new integrations. Most modern web applications and services will support the OpenID Connect\OAuth 2.0 protocol and this protocol is now considered the industry standard. Modern applications should also be able to integrate with Azure SSO, because the service produces standard SAML and OAuth 2.0 access tokens. Therefore, the service generating these tokens should not be relevant.



Users will authenticate to Azure AD and the Azure SSO service will produce OAuth 2.0 access tokens to allow SSO to web applications hosted either in Azure, AWS or any other service provider on the Internet.

Azure SSO\SAML

This option, whilst using the strategic STS of Azure SSO, uses the older SAML protocol. There are some limitations as to the information that can be included in a SAML token produced by Azure SSO, so this combination of STS and protocol is not always the best choice. If the application can only consume SAML tokens, then the choice will depend on what information needs to be included in the tokens. If the attributes do not require any kind of manipulation and are available in the Azure AD, this this integration option will be a valid choice.



3.5 AZURE SSO\OPENID CONNECT\OAUTH 2.0

In order to integrate an application with Azure AD so that it can use Azure SSO to authorise users, a configuration items called an **Application Registration** must be created. This is created in the Azure Management console for the HMRC Azure Tenant.

The following section details the integration steps required when using the Azure SSO service and OpenID Connect\OAuth 2.0 as the integration protocol.

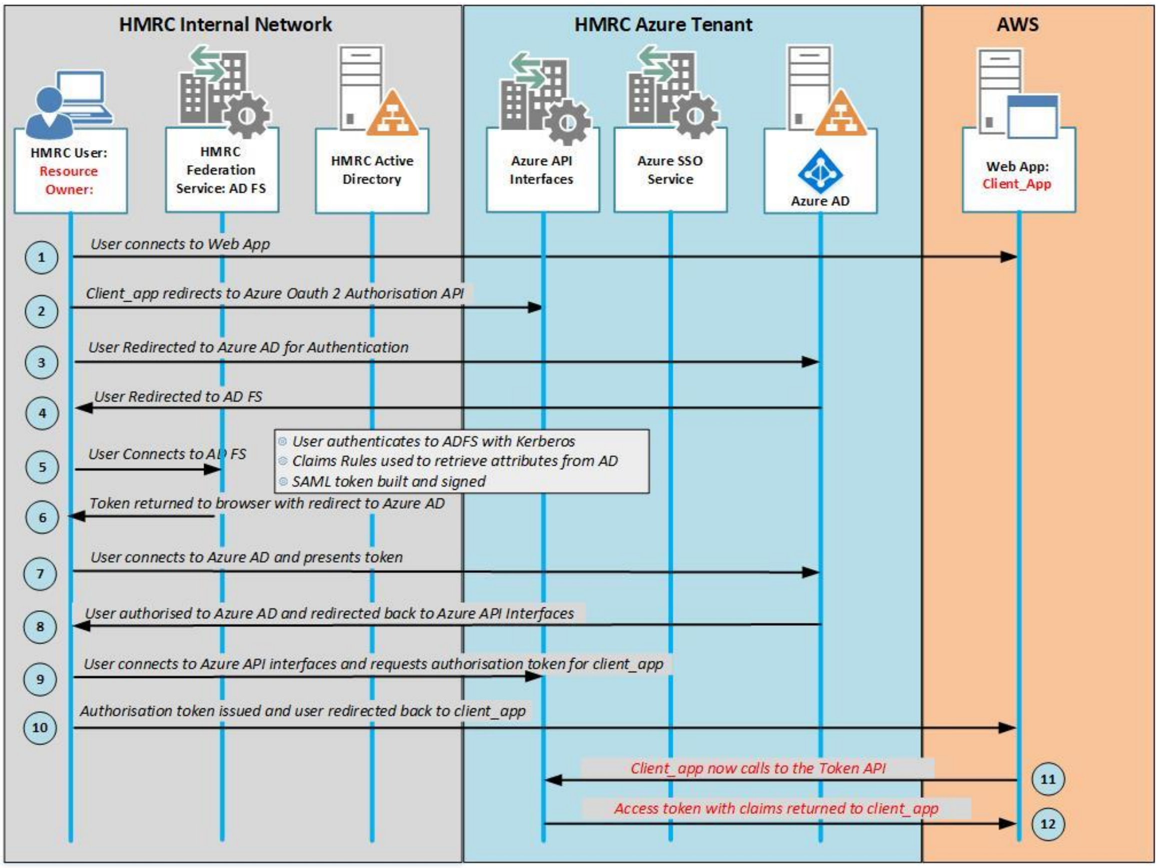
The following high-level processes will need to be followed to create an integration:

