payments strategy forum

December 2017

NPA Design and Transition Blueprint

Project/Programme Manager:	Adrian Burholt
Sponsor:	Payments Strategy Forum
Date of Final Approval:	11/12/2017
Approved by:	Otto Benz

Version / Document History

Version No	Date	Author	Comments
1.0	26th July	NPA workstream 2	First version
2.0	11th December	NPA workstream 2	Name changed from Design and Transition Supporting Document to Design and Transition Blueprint. Post consultation update: - Further analysis and explanation of running Direct Debits and Credits over the NPA - API and message flows section added Minor amendments - Improved definition for the consent and auth store components - JSON and XML positioning update - Design principles for multi-vendor options added - Further enhanced data use cases added - Minor change to the definition of attended and unattended payments

Contents

1 A New Payments Architecture – Introduction

1.1 About this Document

This document is an updated version of the Design and Transition Supporting Document published in July 2017 and takes input from the consultation feedback and subsequent discussions with industry stakeholder groups. The main updates include:

- Further analysis and description of how Direct Debits and Credits will work on the NPA. This was in response to feedback received through the consultation process. Especially around how Direct Debits could be supported by a push mechanism.
- In-depth analysis and description of the API and message flow for the NPA

In addition, amendments have been made to:

- Improve definition of the consent and auth store components
- Include further analysis of the messaging formats (JSON and XML)
- Add design principles for multi-vendor options
- Provide additional enhanced data use cases
- Improve the definition of attended and unattended payments

This document will be handed over to the NPSO.

1.2 Next Steps - Detailed Design Work

Our work since consultation and further discussion with stakeholders has also resulted in a list of key detailed design areas to focus on in more detail (see below). In particular and in common with many respondents, we recognise the importance that the payments industry places on Direct Debit.

The NPSO will be responsible for performing the next phase of design work for each of these key areas of focus. The result of this design work should be to determine the optimal solution for delivering the current retail payments system operators' products and services over the NPA that meets with regulators' requirements to enable competition, address customer detriments, limit disruption to service users, and ensure stability and resilience. The NPSO will be responsible for performing this next phase of design work.

I. Architecture & Payment Processing

- The role of the TPSP routing / validating / disaggregating payment files in place of retail payments system operators.
- The control of CASS during the validation process that the TPSP is now handling.
- The impact of replacing Bacs "A-Messages" with a new interface e.g. amending mandates via the existing ADDACS message.
- The potential clearing cycle for Direct Debits and Direct Credits.
- Identifying any additional detriments within existing retail payments system operators' services that need to be addressed during the service refresh.

II. Legal

- There will be a set of legal activities initiated by the NPSO in 2018 to assess the impact of the NPA on existing payment instruments, e.g. Direct Debit.

III. Service User Processes

- The role of the receiving PSP aggregating payment files instead of retail payments system operators.
- The impact of the reconciliation process for a large corporate and/or government department.
- The identification and process alignment for the Grade 3 government Direct Credit submitter.
- The economic and practical model for delivering services.

IV. Assurance

- As the design process moves through its stages, assurance and liability issues will be fully considered to ensure that customer impact and system security and resilience remain intact.

V. Regulatory

- The ownership and control of retail payments system operators' services, for example, ISA transfer, Bulk redirection, Affiliate training, Service User audits.

1.3 NPA Design Principles

The blueprint sets out a set of core design principles to underpin the NPA. The principles, extended into design considerations, have guided the NPA development journey as shown in table 1.1 below.

Core Design Principle	Design outcomes
1. A single set of standards and rules with strong central governance	The NPSO will be the central body that governs the NPA, including the setting of standards and rules, such as for overlay services and for technical considerations such as security. It will also be responsible for: PSP registration and certification of overlay service providers; defining and maintaining the standards for NPA operation.
2. End-to-end interoperability (including Application Programming Interfaces and a common messaging standard)	The NPA design is predicated on the establishment of a common set of standards to provide interoperability between NPA layers and participants. This has been achieved by: a. Setting clear boundaries for and, separation of, layers. b. Recommending ISO 20022 as the payment messaging standard. c. Support the transitioning methodologies.
3. A collaborative infrastructure, allowing multiple providers of overlay services to compete in the market simultaneously	Existing payment systems are operated as individual schemes with single service providers and access mechanisms. Our approach to the NPA design is to facilitate competition for services, and allow multiple vendors to operate services. This is achieved by: a. Taking a vendor agnostic design approach. b. Specifying a push payment model for all payment types. c. Adopting industry-wide standards and approaches.
4. The need to ensure our payment systems are secure and resilient, with financial stability as a key foundation	The NPA is bound by security and resilience requirements similar to existing payment systems, and financial stability must be enforced. The design proposition takes this into consideration and mandates the following: a. A common security standard.

Core Design Principle	Design outcomes
	b. Using the Bank of England's (BoE) RTGS system for settlement and ensuring settlement can always complete. c. The status of a transaction will always be known.

Table 1.1 NPA Design Principles and Outcomes

1.4 NPA Attributes

In the blueprint, we recommend that the NPA should adopt the following attributes to be able to best meet the design principles listed above.

1.4.1 Layered Approach

Currently, it is very difficult to make changes to payment systems without impacting those who use them. Multiple participants (some of whom will be competitors) that have to collaborate on changes will need to agree on implementation and testing approaches. The current systems are slow to change and act as a brake on innovation. To address this, we recommended a layered approach.

This layered model is one in which capabilities are separated into discrete layers. Each provides a defined function or part of the payment value chain, based on an agreed standard. 'Upgrade paths' for the components split across layers will be simplified and each layer can be changed with minimal impact on others. Different providers can compete for the delivery of the components within a layer; some layers may support multiple providers delivering services at the same time.

This approach fosters competition, innovation and ease of access to new entrants. It also reduces systemic risk, service outages and overall costs. This reduction is achieved through providing a clear layered structure and unifying interfaces and standards.

1.4.2 Overlay Services

A payment involves the transfer of value from a payer to a payee. The exchanges between the payer and payee do not technically need to be part of the underlying payment mechanism. The exchanges and supporting data can be delivered through overlay services.

The NPA has been designed to facilitate the emergence of end-user overlay services and PSP overlay services. These applications will 'plug' into the NPA system to provide 'core' and 'additional' services. The additional services are likely to be tailored to particular payments use cases and end-users.

Third Party Service Providers (TPSPs) will make use of the accessibility of the layered model to provide end-user overlay services, such as Request to Pay and Confirmation of Payee. Payment Service Providers (PSPs) will also be able to provide both end-user and PSP overlay services. We anticipate a high level of innovation within this layer.

1.4.3 Common Messaging Standards

Common messaging standards are necessary to enable interoperability between payments systems and reduce complexity. In this blueprint, we recommend the adoption of ISO 20022 to align the UK with global standards and modernise the UK's payments infrastructure.

We expect the use of ISO 20022 as the common messaging standard to deliver national interoperability and potential for international connectivity (e.g. SEPA immediate payments). Standardising messaging formats will reduce complexity and provide the basis for functional enhancements and innovation. It will also, reduce future development and integration costs. The ability of ISO 20022 to support the delivery of enhanced data and the tracking of payment status are additional benefits.

1.4.4 'Push' Payment Model

In this blueprint, we point to the use of push payments to provide simplicity and increase customer control. Today in the UK, push payments (e.g. Faster Payments) work alongside a pull payments model which supports services such as Direct Debits.

During the development of the blueprint, the concept of a push only payments model has been developed further to establish whether our proposition is suitable in light of the Forum's commitment to enabling competition, innovation and minimise risk in payment systems.

It is important to note that we envisage that Direct Debit payments will continue to be payee-initiated "pull" requests. We have set out the "push" payment concept as an underlying technical mechanism, which will support "pull" payments by means of overlay services. We have set out an approach for Direct Debit in which PSPs will execute Direct Debit requests on payees' behalf by converting them to "push" payments (to accept the requests) or as rejected advice where the payments cannot be applied. We believe that the NPA design for Direct Debits is consistent with the current ICS model for processing cheque payments. While we recognise that the adoption of the push model for the NPA may require further validation of the regulatory and contractual framework for payments processing, at this stage we do not believe that adoption of the push model would preclude the current operation of Direct Debit, which we see as a critical service to support.

