AccessPay Service Descriptions

V. 2.5

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

The BACS Service

This service allows a business to make or collect payments to/from a bank account for which they have a Service User Number ('SUN') using Bacstel-IP for the Direct Credit, Direct Debit and AUDDIS schemes. The service provides the following:

1. The ability to create user accounts up to a maximum of the number of user accounts specified in the Sales Order
2. The ability to deactivate user accounts
3. The ability to create the number of SUNs specified in the Sales Order (these must be of the Direct Submitter type for Bacs)
4. The ability to link the number of Bank Accounts specified in the Sales Order to one or more SUNs.
5. The ability to upload files, using the number of different Payment File Formats specified in the Sales Order. The Payment File Formats will contain data relating to payments and/or collections. The data can be uploaded via the [customer_sub_domain].accesspay.com website
    a. Each file must contain 100,000 transactions or less
    b. No more than 5 files can be uploaded every 15 minutes
    c. The selection of which of the defined SUNs the payments will be made from will be done manually from the customer_sub_domain.accesspay.com website or the SUN will be contained within the Payment File Format.
    d. The Payment File Formats must be defined by the Customer during the data collection exercise within 14 days from the Commencement Date, otherwise a Standard File Format will be applied for each
    e. If clients need files that contain more than 100,00 transactions or need more than 5 files to be uploaded every 15 minutes then this can be accommodated and agreed between the two parties, as long as AccessPay are informed with 24-hour notice before these files are uploaded.
6. The ability to validate the uploaded data relating to payments and collections to check:
    a. The information needed by Bacs is present or can be added by the system
    b. Sort codes and account numbers are in the correct format using a modulus check
7. The ability to receive email notifications to notify named Users when a file is uploaded, if any submitted file fails the validation checks above, and when a file has been delivered to Bacs.
8. The ability to review files that have been uploaded but not yet submitted to Bacs at a summary level (number and value of Direct Debits, Direct Credits and AUDDIS) and by looking at each transaction within the uploaded file.
9. The ability to cancel a file that has been uploaded but not yet submitted to BACS
10. The ability to set the Bacs processing date up to 30 days forward from the date on which the file was uploaded
    a. This is Step 2 in the standard 3-day Bacs submission cycle (Step 1 – input, Step 2 – processing, Step 3 – payment. Payment is made the next banking day after the processing date.
11. The ability to digitally sign and submit a payment file to Bacs using a Bacstel-IP / FPS approved smart card and card reader
    a. These smart cards and readers are industry standard and to work in a live environment require a program which must be installed on a non-thin client PC within the Customers IT network with which the Bank supplied card reader is compatible, which is running Windows 7 or later and which has been given access to connect to Bacstel-IP through the Customers corporate firewall.
12. The ability to download the following Bacs reports (in .xml, .csv or .html formats) to the PC on which the smart card reader is installed using a Bacstel-IP approved smart card and reader
    a. ARUDD / AUDDIS / ADDACS reports
    b. ARUCS / AWACS reports
    c. Withdrawal reports
    d. Input reports
    e. Arrival reports
    f. These smart cards and readers are industry standard, and to work in a live environment require a program which must be installed on a non-thin client PC within the Customers IT network with which the Bank supplied card reader is compatible, which is running Windows 7 or later and which has been given access to connect to Bacstel-IP through the Customers corporate firewall

13. The ability to view the contents of any file submitted to BACS for processing through the service, and any Bacs submission summary received in response.

The sFTP service

Access to an SFTP server with a unique username and password.

a. The Suppliers standard folder structure and permission set will be used, which involves a Inbound folder (for file uploads) per Payment File Format.

b. A single user account will be provided

c. In addition to username & password the link will be secured using an SSH-2 RSA, 2048bit key pair which must be generated by the Customer. Supported keys and parameters are.

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

2. The Customer must provide the key pair referenced above within 14 days of the Commencement Date, otherwise the system will be configured to operate without the SSH-2 encryption (so it is FTP rather than sFTP)
3. The service will check the sFTP folder structure at least every 5 minutes to check for new payment files, and if any are found these will be treated in the same way as files uploaded via the web interface – they will be assigned to a submission configuration and treated accordingly
   a. The bank account to be used for Payment File Format will be contained within the file or will be configured per submission configuration
4. For files uploaded using the sFTP service the Customer is able to manually amend the processing date or select the SUN to be used from a drop-down list.