- Register the application in Azure AD
- Configure the application roles in the manifest (optional)
- Map the Azure AD groups to the application roles or assign them to the application registration
- Create the Authority_Secret value
- Enable Mapped Claims in the application manifest (optional)

As indicated, not all of the steps above are required for all application registrations.

3.5.1 Detailed Communication Flow

As mentioned in section 3.3 above, all HMRC users are authorised to Office 365\Azure AD by the on-premise AD FS service. This leads to the following communications flow each time a user first accesses an application:


HMRC Internal Network
HMRC Azure Tenant
AWS
HMRC User: Resource Owner:
HMRC Federation Service: AD FS
HMRC Active Directory
Azure API Interfaces
Azure SSO Service
Azure AD
Web App: Client_App
1 User connects to Web App
2 Client_app redirects to Azure Oauth 2 Authorisation API
3 User Redirected to Azure AD for Authentication
4 User Redirected to AD FS
5 User Connects to AD FS
User authenticates to ADFS with Kerberos
Claims Rules used to retrieve attributes from AD
SAML token built and signed
6 Token returned to browser with redirect to Azure AD
7 User connects to Azure AD and presents token
8 User authorised to Azure AD and redirected back to Azure API Interfaces
9 User connects to Azure API interfaces and requests authorisation token for client_app
10 Authorisation token issued and user redirected back to client_app
11 Client_app now calls to the Token API
12 Access token with claims returned to client_app

The following is an explanation of each of these communication steps:

1. The user will connect to the web application using their browser
2. The Authority application needs to get an authorisation code from the Azure AD Tenant Authorisation API
3. To authenticate, the user must be redirected to the Azure AD.
4. The user is redirected to AD FS on the HMRC internal network in order to authenticate
5. The user is authenticated by AD FS using their logged in credentials and Windows Integrated Authentication (WIA)
6. AD FS builds the SAML token for authorisation to Azure AD\Office 365 and returns it to the user, the user is now redirected back to Azure AD
7. The user connects to Azure AD and is authorised
8. Once authorised the user is redirected to the Azure AD Authorisation API and requests the authorisation token for the Authority application
9. The Authorisation Token is issued, and the user is returned to the Authority application
10. The Authority application now takes the authorisation token and presents it to the Azure token API for HMRC’s Azure tenant
11. The access token is issued with the correct claims in it as configured when the application is registered in Azure AD
12. The Token is returned to the Authority app and used to authorise the user

If the user has already accessed an Office 365 application or service prior to accessing the web application, then they have already been authorised to Azure AD. This means that steps 3 to 7 above will already have been completed and are not relevant.

Note the interactions in steps 10 to 12. These are between the application servers and the Azure API endpoints. Therefore, your application must be able resolve the URL of the Azure API and then initiate a TCP\IP connection to it. This will almost always be via a proxy service and the server will have to be configured to route to and authenticate to the proxy service in order to reach the API.

3.5.2 Network Protocols

- All communications performed by the Authority will use standard HTTPS on port 443\TCP
- All communications between the Authority application and the Azure APIs will use HTTPS on port 443\TCP

The above assumes that the Authority application communications are protected by Transport Layer Security (TLS) and use HTTPS from the browser.

3.5.3 DNS Name Resolution

Authority and application name resolution requirements differ dependent on whether the application is consuming SAML tokens or OAuth 2.0 access tokens. For a SAML integration, the Authority needs to be able to resolve and connect to the application and the Azure SSO service. Due to the more complex requirements of an OpenID Connect\OAuth 2.0 integration, both the Authority and the application servers need to be able to connect to a couple of APIs in order to get an authorisation code and then retrieve a bearer token.

Authority to Application

Authority devices will need to be able to resolve the URL of the target application to an IP address to which it can route packets. If the application has a different URL on the internal network to that on the internet, then both names should be resolvable.