In summary, we concluded that a push only model offers many advantages but recognise that for some of the industry, changes will be required to support the Direct Debit process. We have set out our view on the benefits and challenges below.

A transition approach has been defined to minimise the impact on existing providers and is set out in the Implementation Plan document. The approach gives time to Third Party Service Providers, including current independent software providers, bureaux and gateway providers, to update their systems. This approach enables existing payment formats to continue over the NPA with no or limited negative impact on the current users of services such as Direct Debit.

Category	Benefits	Challenges
Customer Control	• E-mandates will provide stronger customer authentication to ensure that a customer's Direct Debit Instruction (DDI) authorisation is not comprised due to fraudulent abuse. • Customers continue to be protected by a refund guarantee as they are today under the Direct Debit scheme. • Enhanced data can provide an opportunity for a customer to view related payment data to support any Direct Debit queries. This could minimise indemnity claims.	• The delivery of a new payments system may require contractual customer consent and may require clear responsibilities for payment liability to be re-stated.

Category	Benefits	Challenges
Systems and Processes	• A consistent and simplified payments delivery approach through the use of one payment mechanism with a single set of messaging, Application Programming Interfaces (APIs), standards and connectivity for all payment types. • The support of enhanced data to enable better customer experiences and streamline business process building on the use of ISO 20022.	• As payments messaging moves to ISO 20022 there will be a need for end-users to upgrade to ISO 20022 or establish, via a TPSP, a service that translates messages from existing formats to ISO 20022. • In this latter case an end-user, such as a utility company, could, therefore, continue to create their existing collection file via their billing system with no or limited internal technical changes needing to be applied. They will forego the benefits of some new services such as enhanced data when using a translation service. • Service providers and vendors that currently provide a bureau service or software solutions to collect Direct Debit payments on behalf of an end-user will need to redevelop their technical solutions for mandate management and payment collection. Supporting an e-mandate authorisation and processing an unpaid Direct Debit advice are two examples where the Direct Debit process will change under the NPA.
Operational	• We see that the adoption of push payments will simplify operational processing by ensuring payments are made using cleared funds. Direct Debit payments will continue to be initiated by the payee as a payment request. The PSP will continue to execute the payment on the due date, but only authorised cleared funds will be submitted for clearing and settlement. Payments that cannot be applied will be rejected as an unpaid "advice" and will not be submitted for clearing. The payee is therefore presented with a much more accurate cash flow position on the payment due date in comparison to current processes. • Enables flexible settlement cycle capability in the future.	• Organisations that rely on the current unpaid Direct Debit process for automating back office processing (such as arrears) may have to amend their operations to cater for the new unpaid "advice" message being received on the payment due date. • There will be a more involved collection process on the payee receiver side which will be required to receive the funds from multiple payers.

Category	Benefits	Challenges
Participant innovation benefits	• A simplified payment mechanism underpinned by a common set of APIs and messaging will provide current and future TPSPs with increased scope for innovation and the development of more competitive propositions for end-users.	

Table 1.2 Push Only Model Benefits and Challenges

Overall, we believe that the push payment model provides a number of benefits and do not see a significant impact on the overall risk of undertaking payments by moving to a push-only model. It is on this basis therefore that we have continued to base the NPA on a push only approach.

1.4.5 Stable Transition Model

Payments are of national importance and system stability is critical. The NPA has been designed to support the transition from current schemes with minimal risk and service disruption by avoiding a 'big bang' launch and ensuring payment interoperability on 'Day1'. We have defined a clear transition roadmap to allow existing payment systems to co-exist during the transition period with the parallel running of the current and new systems. Please refer to Section 6 for further detail on the transition approach.

1.4.6 Common Security Standard

The UK payments infrastructure is highly regarded globally for good security, relatively low fraud levels and high overall resilience. The design of the NPA intends to focus on maintaining these standards and improving them in the future.

We expect the New Payment System Operator (NPSO) to mandate a common security standard for all participants of the NPA, thus providing security, resilience and stability across more open payments architecture. The standards and recommendations from the second Payment Services Directive (PSD2) will be incorporated into this common security standard. Where relevant and possible, we expect to see the use of the security functions being developed by Open Banking to minimise delivery and operational impacts.

1.5 Alignment to Industry Initiatives

The design of the NPA where possible has taken consideration of on-going regulatory and industry initiatives, in particular:

1.5.1 Payment Services Directive 2 (PSD2)

PSD2 is proposed as a way to respond to the changes in the payments landscape and to promote improvements and innovation in payment services across Europe. PSD2 includes proposals to:

- Level the playing field for payment service providers, including new players.
- Ensure a high level of consumer protection and payments security.
- Encourage lower prices for payments.
- Facilitate the emergence of common technical standards and interoperability.

The NPA is fully aligned with PSD2 and each layer of the architecture has been designed to work within and support the PSD2 framework. This includes areas of the NPA design, such as payment initiation, which includes the new PSP definitions and security standards.

1.5.2 Open Banking

Open Banking provides a standard and framework for how PSP data should be created, shared and used. Specifically, it provides standards for 'open APIs' that enable PSPs to support data sharing requests. It is recommended that the NPA adopt these APIs as they meet (or will meet) the needs of the NPA and could reduce the need for additional development by the organisations offering services within the different layers of the NPA.

It is also recommended that consideration is given to adopting Open Banking directory services once it is clear how it will support all the potential users of the directory (and not just the CMA9 PSPs). An assessment of the Open Banking directory service indicates that it can meet the requirements of the different roles and layers within the NPA, such as supporting the delivery of the key functions of participant registration, identity access management and security authentication. Should it be required, however, the NPA would not preclude the use of a third party provided an alternative for the supply of the directory services capability.

Further analysis, since July 2017, has identified a number of APIs and directory services extensions that will be required to enable the full capabilities of the NPA and which are not currently on the Open Banking roadmap. The NPSO will need to consider its options for accessing or procuring these additional capabilities during its detailed NPA design work.

1.5.3 General Data Protection Regulation (GDPR)

GDPR impacts all organisations that process European Union citizen's personal data and aims to encourage organisations to construct a data protection strategy with privacy at the core. Key features of GDPR include pseudonymisation of customer data whether in transit or at rest and that the customer's details are the property of the customer.

The design of the NPA should not inhibit the NPSO's ability to build a GDPR compliant system and to enable their governance role which will want to ensure the participants within the layers of the NPA can also be compliant with both the GDPR technical security, customer rights to data and privacy requirements.

1.5.4 Fourth Money Laundering Directive (4MLD)

The Fourth Money Laundering Directive prevents the use of the financial system for the purposes of money laundering or terrorist financing. Much of the directive points to procedural changes outside of the NPA, however, the NPA's support of enhanced data and payment status capabilities could be used (if so directed by applicable laws) to provide valuable information in the campaign against money laundering and associated illicit activities. Along with the other regulatory requirements, it is suggested that this area will require further consideration as the NPA is specified, procured and delivered.

1.5.5 Real Time Gross Settlement (RTGS)

The NPA will use the BoE's RTGS service for the net settlement of payments between settlement participants. The NPA architecture has been designed with this settlement service at its core and will work with the BoE to be fully compliant with the requirements for interfacing with the renewed RTGS.

2 NPA Conceptual Model and Description

The following section presents our vision for the NPA. Contained is an overview of key elements that form the basis of the overall conceptual model for the NPA. The details in this section are intended to provide a view on the core responsibilities (scope) of each element. It is not intended that the scope is used as a comprehensive specification but only be used to highlight features that are material to understanding the NPA.

The logical structure of the layers and elements do not prescribe or dictate the physical implementation. The architectural concept being proposed sets out how UK retail interbank payment systems[1] can be built to enable simpler access, on-going stability and resilience, greater innovation and competition, along with increased adaptability, and better security to meet the needs of current and future generations of payments service users.

Taking a standardised and layered approach would also suggest that investments made in payment systems can be better protected, as, over time, each layer can evolve with minimal impact on the other layers. This 'isolation between layers' aspect of the NPA is also expected to mitigate against the risk of service outages and provide an easier upgrade path for the various components within the layers.