The API Service

The API Service details are available **here**

The FPS service

This allows a business to make payments from a bank account for which they have a Service User Number ('SUN') using the Faster Payment DCA Service provided by some UK sponsor banks. The service complements the Bacs Service and additionally provides the following:

1. The ability to transmit Faster Payment (Direct Credit) files to Secure-IP on the same day on which the file was uploaded only (forward dating Faster Payments is not possible)
2. The ability to download a Faster Payments Input Report (in .csv or .xml format) within 4 days of transmitting the original submission file.
3. The ability to create the number of SUNs specified in the Sales Order (these cannot be changed and must be of the Direct Submitter type and for FPS)
4. The validation of the uploaded payment files to check
   a. The information needed by FPS is present
   b. Sort codes and account numbers are in the correct format using a modulus check
5. The ability to digitally sign and submit a payment file to FPS using an FPS approved smart card and card reader

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

a. These smart cards and readers are industry standard and to work in a live environment require a program which must be installed on a non-thin client PC within the Customers IT network with which the Bank supplied card reader is compatible, which is running Windows 7 or later and which has been given access to connect to FPS through the Customers corporate firewall

The HSM Submission Service

The HSM Service complements the Bacs and/or FPS Services and allows a user to store a digital certificate for authenticating and signing payment files, before transmission to Bacstel-IP or Secure-IP. The Service provides the following:

1. The storage of the number of Bank issued Bacs or FPS certificates as outlined in the Sales Order Form in a Hardware Secure Module device ('HSM') which provides a hardware and IP address dependent Certificate Signing Request
2. The ability to digitally sign and submit an uploaded file to Bacs or FPS using the digital certificates stored in the HSM which relate to Client
3. The Customer must agree to using the smartcard method of file signing and submission for at least 2 weeks, before using the HSM method of signing
4. The certificates provided by the Client must be HSM specific digital certificates provided by their Bank

The Reports Download Service

This service complements the HSM Submission Service, and the Bacs and/or FPS Services and uses the digital certificate stored on the HSM device to automate the download of Bacs reports. The Service provides the following:

1. The ability to configure a report download schedule where the Service will request reports based on previously defined parameters. Those parameters are:
    a. Report type
    b. Date Range / Processing Date
    c. Previously Accessed
    d. Service User Number(s)
2. The ability for the Service to poll the Bacstel-IP and Secure-IP services with the following frequencies:
    a. Bacs Service – maximum 2 times per Business Day
    b. FPS Service – maximum 12 times per day
3. The ability for the reports to be downloaded to the sFTP folder agreed during onboarding, with the following configuration options:
    a. Reports segregated per SUN and report type
    b. All reports dropped into a single sFTP folder
4. The ability for the reports to be accessed by request to our API endpoint
5. Where a customer has subscribed to the Reports Download Service, the customer must ensure that any active automatic download routines (using other Bacs services) are disabled before the activation of this Service.

The Unattended Submission Service

This Service complements the Bacs, FPS and sFTP Services and provides the ability to automate submission of payment/collection files to Bacs and/or FPS, with no manual intervention. The Service provides the following:

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

The ability to automate collection of files from the sFTP Service or via the API Service.

The ability to automate routing of the files, where all required data is contained within the payment file, or the data is configured to be added from a submission configuration.

1. The ability to automate validation of files, using the modulus check described in the Bacs and FPS Services.

The ability to pause the processing of the file, where the modulus check has returned the following result(s):

2. Transaction / file level warning

3. Transaction / file level error

4. The ability to automatically suppress transactions and continue processing the file, where the modulus check has returned the following result(s)

5. Transaction level warning

6. Transaction level error

The ability to automatically deliver the file to Bacs or FPS, where the file waits for a pre-defined waiting period, between 1 and 60 minutes, before delivery is commenced.