Authority to OAuth 2.0 Authorisation API

The HMRC Azure tenant exposes an API which is used allow OpenID Connect Authoritys to obtain an authorisation code after authentication has been performed (see section 2.11.2 above).

The format of the API URL is:

```
https://login.microsoftonline.com/{Tenant_ID}/oauth2/authorize
```

Your Authority devices will need to be able to resolve this URL using DNS and route to the IP address returned through any security controls which may be in place on the network. Note that this URL will resolve to a large number of potential IP addresses, so configuration of security controls will need to factor this in. As HMRC users currently consume Office 365 and a number of other Azure cloud-hosted services, this connectivity should already be in place. It is called out here in case your Authoritys are in a network location where standard connectivity may not be available.

Application to OAuth 2.0 Token API

The HMRC Azure tenant exposes an API which is used allow OpenID Connect Authority applications to obtain an access token by presenting the authorisation token issued to the user (see section 2.11.2 above).

The format of the API URL is:

```
https://login.microsoftonline.com/{Tenant_ID}/oauth2/token
```

Your application servers will need to be able to resolve this URL using DNS and route to the IP address through any security controls which may be in place on the network.

Application to Federation Metadata Endpoint (Optional)

To retrieve and update the token signing certificate, the application server should be able to resolve and route to the following Federation Metadata URL.

```
https://login.microsoftonline.com/{Tenant_ID}/federationmetadata/200
7-06/federationmetadata.xml
```

The TSC can also be retrieved manually by opening this URL in a web browser.

> **Security Note:** All network traffic should be protected by TLS and all URLs should have a HTTPS prefix. The SAML and OAuth 2.0 tokens generated for HMRC users are NOT encrypted by default and therefore must be sent across the network in an encrypted tunnel.

Certificates

A number of digital certificates are involved in both security Authority\server communications and also to allow validation of the OAuth 2.0 tokens generated by Azure SSO.

Authority\Server Certificates

This is the certificate which sits at the front end of the target application and is used to secure the traffic across the network between the HMRC users Authority device and the servers\application. For third-party hosted applications, the certificate must be signed by a public Certification Authority (CA), the HMRC strategic CA is Digicert. If the certificate will contain a service\common name which contains a HMRC owned namespace (hmrc.gov.uk), then HMRC will have to acquire the certificate as a third-party would not be able to request a certificate containing a namespace they do not own.

If the certificate will contain a namespace owned by the third-party vendor (vendor.com), then it must be acquired by them as only they can request certificates for that namespace.

If the Authority application has a different URL for internal users to that used by internet-based users, then both names must be included in Subject Alternative Name (SAN) entries in the certificate. This will prevent users from seeing Common Name (CN) errors in their browsers when they access the application frontend.

OAuth 2.0 certificates signed by the HMRC Azure SSO have signatures on them which allow their origin and integrity to be validated. The public certificate required to allow this validation can be retrieved programmatically from the HMRC Azure Tenant Federation Metadata URL at:

https://login.microsoftonline.com/ac52f73c-fd1a-4a9a-8e7a-4a248f3139e1/federationmetadata/2007-06/federationmetadata.xml

3.5.4 Authority Secret Management

A typical OAuth 2.0 integration will use the authorisation code flow detailed in section 2.12.2 will utilise a Authority secret value to authenticate the Authority application to the Azure token API. This Authority secret and how it will be configured have been discussing in section 2.12.3. The Authority secret will only be valid for 2 years and will need to be replaced before it expires. The process for doing this is included in another document which will be supplied to you by CDG upon request. While the actions detailed in the document are mainly performed by CDG, it is not the responsibility of CDG to renew your Authority secret. This must be managed by the Live Service support team when the renewal is due.

3.5.5 OAuth 2.0 Tokens - Standard Attributes

RFC7519 defines both the protocol definitions and the default token content for the OAuth 2.0 standard. These are listed in the table below for reference.