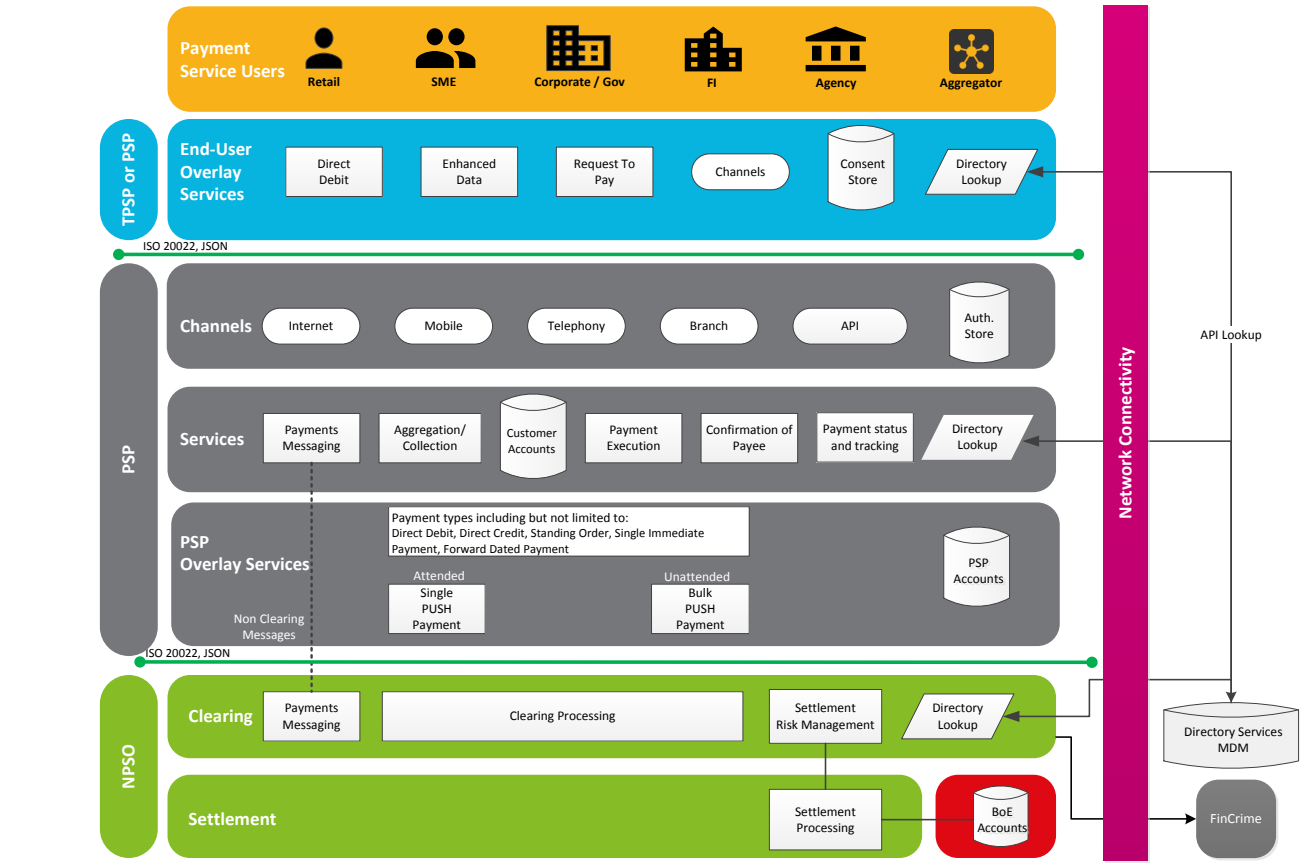
Layering is an already proven architectural approach, as seen for example in the mobile telephony industry, enabling Mobile Virtual Network Operators (MVNOs) to offer a fully mobile service without having the need for participants to own core infrastructure.

The following section explores how such a layered model might function and enable payments in the 21st Century.

2.1 The NPA Conceptual Model Layers

Industry stakeholders have come together to produce a conceptual model for the NPA that defines the relationship between various participants, connectivity mechanisms and supporting components across the layered architecture. The NPA conceptual model is presented in Figure 2.1 below. A description of each layer and its components follows in subsequent sub-sections.

[1] Card payments and CHAPS are out of scope for the NPA design.



Key:

Figure 2.1 NPA Conceptual Model

2.1.1 Payment Service User

Figure 2.2 Payment Service User Layer

Payment service users include Retail (or Consumers); Small and Medium Enterprises (SMEs); corporates and government; Financial Institutions; agency organisations and aggregators. The Payment Service Users make use of payment services in the capacity of a payer, a payee, or an intermediary.

Details of the participation models and potential impacts are covered in Section 7 of this document.

2.1.2 End-User Overlay Services

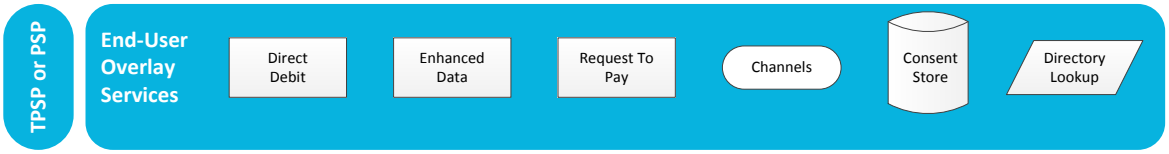


Figure 2.3 End-User Overlay Services Layer

One of the key features of the NPA is the use of overlay services which are expected to improve the payments network, customer experience and provide a vehicle for innovation. The NPA layered architecture has been designed to facilitate the emergence of overlay services. These applications will plug into the NPA system to provide core and additional services.

End-user overlay services are used by payment services users and will be delivered by Payment Service Providers (PSPs) and Third Party Service Providers (TPSPs). NPA will enable the delivery of overlay services such as Confirmation of Payee, Enhanced Data and Request to Pay. Other potential innovative services are expected to be provided within this layer. The end-user overlay services interface to the lower layers of the architecture via Application Programming Interfaces (APIs).

It is understood that PSPs that service customer accounts are likely to be able to assume TPSP based roles without further licensing requirements as per PSD2 Article 26.

This layer also holds the consent store against which PSPs or TPSPs will verify end-user authorisation for payment execution. Alongside the consent store, the end-user overlay layer provides a directory lookup service through which, TPSPs or PSPs will be able to access a subset of the reference data held, e.g. intended recipient details, which will support the routing of payments. The Consent Store and Directory service are referenced in greater detail in the supporting components section.

In addition to providing new APIs enabling TPSPs to submit payments and provide overlay services, it is envisaged that PSPs and TPSPs will provide channel mechanisms enabling customers to continue to submit payments in a similar manner as today. Specifically, corporates and PSPs with indirect access (traditionally called agency payments service providers) should be able to continue to submit payments in a similar manner as they do today by using accredited software sponsored by a direct settling payments service provider.

We envisage that the NPSO will set minimum standards for TPSPs in order to be able to accredit them to provide corporate and indirect participant access in a similar manner to Bacs suppliers today. However, they would not mandate the use of particular standards between participants in the end-user overlay services.

End-User Overlay Services Layer Components

DD (Direct Debit): An end-user overlay service that will support the current characteristics of the customer proposition for a Bacs Direct Debit but running over the NPA.

Enhanced Data: End-user overlay solutions, which allows payment service users to securely store and access additional information related to payment messages.

Request to Pay: Request to Pay is primarily a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment. The message will contain the data required to automatically pre-populate a payment instruction for the payer to authorise its PSP to permit the payment to proceed.

Channels: Channels are the web or mobile user interface provided by TPSPs to their customers to enable access to TPSP services.

Consent Store: The TPSP's Consent Store holds the authorisation token created by the PSP for its Payment Service User. The details stored in the consent store are similar to that of the Authorisation store. For more information see Appendix 1.

The auth token is held in the form of a 'digital token' which allows a TPSP to initiate a payment request on behalf of the customer. The token is passed to the TPSP from the PSP and references the payer's authorisation for that specific payment request.

Directory Look Up: The directory look-up is a function that looks up the master database to get the reference data necessary to make and route payments. Examples of reference data include Sort Code, Overlay level reference data, CASS account transfers and customer reference data, PSP and TPSP endpoints, roles and certificates.