The Approval Service

1. The ability to require that all files are approved, using the Approval Service, using the approval process that is set up in the system before files can be submitted using the Bacs or FPS Services.
2. This approval process works as follows
   a. Up to 2 approval groups can be set up
   b. Each group can contain one or more system users
   c. A rule can be set up which determines whether a submission requires approval
   d. This rule can be based on the total value of the submission and/or the submission type (ie payroll)
   e. This rule will determine which approval group then needs to approve the submission
   f. If one person from the approval group logs in and approves the submission, then that approval step will be complete (if an approval is required)
   g. If 2 approval groups have been set up, then after one group has approved the second group will be required to approve.

The Bureau Service

This supplements the BACS, Direct Debit and sFTP services and provides the following additional functionality:

1. The ability to link Bureau User Numbers ('BUN's) to the service (this BUN cannot be changed)
2. The ability to create and delete bureau customers, each of which will have a unique SUN (of the in-direct submitter type only for Bacs) and bank details (sort code and account number), to a limit of 25 such bureau customers or the number of SUNs specified in the Sales Order.
3. The ability to select a bureau customer and then upload files on behalf of that customer, via the customer_sub_domain.accesspay.com website

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

a. Each file must contain 100,000 transactions or less

b. No more than 25 file can be uploaded every 60 minutes

c. If clients need files that contain more than 100,00 transactions or need more than 25 files to be uploaded every 60 minutes then this can be accommodated and agreed between the two parties, as long as AccessPay are informed with 24-hour notice before these files are uploaded

4. The ability to group submission files from multiple bureau customers into one multi-file for submission to Bacs

5. For files uploaded via sFTP or API the Customer must ensure that the Payment File Format or JSON message contains all SUN and Bank Account details required to submit to Bacs, or the user must select a bureau customer from a drop-down list.

The AccessPay BACS Bureau service

This service allows a business to upload Payments or Direct Debit collections from and to a bank account for which they have an Indirect Service User Number ('SUN') using the Bacstel-IP channel. The business can upload the files to AccessPay, who will then sign and submit the files to BACS, subject to approval using the **AccessPay BACS Bureau Approval Service**. All files which have been approved subject to the AccessPay BACS Bureau Approval Service will be sent to BACS. AccessPay bears no responsibility for checking the content or processing date of the files. AccessPay reserves the right to exclude any transactions or files which are suspected to be fraudulent or illegal transmissions.

The service provides the following:

1. The ability to create user accounts up to a maximum of the number of user accounts specified in the Sales Order
2. The ability to deactivate user accounts
3. The ability to add the number of SUNs specified in the Sales Order. These cannot be changed and must be of the Indirect Submitter type for BACS or be a Direct Submitter SUN which is linked to the AccessPay BUN for contingency.
4. The ability to link 1 Bank Account to 1 SUN (this cannot be changed)
5. The ability to upload files in up to 2 of the Standard File Formats containing a list of payments to be made, via the customer_sub_domain.accesspay.com website
    a. Each file must contain 100,000 transactions or less
    b. No more than 15 files can be uploaded every 60 minutes
    c. If clients need files that contain more than 100,00 transactions or need more than 25 files to be uploaded every 60 minutes then this can be accommodated and agreed between the two parties, as long as AccessPay are informed with 24-hour notice before these files are uploaded
    d. The selection of which of the defined SUNs the payments will be made from will be done manually from the customer_sub_domain.accesspay.com website
    e. The file must contain only BACS valid transaction codes 0N, 01, 17, 18, 19, 0C and 99.
    f. The Payment File Formats to be used must be confirmed by the Customer within 14 days of the Commencement Date of the Sales Order and be in the format(s) outlined in external document AP-PS-149 Payment File Format definition.
6. The ability to upload files up to the maximum number of file submissions specified in the Sales Order.
7. The ability for the user to validate the uploaded payment files to check
    a. The information needed by BACS is present
    b. Sort codes and account numbers are in the correct format using a modulus check
    c. If Direct Credit (Payroll) RTI files are processed, that the RTI code is in the correct format.