Claim Type	Example Value	Notes
aud	3b4aec9c-97eb-4dd4-a736-bae3aef64e45	The intended recipient of the token. The application that receives the token must verify that the audience value is correct and reject any tokens intended for a different audience
iss	https://sts.windows.net/5fec8dec-0202-4951-b86f-a4336acc3605/	Identifies the security token service (STS) that constructs and returns the token. In the tokens that Azure AD returns, the issuer is sts.windows.net. The GUID in the Issuer claim value is the tenant ID of the Azure AD directory. The tenant ID is an immutable and

		reliable identifier of the directory.
Iat	Tue Sep 25 2018 14:32:34 GMT+0100 (British Summer Time)	Stores the time at which the token was issued. It is often used to measure token freshness.
Nbf	Tue Sep 25 2018 14:32:34 GMT+0100 (British Summer Time)	The “nbf” (not before) claim identifies the time before which the JWT MUST NOT be accepted for processing. (RFC 7519)
exp	Tue Sep 25 2018 15:37:34 GMT+0100 (British Summer Time)	The “exp” (expiration time) claim identifies the expiration time on or after which the JWT MUST NOT be accepted for processing. (RFC 7519)
aio	ASQA2/8IAAAA2SBlbfbsvHKByAg 1YeD+k8s2lOggDr2IZO+Kk1dtcf0=	
amr	pwd	Identifies how the subject of the token was authenticated
family_name	Smith	Provides the last name, surname, or family name of the user as defined in the Azure AD user object.
Given_name	Paul	Provides the first or given name of the user, as set

		on the Azure AD user object.
Ipaddr	192.168.10.10	
name	Paul Smith	
nonce	hlc38ake1g	The nonce passed in the request that must be verified by the Authority. (RFC 7519)
oid	5ecfd5b5-dbbc-45a7-8304-b106df20253d	Contains a unique identifier of an object in Azure AD. This value is immutable and cannot be reassigned or reused. Use the object ID to identify an object in queries to Azure AD.
Onprem_sid	S-1-5-21-1671065913-2506172178-4058957284-1127	
sub	vgb3fJoWG-1s8Kkku7F2vgQD5ys5y-vZrT6AqFGr3x8	Identifies the principal about which the token asserts information, such as the user of an application. This value is immutable and cannot be reassigned or reused, so it can be used to perform authorization checks safely. Because the subject is always present in the tokens the Azure

		AD issues, we recommended using this value in a general purpose authorization system
tid	5fec8dec-0202-4951-b86f-a4336acc3605	An immutable, non-reusable identifier that identifies the directory tenant that issued the token. You can use this value to access tenant-specific directory resources in a multi-tenant application. For example, you can use this value to identify the tenant in a call to the Graph API.
Unique_name	paul.smith@securepki.co.uk	Provides a human readable value that identifies the subject of the token. This value is not guaranteed to be unique within a tenant and is designed to be used only for display purposes.
upn	paul.smith@securepki.co.uk	Stores the user name of the user principal.
uti	WaaBZh9sd0GP12OwgCSVAA	
ver	1.0	Stores the version number of the token.

Note that the user PID is NOT included in this attribute set as standard.

The user PID in the HMRC AD is stored in the “saMAccountName” attribute, which is synchronised into Azure AD as “user.onpremisessamaccountname”.

This attribute can be “added” to an OAuth 2.0 token using a configuration item called a Claims Mapping Policy.