2.1.3 PSP Channels

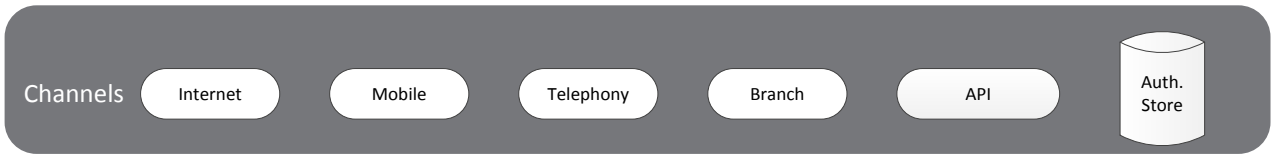


Figure 2.4 PSP Channels Layer

PSUs will be able to transact directly through a variety of channels provided by PSPs, such as the internet, mobile, telephony and branches, as they do today. In addition, TPSPs will be able to provide additional payment service channels by using APIs to interface with PSPs and gain secure access to customer accounts. Rules and standards for APIs are yet to be defined. These will be overseen and governed by the NPSO and where possible aligned to PSD2 and Open Banking.

PSP Channels Layer Components

Internet and Mobile: Digital channels provided by the PSPs to their customers so that they can access the PSP's services.

Telephony: A customer channel to access a PSPs services via the telephone.

Branch: A customer channel to access a PSPs services via a physical branch.

API: Interfaces provided to TPSPs by PSPs to facilitate authorised secure access to their customer accounts and payment services.

Authorisation (Auth) store: The 'Authorisation Store' holds the unique security tokens created when a payer authorises a specific amount to be paid to a specific payee. For more information see Appendix 1.

2.1.4 PSP Services Layer

Figure 2.5 PSP Services Layer

This layer is where the PSPs hold customer accounts and run services that are required to execute and process a payment against customer accounts. For example, a payment transaction such as funds check and debiting the customer would sit within this layer.

PSPs hold customer accounts which store customer funds and run services required to execute and process a payment against customer accounts within this layer.

PSP Services Layer Components

Payment Messaging: A communication channel that facilitates the exchange of non-clearing messages (e.g. reports and adjustments) between the PSP and the clearing and settlement service.

Aggregation/Collection: A function that collects funds for a customer's account and updates their account with the aggregated value.

Customer Accounts: A customer account that can be debited or credited by the PSP.

Payment Execution: A function that processes the payment at the payee's or the payer's PSP account and manages payment execution.

Confirmation of Payee: Confirmation of Payee is a service provided by the PSP to confirm the payee's identity.

Directory Look Up: The directory look-up is a function that looks up the master database to get the reference data necessary to make and route payments. Examples of reference data include Sort Code, Overlay level reference data, CASS account transfers and customer reference data, PSP and TPSP endpoints, roles and certificates.

2.1.5 PSP Overlay Services

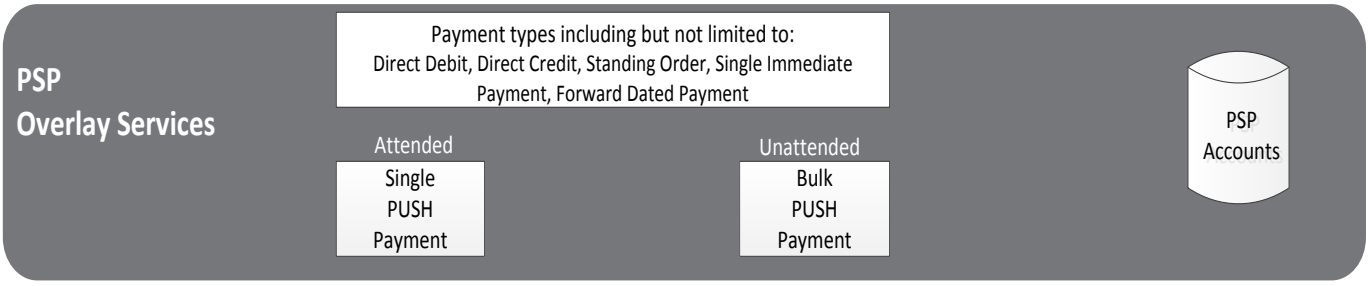


Figure 2.6 PSP Overlay Services Layer

This layer contains the rules, SLAs and protocols for those payment mechanisms through which PSPs can carry out attended and unattended push payments to emulate existing payment types including Direct Debit (e.g. utility bill payments), Direct Credit (e.g. salary payments), Standing Orders, SIPs and Forward Dated Payments. Therefore, the NPA will support today's payment types into the future. New payment types can also be developed for this purpose with the NPSO overseeing the approval process and ensuring interoperability between PSPs.

To support attended and unattended payments, this layer contains the interfaces to support initiation of single push payments and bulk push payments into the clearing layer.

Overlay services to support settlement could be required to provide the configuration and validation for a payment request. The specification for these overlay services could include settlement cycle, net settlement cap and financial modelling.

PSP Overlay Services Layer Components

Single Push Payment (Attended):

Single Push Payment routes and manages attended payment instructions between participants and ensures that the instructions finality rules are followed. This component will support multiple payment types such as SIP.

Coordination of clearing payments will be in near real-time. Attended payments will be processed for clearing immediately with the outcome being delivered to the submitter and the payee's PSP within a defined attended payments SLA.

Bulk Push Payment (Unattended):

Bulk Push Payment routes and manages unattended payment instructions between participants and ensures that that instructions finality rules are followed. The component will support multiple payment types that support bulk file submission such as Direct Credit (payroll processing), Standing Order payments and cheques (ICS).

Coordination of clearing payments will be to an agreed schedule with the outcome being delivered to the submitter and the payee's PSP within a defined unattended payments SLA.

One of the main differences between an attended and unattended payment relates to the different response times and service levels from the clearing layer for the two payment types.

PSP Accounts: PSP accounts are the operational accounts where payment contra entries are made against payment transactions.

2.1.6 Clearing Layer

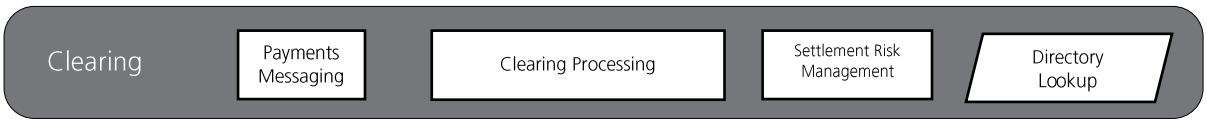


Figure 2.7 Clearing Layer

clearing layer coordinates the non-clearing payments messaging (e.g. threshold alerts), clearing and settlement processing for attended and unattended payments. It also carries out the following functions:

- Assures validation of non-clearing payment messages and their routing.
- Performs settlement risk management.
- Notifies participants of the payment outcome.
- Notifies participants of the settlement outcome.

Payment clearing processing in the NPA is logically split between attended and unattended payments. It allows SIPs to be processed immediately but also provides the flexibility for bulk payments processing to be handled based on configuration parameters.

The settlement risk component is responsible for processing settlement risk checks from clearing processing. Its primary function is to check the transactions can settle by ensuring the clearing and settlement participants (PSPs / authorised submitters) are operating within their Net Sender Cap (NSC).

Impact on scheduled payments

In the current landscape (e.g. Bacs), simultaneous processing of credits and debits on the value date are supported by processing payments from all participants together in the same settlement window. In order to give the customer the best outcome in terms of applying credits and debits to their account, transactions are held until a cut-off is reached after which all credits are applied and then followed by debits. This model allows funds to become available for outbound scheduled payments to be made at the same time as the inbound payment on day 3 of the Bacs process.

The NPA push model cannot ensure inbound payments are received and cleared before an outbound scheduled payment that is due on the same day. Therefore, submitters will need to push payments according to defined SLAs to ensure payments are processed and received by the payee by the expected date.

Payments received for clearing and settlement will always assume that the payer's PSP has authorised and accepted liability for the payment being cleared and settled. In the context of Direct Debits, the TPSP or PSP is responsible for submitting files (on behalf of the collecting organisation) to the payer's PSPs according to defined SLAs to ensure payments are processed and received by the payee by the expected date.