8. The ability for a second user to review files that have been uploaded but not yet submitted to BACS at a summary level (number and value of Direct Debits and Direct Credits) and by looking at each transaction within the uploaded file. This user can forward the file for submission and cannot be the User who uploaded the file.
9. The ability to delete a file that has been uploaded but not yet submitted to BACS
10. The ability to set the BACS processing date, which is Day 2 in the Bacs 3 Day cycle, up to 30 days forward from the date on which the file was uploaded
    a. This is Step 2 in the standard 3-day BACS submission cycle (Step 1 – upload, Step 2 – processing, Step 3 – payment made the next banking day after submission)
11. The ability to forward the file for submission by AccessPay to Bacstel-IP subject to approval using the **AccessPay Bacs Bureau Approval Service**. If the file is forwarded by 1pm on a Banking Day the file shall be submitted to BACS on the same Banking Day. If the file is forwarded after 1pm on a Banking Day the file shall be submitted to BACS no later than the next Banking Day.
12. A twice-yearly account review to assess transactional volumes and subscription level.
13. The ability to restrict access to the Service to a fixed IP address.

The service does **not** provide the following:

1. The ability to retrieve Bacs Reports, such as the Bacs Input Report. This report provides details of the payments that have been sent to Bacs on behalf of the Customer. The Customer must collect their copy of the Input Report via the Bacs Payment Services website following email notification from the Bacs service. If the client is unable to collect their Bacs Input Report for any reason, they must contact their Bacs sponsor before 11am on the Banking Day following Input to verify the Bacs transmission. The Customer must immediately advise the Bureau and their sponsor Bank of any errors identified on the Bacs Input Report. The Customer will also be responsible for dealing with any rejected or adjusted records identified in the Bacs Input Report.
2. The ability to cancel individual payments which have already been approved subject to The AccessPay Bacs Bureau Approval Service. The Customer must therefore arrange for the cancellation of individual payments by contacting their sponsoring Bank.
3. The ability to cancel a batch file of payments that have been approved subject to the AccessPay Bacs Bureau Approval Service. If the Customer wishes to cancel a batch file of payments which have been submitted, they must review the Bacs Input Report and immediately advise their sponsor Bank.
4. The ability to check that the file does not exceed the agreed file limit set by their sponsor Bank. The Customer must therefore perform this check prior to approval of a file subject to the AccessPay Bacs Bureau Approval Service.
5. Any other checking of the submission files or transactions within, other than those details within the above service description.

The AccessPay Bacs Bureau Approval Service

1. The AccessPay Bacs Bureau Service allows customers to upload files to the AccessPay website to be submitted by AccessPay to Bacstel-IP.
2. In order for a file to be successfully forwarded for submission by AccessPay, two different users will need to be involved in the process.
3. Two distinct user roles will be offered:
    a. **Uploader** – This role allows the user to upload the payment or collections file to the AccessPay website. This user will route the file by selecting the Bank Account, Service User Number and processing date of the file. This user will also carry out the validation of the file by initiating a modulus check. This user can suppress any transactions from the file which have received a Warning from the modulus check. Any Errors returned from the modulus check will be automatically suppressed and removed from the submission file. The resulting submission file shall be defined as the 'Final Uploaded Transactions File'.

   b. **Approver** – This user role will allow the user to approve the 'Final Uploaded Transactions File' and forward such file for submission by AccessPay. This user can review the transactions contained within the file. The user can also check the control totals of the file:
      i. Total number of transactions in the submission file
      ii. Total value of the transactions in the submission file.

4. Multiple user accounts can be configured, with each being categorised as an Uploader or an Approver.
5. Both user roles will be able to log in to the system using a username and password.
6. Both user roles will be required to log in to the website using either SSO or MFA to validate their credentials

The AccessPay Bacs Bureau Support Services

1. The AccessPay Bacs Bureau Support Services shall be provided by the Supplier during the Support Hours and shall comprise a telephone help desk to provide first-line technical support to users of the Supported Software.

2. The AccessPay Bacs Bureau Support Services shall be subject to a fair use policy.

The AccessPay Intermediary BACS Bureau service

This service allows an intermediary business to upload Payments or Direct Debit files from and to a bank account on behalf of their client who is an Indirect Bacs Service User. The intermediary is authorised by the Service User to process files using their Indirect Service User Number ('SUN') using the Bacstel-IP channel. The intermediary can upload the files to AccessPay, who will then sign and submit the files to BACS, subject to approval using the **AccessPay BACS Bureau Approval Service**. All files which have been approved subject to the AccessPay BACS Bureau Approval Service will be sent to BACS. AccessPay bears no responsibility for checking the content or processing date of the files. AccessPay reserves the right to exclude any transactions or files which are suspected to be fraudulent or illegal transmissions.