AZURE SSO\SAML

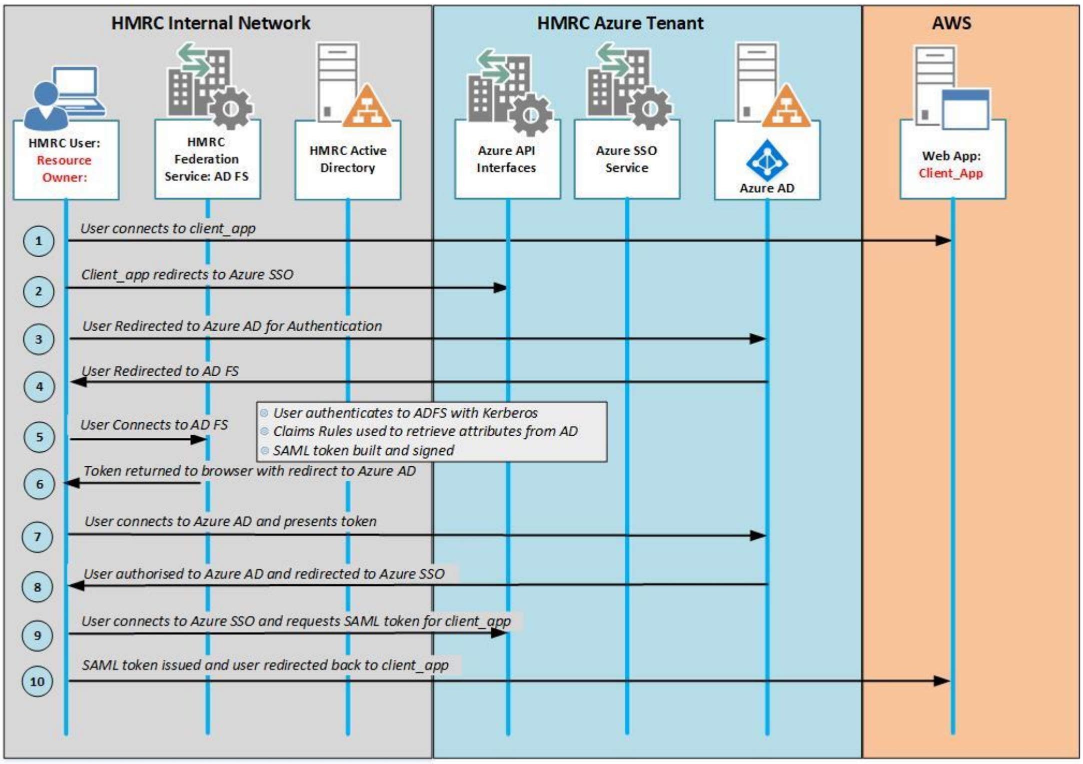
Azure SSO can also generate security tokens based on the SAML 2.0 protocol which is still the most popular standard for SSO integrations. If the consuming application is only able to integrate with SAML-based SSO, then the following sections will detail how this is accomplished with Azure SSO.

Azure AD uses a different name in the management console for a SAML-based SSO integration. The configuration item that CDG will create is called an **Enterprise Application** registration.

Detailed Communication Flow

The following section details the integration steps required when using the Azure SSO service and SAML 2.0 as the integration protocol.

As mentioned in section 3.3 above, all HMRC users are authorised to Office 365\Azure AD by the on-premise AD FS service. This leads to the following communications flow each time a user first accesses an application:


HMRC Internal Network
HMRC Azure Tenant
AWS
HMRC User: Resource Owner:
HMRC Federation Service: AD FS
HMRC Active Directory
Azure API Interfaces
Azure SSO Service
Azure AD
Web App: Client_App
1 User connects to client_app
2 Client_app redirects to Azure SSO
3 User Redirected to Azure AD for Authentication
4 User Redirected to AD FS
5 User Connects to AD FS
User authenticates to ADFS with Kerberos
Claims Rules used to retrieve attributes from AD
SAML token built and signed
6 Token returned to browser with redirect to Azure AD
7 User connects to Azure AD and presents token
8 User authorised to Azure AD and redirected to Azure SSO
9 User connects to Azure SSO and requests SAML token for client_app
10 SAML token issued and user redirected back to client_app

The following is an explanation of each of these communication steps:

1. The user will connect to the web application using their browser
2. The web application redirects the user to Azure SSO to obtain a SAML token
3. To authenticate to Azure SSO, the user must be redirected to the Azure AD
4. The user is redirected to AD FS on the HMRC internal network
5. The user is authenticated by AD FS using their logged in credentials and Windows Integrated Authentication (WIA)
6. AD FS builds the SAML token for authorisation to Azure AD\Office 365 and returns it to the user, the user is now redirected back to Azure AD

7. The user connects to Azure AD and presents the SAML token for authorisation
8. Once authorised the user is redirected to Azure SSO and requests the SAML token for the Authority application
9. The SAML Token is issued, and the user is redirected back to the Authority application
10. The Authority application validates the SAML token and allows the user access

If the user has already accessed an Office 365 application or service prior to accessing the web application, then they have already been authorised to Azure AD. This means that steps 3 to 7 above will already have been completed and are not relevant.