Receiving Cleared Payments

Participants processing bulk payments today receive a single file of inbound payments to process. To provide a consistent experience, the NPA could batch together cleared payments for a receiver that does not have the capability to receive and process multiple files throughout the day.
The batching of cleared payments could be managed by the NPSO to ensure that the cleared payments are processed consistently for all receiving participants. The NPSO will need to ensure that the frequency of receiving inbound payments will allow the payee to receive inbound payments (making funds available) in time to allow scheduled outbound payments to be submitted for clearing and settlement.

Returns / Receiver Rejected Payments

Returns will be managed as a new submission from the original payee's PSP to the original payer. The original payee's PSP will be the sender and the original payer will be the receiver. It is assumed that the payment messages will allow the participants to identify that the payment is a return and allow them to identify the original payment being returned.

Clearing Layer Components

1. Payments Messaging

A communication channel that facilitates the exchange of non-clearing messages (e.g. reports and adjustments) between the PSP and the clearing function.

2. Clearing Processing

The clearing processing element is responsible for coordinating clearing of attended and unattended payments.

Clearing and settlement are designed to be similar for all payment types, attended (single) or unattended (bulk). Payments that are submitted for clearing will be from a single sending PSP to a single receiving PSP.

Authorised submitters will be responsible for splitting the files and ensuring that only payments authorised by the payer's PSP are submitted for clearing.

For attended payments, coordination of clearing payments will be in near real-time. Attended payments will be processed for clearing immediately with the outcome being delivered to both the submitter and the receiver within a defined SLA.

For unattended payments, coordination of clearing payments will be to an agreed schedule, with the outcome being delivered to both the submitter and the receiver within a defined SLA.

The information flow below demonstrates the relationship between the NPA elements. This is a conceptual representation and does not cover all the information being exchanged.

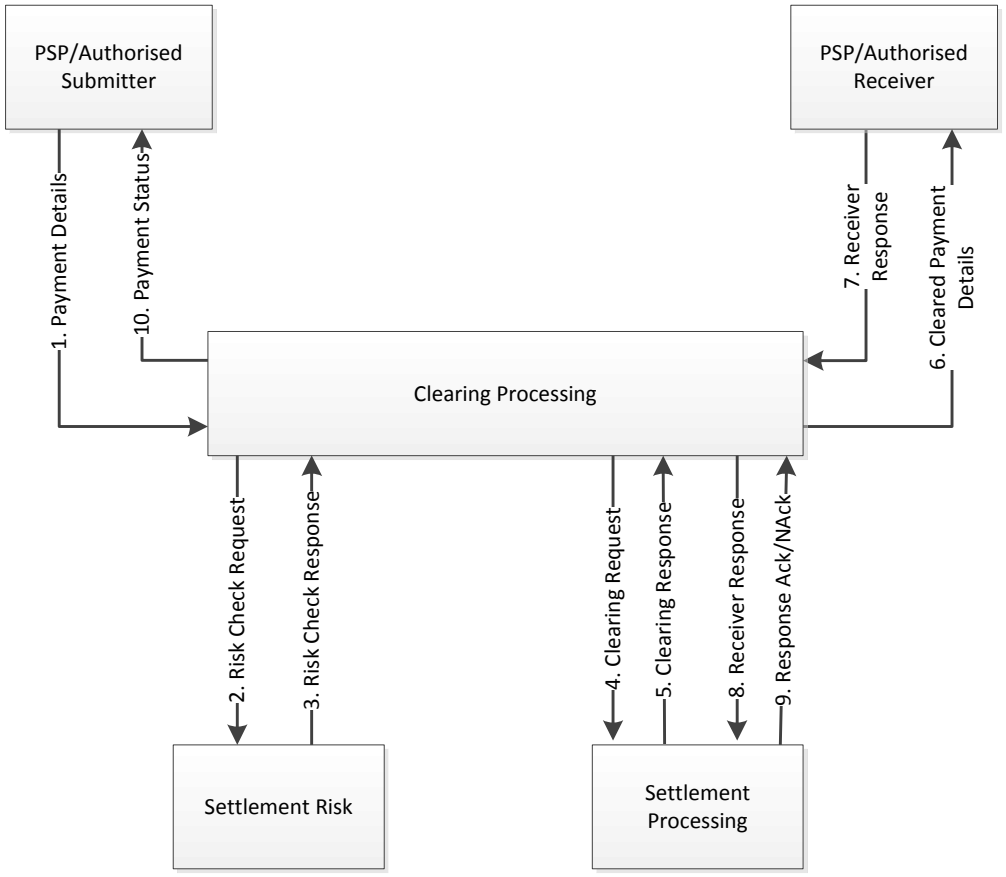


Figure 2.8 Clearing Processing

The following key features will be delivered by clearing processing:

- Receive single and bulk outbound payments from authorised submitters.
- Co-ordinate clearing of attended and unattended payments within specified SLAs:
    - Verify/authenticate file senders.
    - Check the integrity of the payment files.
    - Validate files.
    - Request settlement risk checks (Settlement Risk) and creation of settlement obligations (Settlement Processing).
    - Send cleared payments to receive PSPs (including signing and ensuring file integrity).
- Batching unattended cleared payments for receiving PSPs according to configurable criteria.
- Manage duplicate outbound payments/repeat messages.
- Retry or repeat sending bulk files where there is no response or acknowledgement.
- Receive or send acknowledgements (ACK) and negative-acknowledgements (NAK).
- Share payment transaction data with Financial Crime.
- Operational and regulatory reporting.

3. Settlement Risk Management

Initial analysis suggests a number of ways in which settlement risk positions for non-settling participants can be managed. The following is a viable model, but further analysis is required.

The settlement risk element is responsible for processing settlement risk checks from clearing processing. The primary function of Settlement Risk Management is to check that the transaction can settle by ensuring the clearing and settlement participants (PSPs / authorised submitters) are operating within their NSC.

NSCs will be maintained for settlement participants and non-settlement participants. Since single and bulk settlement cycles are likely to be different, separate NSCs for each will be managed by the NPSO.

4. Direct Non-Settling Participant

Clearing and settlement risk for non-settling participants will operate against an NSC which is owned and managed by their sponsor. Real-time authorisation by the sponsor will not be required. The sponsor's available balance must total the value of the sponsor's own available balance plus the aggregate value of all NSCs for sponsored non-settling participants. The direct non-settling participant's sponsor will need to be a direct settling participant.

5. Direct settling Participants

For Direct Settling participants, the accountability for clearing and settling will remain against their own NSC.

6. Indirect Non-Settling Participants

Indirect participants will be using their connected sponsor to submit their payments for clearing and settlement. Accountability for clearing and settling will remain against their sponsor's NSC.

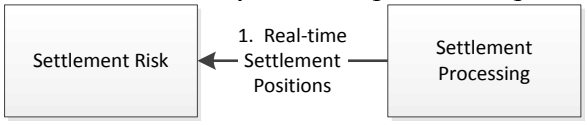


Figure 2.9 Settlement Risk Management

The following key features will be delivered by the settlement risk function:

- Receive and process settlement risk requests from attended and unattended clearing processing.
- Manage real-time NSC updates that are used in settlement risk checks.
- Manage the available balance in line with the clearing results.
- Check that transactions can settle.
- Maintain NSC thresholds and alerting settlement participants when thresholds are close to being breached.

7. Directory Look Up

The directory look-up is a function that looks up the master database to get the reference data necessary to make and route payments. Examples of reference data include Sort Code, Overlay level reference data, CASS account transfers and customer reference data, PSP and TPSP endpoints, roles and certificates.

2.1.7 Settlement Layer

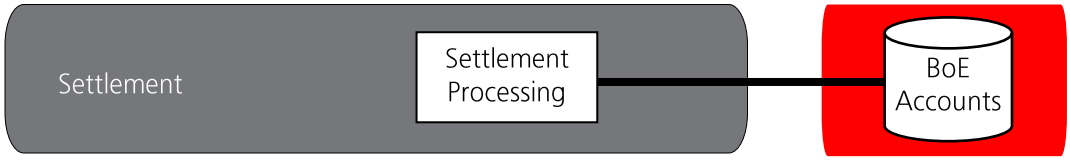


Figure 2.10 Settlement Layer

The Settlement layer is the single point of control for all payment instructions. It is where the actual movement of funds is finalised. It provides configurable settlement options with the BoE. Settlement processing's primary responsibility is to create settlement obligations for cleared transactions and to facilitate the settlement completion with the BoE according to configured cycles for particular payment types.