The service provides the following:

1. The ability to create user accounts up to a maximum of the number of user accounts specified in the Sales Order
2. The ability to deactivate user accounts
3. The ability to add the number of SUNs specified in the Sales Order. These cannot be changed and must be of the Indirect Submitter type for BACS or be a Direct Submitter SUN which is linked to the AccessPay BUN for contingency.
4. The ability to link 1 Bank Account to 1 SUN (this cannot be changed)
5. The ability to log in to the website using an approved username and password and MFA or SSO for further validation
6. The ability to upload files in up to 2 of the Standard File Formats containing a list of payments to be made, via the customer_sub_domain.accesspay.com website
   a. Each file must contain 10,000 transactions or less
   b. No more than 5 file can be uploaded every 60 minutes
   c. If clients need files that contain more than 10,00 transactions or need more than 5 files to be uploaded every 60 minutes then this can be accommodated and agreed between the two parties, as long as AccessPay are informed with 24-hour notice before these files are uploaded.
   d. The selection of which of the defined SUNs the payments will be made from will be done manually from the customer_sub_domain.accesspay.com website

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

e. The file must contain only BACS valid transaction codes 0N, 01, 17, 18, 19, 0C and 99.

f. The Payment File Formats to be used must be confirmed by the Customer within 14 days of the Commencement Date of the Sales Order and be in the format(s) outlined in external document AP-PS-149 Payment File Format definition.

7. The ability to upload files up to the maximum number of file submissions specified in the Sales Order.

8. The ability for the user to validate the uploaded payment files to check

   a. The information needed by BACS is present

   b. Sort codes and account numbers are in the correct format using a modulus check

   c. If Direct Credit (Payroll) RTI files are processed, that the RTI code is in the correct format.

9. The ability for a second user to review files that have been uploaded but not yet submitted to BACS at a summary level (number and value of Direct Debits and Direct Credits) and by looking at each transaction within the uploaded file. This user can forward the file for submission and cannot be the User who uploaded the file.

10. The ability to delete a file that has been uploaded but not yet submitted to BACS

11. The ability to set the BACS processing date, which is Day 2 in the Bacs 3 Day cycle, up to 30 days forward from the date on which the file was uploaded

    a. This is Step 2 in the standard 3-day BACS submission cycle (Step 1 – upload, Step 2 – processing, Step 3 – payment made the next banking day after submission)

12. The ability to forward the file for submission by AccessPay to Bacstel-IP subject to approval using the **AccessPay Bacs Bureau Approval Service**.

13. A twice-yearly account review to assess transactional volumes and subscription level.

15. The ability to restrict access to the Service to a fixed IP address.

The service does **not** provide the following:

1. The ability to retrieve Bacs Reports, such as the Bacs Input Report. This report provides details of the payments that have been sent to Bacs on behalf of the intermediary's client. The intermediary should ensure their client collects their copy of the Input Report via the Bacs Payment Services website following email notification from the Bacs service. If the intermediary's client is unable to collect their Bacs Input Report for any reason, they must contact their Bacs sponsor before 11am on the Banking Day following Input to verify the Bacs transmission. The intermediary's client must immediately advise the Bureau and their sponsor Bank of any errors identified on the Bacs Input Report. The intermediary and their client will also be responsible for dealing with any rejected or adjusted records identified in the Bacs Input Report.

2. The ability to cancel individual payments which have already been approved subject to The AccessPay Bacs Bureau Approval Service. The intermediary's client must therefore arrange for the cancellation of individual payments by contacting their sponsoring Bank.

3. The ability to cancel a batch file of payments that have been approved subject to the AccessPay Bacs Bureau Approval Service. If the intermediary's client wishes to cancel a batch file of payments which have been submitted, they must review the Bacs Input Report and immediately advise their sponsor Bank.

4. The ability to check that the file does not exceed the agreed file limit set by intermediary's clients' sponsor Bank. The intermediary must therefore perform this check prior to approval of a file subject to the AccessPay Bacs Bureau Approval Service.

5. Any other checking of the submission files or transactions within, other than those details within the above service description.