3.5.6 Network Protocols

- All communications performed by the Authority will use standard HTTPS on port 443\TCP
- All communications between the Authority application and the Federation Metadata endpoint will use HTTPS on port 443\TCP

The above assumes that the Authority application communications are protected by Transport Layer Security (TLS) and use HTTPS from the browser.

3.5.7 DNS Name Resolution

In a SAML 2.0 integration, all communications are driven from the Authority browser. Due to this, the Authority browser needs to be able to resolve the URL of the applications and the URL of the Azure SSO Security Token Service. Note that all of the Microsoft URLs will already have been configured for HMRC Authoritys as part of the Microsoft Office 365 deployment. Therefore, they are included here in case the application is being accessed by non-standard HMRC Authority devices which may not have the ability to resolve or route to them.

Authority to Application

Authority devices will need to be able to resolve the URL of the target application to an IP address to which it can route packets. If the application has a different URL on the internal network to that on the internet, then both names should be resolvable.

Authority to Azure SSO Security Token Service

In a SAML integration, the Authority application is redirected to the Azure SSO STS to retrieve a SAML token.

The format of the STS URL is:

```
https://sts.windows.net/ac52f73c-fd1a-4a9a-8e7a-4a248f3139e1
```

Your Authority devices will need to be able to resolve this URL using DNS and route to the IP address returned through any security controls which may be in place on the network.

Application to Federation Metadata Endpoint (Optional)

If the target application is capable of consuming Federation Metadata (see section 2.9), then it will need to be able to resolve and route to the following URL

https://login.microsoftonline.com/ac52f73c-fd1a-4a9a-8e7a-4a248f3139e1/federationmetadata/2007-06/federationmetadata.xml

The TSC can also be retrieved manually by opening this URL in a web browser.

3.5.8 Certificates

Authority\Server Certificate

Network traffic to the Authority application should have its communications protected using HTTPS. The certificate protecting these communications will need to be trusted by all Authoritys irrespective of whether it is signed by the HMRC internal PKI or a public Certification Authority (CA).

If the Authority application has a different URL for internal users to that used by internet-based users, then both names must be included in Subject Alternative Name (SAN) entries in the certificate. This will prevent users from seeing Common Name (CN) errors in their browsers when they access the application front-end.

SAML Signing Certificates

Each Enterprise Application registration created in Azure AD will automatically have a SAML Signing Certificate generated as part of the process. This is a self-signed certificate which is valid for 3-years and will be used by Azure SSO to sign the SAML tokens that it produces in response to HMRC user requests.

Renewal of this certificate is vital in order to keep the SSO service for the application functional. If the certificate expires then Azure SSO will no longer be able to use it to create signatures on SAML tokens and the SSO service will fail.

A separate document is being prepared which will detail the renewal processes for SAML Signing Certificates (SSC) which can be used by projects to plan their certificate management processes.

3.5.9 Accessibility

The Supplier shall work toward achieving WCAG 2.1 AA accessibility standards in respect of the Services by the Operational Service Commencement Date or as earlier as practically possible thereafter, in accordance with the Authority’s legal requirement to ensure all digital services and products purchased and/or operated meet public sector accessibility regulations.

0 TERMS & ABBREVIATIONS

Term	Explanation\Expansion
AADC	Azure AD Connect
ACS	Assertion Consuming Service
AD	Active Directory
AD FS	Active Directory Federation Services
Azure	Microsoft Cloud Service
CSP	Cloud Service Provider
CTO	Cloud Technology Office
DG	Delivery Group
GCDS	Google Cloud Directory Sync
HMRC	HM Revenue & Customs
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Secure
IdP	Identity Provider
JSON	Java Script Object Notation
JWT	JSON Web Token
OAuth 2.0	Open Authorisation version 2
OIDC	OpenID Connect
PrD	Process Document
RFC	Request for Change
RP	Resource Provider
SAML	Security Assertion Mark-up Language
SCIM	System for Cross-domain Identity Management
SRS	Service Request System

Term	Explanation\Expansion
SSC	SAML Signing Certificate
SSO	Single Sign-On
STS	Security Token Service
TeN	Technical Note
TSC	Token Signing Certificate
URL	Universal Resource Locator
WAP	Web Application Proxy
XML	eXtensible Mark-up Language