There is no concept of a failed settlement, only delayed completion of settlement. Prefunded collateralisation means settlement will always occur on cleared and accepted payments. The settlement completion may be delayed and forced manually, but it will always occur.

Two deployment options for settlement are outlined in Section 3 below.

Settlement Layer Components

1. Settlement Processing

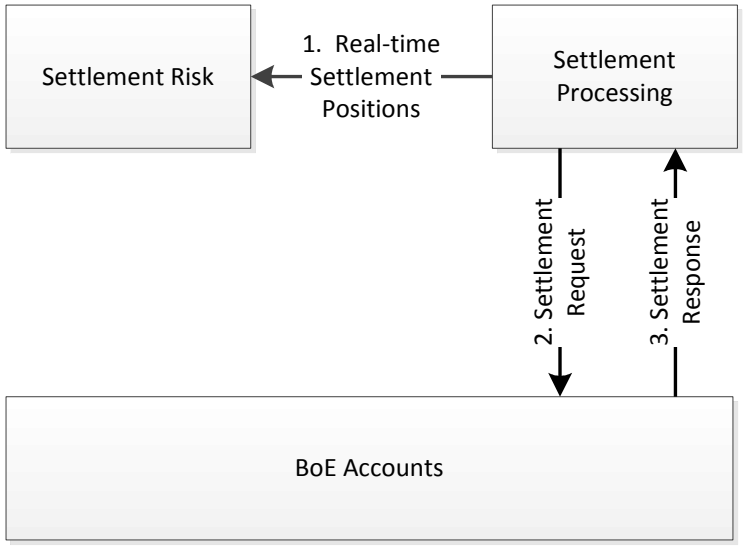


Figure 2.11 Settlement Processing

The primary responsibility of settlement processing is to create settlement obligations for cleared transactions and facilitate the settlement completion with the BoE according to configured settlement cycles for the payment types. The configuration of settlement cycles will allow settlement completion for attended and unattended payments to operate independently of each other.

The following key features will be delivered by settlement processing:

- Maintain the settlement position (create settlement obligations for cleared transactions) for settling participants separated by payment type (attended and unattended).
- Perform multilateral netting between settlement participants and initiate a settlement with the BoE according to configured settlement cycles for each payment type.
- Ensure that each directly settling participant cannot exceed their net sender position which includes their own NSC and that of any participants they sponsor. The net sender position must be collateralised via cash held in a Reserves Collateralisation Account (RCA) at the BoE.
- Operational and settlement participant reporting.

2. Bank of England Accounts

Within the BoE Accounts, the individual PSP RCA accounts are held to provide cash collateral that ensures that the multilateral settlement of cleared payments will take place by holding funds equal in value to the maximum net exposure of each PSP. Collateral will only be used in the event of a participant being unable to settle from their reserves/ settlement account.

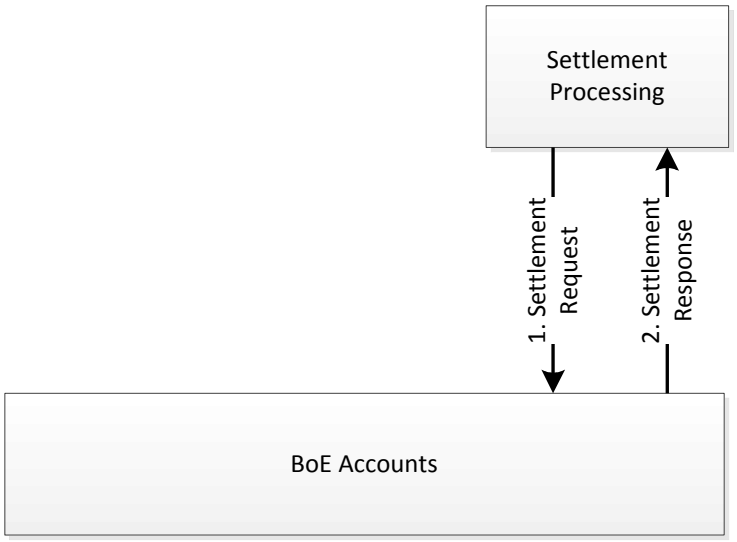


Figure 2.12 BoE Accounts

The BoE RTGS implementation supports a unified settlement approach across all attended and unattended payment types. A single minimum available balance will be available for each participant for all their payment types. The minimum available balance will be the overall default NSC for each participant.

The NPSO will have responsibility for allocating the overall NSC to the payment types. When additional available funds are made available, the NPSO can adjust the NSC for each payment type accordingly. The settlement participant is responsible for determining the overall NSC and allocating it between its sponsored non-settlement participants.

The following key features of the BoE's RTGS system will be required:

- Manage a single liquidity position and available balance for all payment types.
- Support the interoperability of the NPA with the existing payment schemes during the transition.
- Manage adjustments in available funds and changes to available balance (increase or decrease) and making these available in real-time to the NPSO.
- Processing multilateral settlement requests according to NPA configured cycles in settlement processing.

2.1.8 Network Connectivity Layer

The Network Connectivity Layer will provide the networking infrastructure to access the NPA. To maintain security integrity, it is expected that participants accessing the NPA will conform to industry best practice and adhere to the network authentication, security requirements and specifications to be defined by the NPSO.

Connectivity between the layers and components will be open to multi-vendor competition and will not be tied to a single provider or a particular network element in order to ensure that competition is enabled and vendor 'stickiness' reduced.

Network Principles

A number of principles have been established that will inform the network design, security model and NPA responsibility. These are:-

- Security and network requirements can be different for each layer.
- There should be a common operational standard for all connections.
- There should be a common technology standard for all connections such that multiple network providers are able to fulfil the requirements and can provide a service in this space.

Network Technology

Channels: The NPA should support both public and private channel connections such as Private Multi-Protocol Label Switching (MPLS Cloud) and the public internet.

Authentication: Mutual authentication of both the source and destination will be required. The recommendation is to use Transport Layer Security (TLS) and carry out authentication using Public-key Cryptography.

Network Aggregation: The use of network aggregation technology to provide a common connection to clearing.

Network Resilience: The external networks to NPA must provide resilience against network failures. The network must be capable of detecting a failure and be able to recover services in an efficient manner to agreed SLAs, ideally without services being disconnected. Network architectures are complex and therefore sophisticated resilience mechanisms will be required and should include best practice system design techniques such as an active/ active standby design. The network topology must allow for the re-routing of traffic in the case of a failure without affecting the service. The following are high-level network requirements for NPA:-

- The network will be required to operate and have availability as defined by the NPSO.
- Implementation will conform to industry best practice as a minimum to ensure the appropriate resilience and availability levels.
- Network components must have resilience as the core architecture, i.e. dual components, dual circuits.
- Quality of Service (QoS) will be required to provide priority where required for NPA.
- Redundancy options must be considered, i.e. switches, active/active routers.

The extent of how levels of network resilience will vary by layer, service or component is expected to be a matter for the NPSO to determine. As an example, the clearing and settlement layer network interfaces would be expected to have a higher network resilience than a PSU accessing their PSP account via a mobile network.

Design Principles

The network layer should support the following design principles:

- There should be a clear abstraction of the connectivity from clearing layer
- There should be a single defined interface with clearing layer

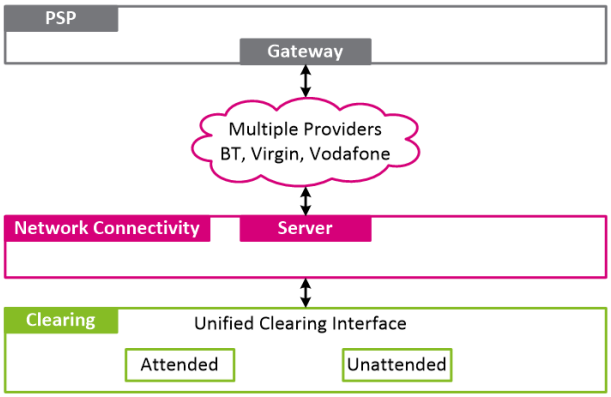


Figure 2.13 Multi-Vendor Deployment Approach - Network Layer

2.1.9 Supporting Components: Master Directory and Financial Crime Analytics

Two further components that sit outside of the layered architecture are the interface to Financial Crime and the master directory. These elements are described below:-

Directory services

Directory services are an essential feature of the NPA architecture which enables participant access to API services and reference data. NPA will require access to a number of data sets to perform front office functions, transact a payment, and perform back office functions. Access to these data sets will potentially be required through all levels of the NPA architecture.