The PGP Encryption service

The PGP encryption service allows a customer of one of the following services - The Bacs Service, The FPS Service, The Bureau Service, The AccessPay Bureau Service, The AccessPay Intermediary BACS Bureau service to upload payment files which have been encrypted by the customer using PGP encryption. Files can be uploaded using the sFTP service or manually through the user interface.

The service provides the following:

- The ability to encrypt payment files with an AccessPay PGP public key
- The ability for those payment files to be subsequently decrypted by the AccessPay private key
- The ability to configure submission configurations to only accept PGP encrypted payment files
- The ability to configure submission configurations which do not require a payment file to be encrypted
- The ability to configure a new PGP key when an existing key is due to expire.

The Payment Screening Service

The Payment Screening Service allows a user to set rules around alerting potentially erroneous, fraudulent, or anomalous transactions within payment files. The rules can be configured against submission configurations or submission purposes. The service provides the following:

- The ability to enable the Payment Screening service for an organization that subscribes to the BACS or FPS services
- The ability to enable the Payment Screening service for an organization that subscribes to the Host-to-Host Service
-
- The ability to select the system objects (Submission Configurations or Submission Purposes) against which the Payment Screening Service rules will be configured
- The ability to set Payment Screening Service rules against one or more system objects
- The ability to grant users the 'Payment Screening Review' permission, which provides the following:
    - The ability to view file-level alerts based on the Payment Screening Service rules
    - The ability to view transaction level results based on the Payment Screening Service rules, which can be categorised as Low, Medium and High.
    - The ability to filter such transactions based on the Payment Screening status
    - The ability to view limited details of the reason for any alert based on the Payment Screening Service rules.
- The ability to set one or more rules from the following list:
    - Amount Threshold, which provides the ability to configure transaction-level alerts based on the transaction value
    - Total Transaction amount, which provides the ability to configure file-level alerts based on the total value of all transactions in the file
    - Total transaction count, which provides the ability to configure file-level alerts based on the total count of all transactions in the file.
    - Duplicate Third Party, which provides the ability to configure transaction-level alerts based on quantity of transactions in the file which contain duplicate combinations of Sorting Code and Account Number.
    - Creditor Unrecognised, which provides the ability to configure transaction level alerts based on the number of previously submitted transactions to a particular combination of Sorting Code and Account Number
    - Duplicate Amount Third Party which provides the ability to configure transaction-level alerts based on quantity of transactions in the file which contain duplicate combinations of Sorting Code and Account Number for the same transaction value.
    -
- The ability to cancel a file if the Payment Screening Service rules are deemed to have detected an erroneous, fraudulent, or anomalous transactions.

The service does not provide the following:

- The automated suppression or removal of any transaction(s) based on the Payment Screening Service rules
- The automated cancellation of any file based on the Payment Screening Service rules.

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

The MFA Service

The MFA Lite Service allows a customer of one of the following services - **The Bacs Service**, **The FPS Service**, **The Bureau Service, The AccessPay Bureau Service**, **The AccessPay Intermediary BACS Bureau service, The AccessPay Host to Host Service** to secure access to such services by utilising 'Multi-Factor Authentication'. This means, in addition to entering a username and password (after navigating to a predetermined URL) a user must authenticate their user credentials by using a Smartphone-app, a physical token such as a Yubikey, or any other hard or soft-token which supports "Universal 2 Factor Authentication" (U2FA).

The use of **The MFA Lite Service** is subject to Duo Terms and Conditions set out at: https://duo.com/legal/pass-through-terms

The AccessPay Host-to-Host Service

The AccessPay Host-to-Host Service is a service which allows a Customer to send and receive messages using a direct link to their Bank. The service uses the direct link to the Bank to instruct payments and collections, receive response messages related to the instructions of payments and collections and further allows the retrieval of bank statements in the proprietary format offered by the bank.

The service provides the following:

- The ability to connect to the Bank's FTP Server to push or pull messages
- The ability to secure such connection by authenticating with the FTP server using Username, Password and SSH Key
- The ability to sign outbound messages (push) with 1 PGP key
  The ability to PGP encrypt outbound messages (push) with the Bank provided public key
- The ability to rotate these PGP keys every two (2) years
  The ability to send (push) payment messages to the Bank in the Pain.001 v3 (CGI-MP) format or other previously agreed format in the sales order
  The ability to collect (pull) payment response messages (Payment Status Reports) in the Pain.002 format or other previously agreed format in the sales order
- The ability to review payment statuses applied to transactions in the user interface.

The service is provided by the Bank, to the Customer, therefore the Customer should note that the services outlined **do not include**:

- Any cost of the Host-to-Host service(s) from the Bank(s)
- Any appropriate transaction fees associated with the instruction of payments or collections
- Any fee associated with the generation or retrieval of payment status reports
- Any fee associated with the generation or retrieval of bank statement messages.

The AccessPay Cash Management Service

AccessPay Cash Management automates the gathering of bank statement data, by routing bank statement information from bank accounts owned by an organisation via a SWIFT or Host-to-Host [is API a route here?] Channel to a single data repository – the AccessPay Cash Management database. The AccessPay Cash Management database normalises the data and then

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

presents it in an easily consumable user interface, where it can be represented and reviewed by region, by bank, by currency, by business unit or by legal entity and exported as sanitised csv files for ERP / Back Office System integration (depending upon which service elements are specified in the Sales Order Form).

The Service provides the following:

Users:

- Allows the creation of system users of the following four types:
    - Admin
        - Allows the creation of system users.
        - Allows the amendment of system user rules and permissions.
        - Allows the activation and deactivation of system users.
        - Allows a user to assign role(s) to other users.
        - Allows a user to change the role(s) of other users.
    - Read-Only (Oversight)
        - Allows the user to view the system data and view reports that have been generated.
    - Complete
        - Allows Read-Only access
        - Allows a user to create, update and deletion of system objects (i.e. statements, sweeps, transfers etc) but not user permissions
        - Allows a User to tag bank accounts using custom labels.
    - Treasury
        - Allows creation, update and delete of forecasts and balances
        - Allows a User to tag bank accounts using custom labels.
- Allows all Admin User types to:
    - Change their password [this is under preferences]
    - Change their name details
    - Change a mobile phone number
    - Change a user email address
    - Enable Two-Factor Authentication
    - Amend their User Preferences, which includes:
        - Base currency
        - Default filter criteria
        - Logical breakdown
        - Time zone
        - Change password

Banks and Bank Accounts

- Allows the addition of the number of BICs or Bank Connections as specified in the Sales Order via a SWIFT or a Host-to-Host Channe. API for HSBC only currently.
- Allows the manual creation of bank accounts within the AccessPay Cash Management system only
- Allows the automatic creation of bank accounts within the AccessPay Cash Management system only via bulk upload using a .csv template.
- Allows the receipt and processing of the following bank statement message types:
    - MT940 .fin messages as per the SWIFT MyStandards specification, plus Mt942, Camt 53, Camt 52.

- Where the customer is using their own SWIFT BIC, the service allows the Customer to link the above statement messages to bank accounts within the AccessPay Cash Management system using an Account Identifier via the Orphaned Statement process
- Where the customer is using the AccessPay BIC the service allows the Customer to link the above statement messages to bank accounts within the AccessPay Cash Management system by using the sender BIC within the MT940 message and the Account Identifier.
- Allows users to assign/remove the following additional data to/from a bank account:
    - Account Name
    - Account Identifier

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

- Account Number / IBAN / Bank Name / Bank BIC / Branch Code
- Legal Entity
- Country / Currency
- Open / Closed
- Account Type
- Custom Labels "tags"; the User is able to type free format text, assigning labels to a bank account to allow logical grouping and therefore reporting

Legal Entities

- Allows Users to create, update and delete legal entities.
- Allows Users to link these legal entities to a parent entity
- Allows Users to link a legal entity to a bank account within the AccessPay Cash Management system
- Allows Users to assign additional name and address details data to a legal entity.

Balances

- Allows Users to view opening and current balances by currency, bank, country, tags, legal entity & bank account
- Allows users to filter their view of their opening and current balances based upon currency, bank, country, tags, legal entity & account.
-
- Allows users to view balances in local (domestic) or base (converted) currency

Statements

- Allows Users to view MT940, Camt 52/53 statements that have been sent from their Banks via the Host-to-Host or SWIFT Channel in a statement view within the AccessPay Cash Management system. [API's for HSBC only
- .