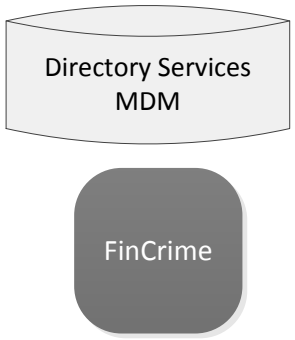


Figure 2.14 Directory and Financial Crime Components

There is no single architectural component that comprises the directory services; rather it is best to consider it a sub-system of interacting components. The directory will need to provide a number of functional capabilities such as participant enrolment, identity access management and will also be a certificate authority.

The directory will provide essential reference data to support payment initiation and execution. These datasets will need to be mastered and governed. The proposal is that the function of Master Data Management is a centralised function controlled, administered and governed by the NPSO. It is envisaged that access to data within the directory will be available at all layers between the end-user overlay services and settlement layers. This is central to the enablement of greater competition in the payments systems market. The requirements for directory services is split between functional and data services.

Directory services is a critical element of the NPA and will be subject to high availability requirements and resilience levels. Consideration must be given to ensure data availability using industry best practice, including data replication and active-active deployment configurations.

Directory Services Functionality

Functionally directory services will provide the following capabilities:-

1. Participant enrolment
   Participants will be set-up and configured in the NPA based on their role(s) in payment processing. This will enable participants to be assigned access to services that they require to process payments, i.e. APIs, reference data.

2. Identity Access Management (IAM)
   IAM is an industry-wide term for the security and business process that allows access to the right services, to the right people, at the right time. We recognise that IAM is a key security feature of the NPA and will be an integral component to meet the necessary regulatory obligations.

3. Certificate Authority (CA)
   The CA function provides the digital signature capability for authentication and validation events in the NPA. The scope and extent of these will evolve as the detailed security proposition is realised.

Directory Services Data Sets

The NPA will require a number of data sets to support payment initiation and execution. These data sets are indicatively grouped as follows;

1. Enrollment data
   Enrollment data will be the information that the NPA requires to know about a participant in order for them to safely and securely undertake the processing of payments. The data will enable the correct access management to be applied to the participant for example.

2. Routing data
   Participants will require the latest available sort code and account data to route a payment correctly to its ultimate destination participant. This will encompass relevant schemes or industry-wide processes that switch or move customers to a new sort code and/or account.

3. Reference data
   NPA reference data covers those aspects where a data lookup is required. This will include items such as settlement configuration parameters, system calendars and code descriptions.

An assessment of the Open Banking directory service indicates that it can meet the requirements of the different roles and layers within the NPA, such as supporting the delivery of the key functions of participant registration, identity access management and security authentication. As a result, it is recommended that consideration is given to adopting Open Banking directory services, once it is clear how it will support all the potential users of the directory (and not just the nine PSPs initially mandated by the CMA to implement Open Banking).[2] If an alternative directory services supplier is chosen, the NPA will support this requirement from an architectural design perspective.

Directory Services Deployment Options

The deployment options (e.g. centralised vs. distributed, replication vs. look-up) for the directory services will be subject to a number of technical and commercial considerations and it is recommended that these are further reviewed in the post-consultation feedback. There are a number of deployment models that can be used for the data sets in order to facilitate competition in the market for the management and distribution of directory services. The examples below are not exhaustive but provide a view that is useful when considering the options.

1. Centralised Directory Service

This model supports 'for the market' competition with a centralised vendor, or vendors, managing the physical hosting of the data centrally. Data is accessed, via APIs, by authorised participants through all layers of the NPA. Master Data Management is controlled centrally.

[2] See Glossary.

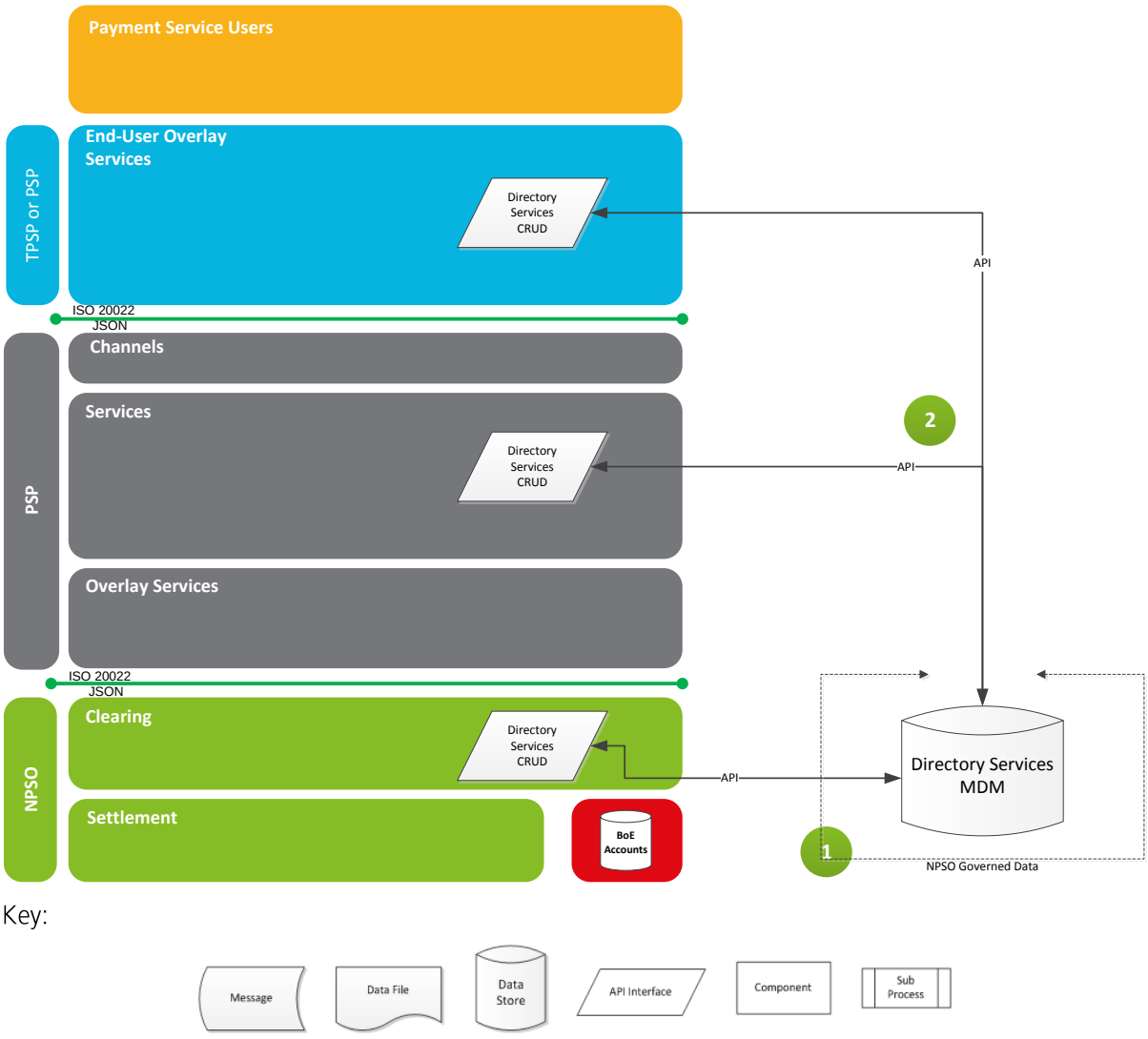
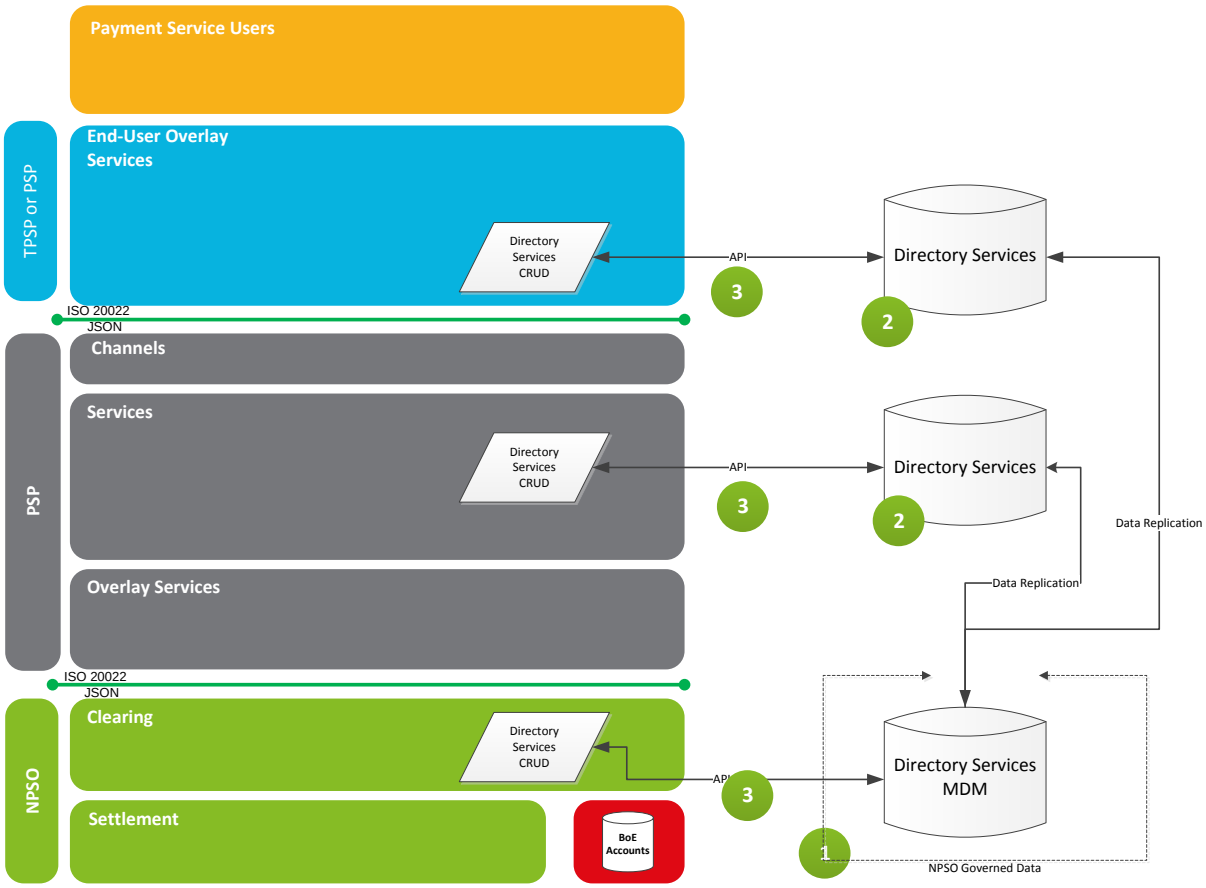