Search

- Allows Users to search by the database of received MT940 messages by : bank, currency, country, account, tags, debit/credit, value date, value date range, amount, amount range , legal entity or reference.

Reporting

The Reporting Service allows Users to create p reports based on the statement data stored within the AccessPay Cash Management system: Tere is a list of 6 standard reports that data can be queried from

- Users are able to query data to form a report by:
  - Currency
  - Bank]
  - Bank account
  - Legal entity
  - Tag / label
  - Date range
  - Time scale
- Users are able to create, update and deactivate scheduled reports.
-
- Users are able to schedule the execution of these reports. Once generated each report becomes available in the generated reports tab
- Users are able to export the reports to .csv, where the .csv is downloaded from the browser; the .csv report is also visible in the generated reports tab
- Users are able to select that each report, once generated, is also transmitted by email to a list of email addresses which can be saved and subsequently amended.
- .
- Users are able to schedule the execution of these report to be exported to a file location where they can be retrieved by using the sFTP Service or delivered to specific email addresses.

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

Alerting

- Allows a User to configured alerts sent by email and/or SMS, to advise a user. List of alerts include:
    - Missing MT940 (by bank account / time / time zone)
    - Balance warnings
    - Cash inflow / outflow

Definitions:

Account Identifier: Is a unique key (per Bank) belonging to a bank account which is usually read from Tag 25. This unique key can **only** be an IBAN or a combination of Branch Code and Account number (i.e. BBAN).

The Open Banking Service

As a Registered Account Information Service Provider, AccessPay facilitate the capabilities to provide consent to your banking partners in order for AccessPay to provide AISP services on your behalf.

- You are able to provide consent by selecting your banking partner and being redirected to their online banking login page. Upon successful login, you will be asked to confirm whether you want to consent to AccessPay retrieving your account data, including but not limited to Account Static, Balance and transaction information, historically and going forward. {elaborate}

- **Account** static may include your Sort Code, Account Number, IBAN, Account Name, Address and beneficial owner information.

- **Balances** include Current Available balance on the accounts you have provided consent for and AccessPay will use this with the transaction data to determine the Opening and Closing balances on a daily basis.

- **Transaction data** may relate to both Debit and Credits and may include information such as references, beneficiary details including name and address, card numbers, accounts, sort codes, IBANs, SWIFT BICs, FX rates, interest & charges and other information relating to a given transaction.

AccessPay will use a combination of Balance and Transaction information in order to create a pseudo statement.

Consent can be revoked at any time by the user. Do this through your online banking portals.

You will need to re-authenticate with each of your banking partners approximately every 90 days, after which your consent will expire. AccessPay will advise of consents expiring however you are responsible for ensuring consents are maintained.

AccessPay may provide this service in partnership with other authorised Third-Party Providers.

AccessPay Single Sign On Service SSO

Single Sign-On (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029

Currently AccessPay users are each assigned a 'local login' meaning that every user has a username and password created in AccessPay and is used to verify the identity of the user. SSO will mean that your users will be able to register with AccessPay and log in using credentials issued by your organisation.

AccessPay supports SAML 2.0 Single Sign-On

The AccessPay Audit Module

This service allows designated Security or Audit employees to be able to run specific reports on activities that have taken place in the AccessPay platform. Reports are configurable by purpose and date-range, to allow our customers to save time on reporting when it comes to their required auditing season. Access to the Audit Service allows access to all 6 reports in their entirety, so clients must review which users are granted access permissions to match their security policies

Reports include:

- File Journey - report of all files processed through the platform, including which users uploaded, approved and submitted the file with time and date stamps of all steps.
- Admin Changes – changes that have been made, approved or rejected by your Admin Users.
- User Permissions – permissions of specific users within a predefined date range.
- Transaction Report – details of all transactions processed across multiple files, including suppressed transactions.
- User Access Monitoring – a log of users that entered the AccessPay platform with time and date stamps, as well as successful or unsuccessful login attempts

AccessPay Account Name Verification Service

Service details are available here

www.accesspay.com | +44 (0) 161 250 7778 | info@accesspay.com | AccessPay | City Tower, Piccadilly Plaza, Manchester, M1 4BT, UK | Company Registration Number: 08033029