Figure 2.15 *Centralised* Directory Service

1. Data is mastered by the NPSO (or authorised vendor). Data is managed in the central database.
2. Authorised users of the data utilise the data via direct lookup APIs.

2. Distributed Directory Service

This model provides competition 'for and in the market'. The option to commercially package data and allow participants to obtain this data directly from vendors is supported. The governance overhead is increased and SLA enforcement would be required to ensure the most up to date data is available. Data access would be via a participant/vendor relationship. Master Data Management is controlled centrally.



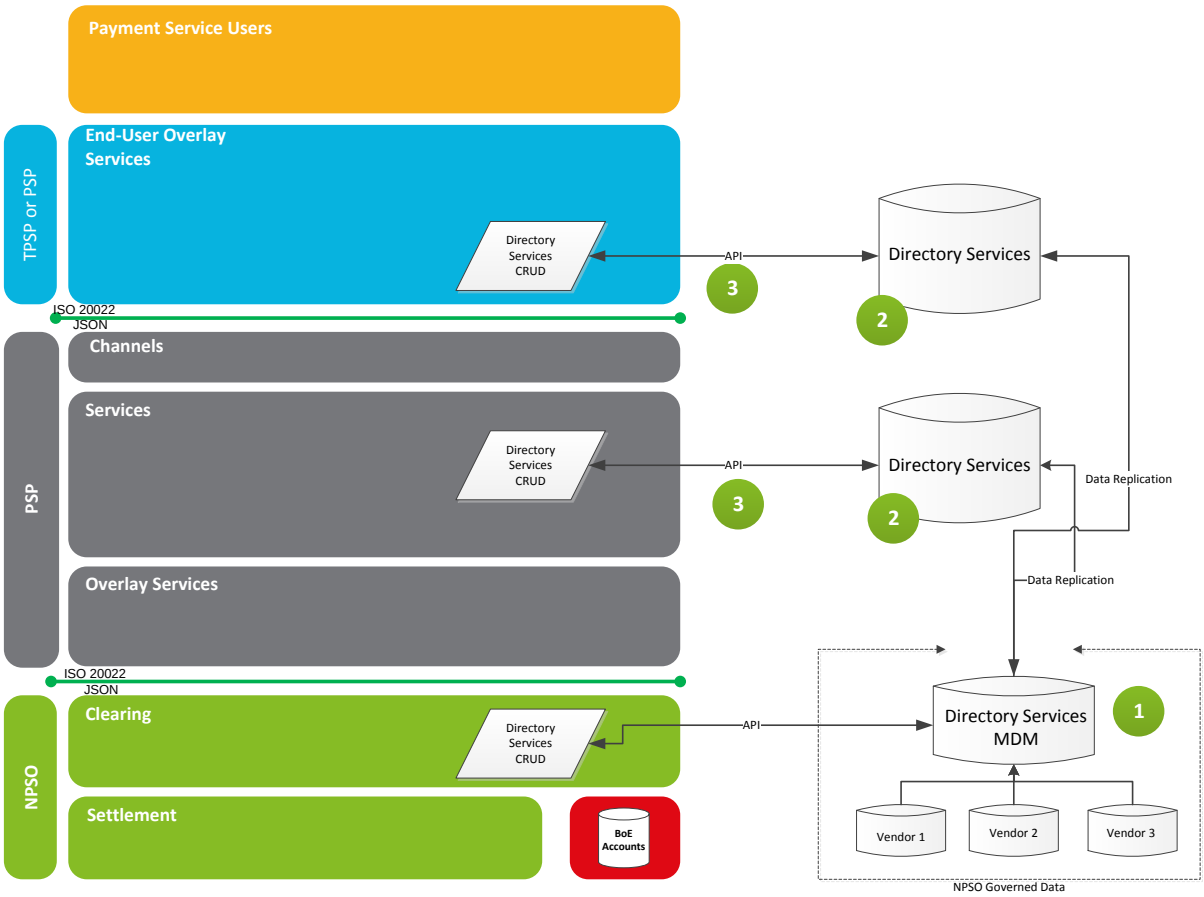
Key:

Figure 2.16 Distributed Directory Service

1. Data is mastered by the NPSO (or authorised vendor). Data is managed in the central database
2. Data is replicated to locally managed databases. This would be subject to commercial agreements between the NPSO and the vendor(s)
3. Authorised users of the data utilise the data via lookup APIs.

Multi-Vendor Directory Service

This model provides competition 'for the market' and 'in the market'. It provides the option to commercially package data and allow participants to obtain this data directly from vendors. The governance overhead is further increased and SLAs enforcement would be required to ensure the most up to date data is available. Data access would be a participant/vendor relationship. Master Data Management is controlled centrally but would be more complex as the number of central vendors increase.



Key:

Figure 2.17 Multi-Vendor Directory Service

1. Data is mastered by the NPSO (or authorised vendor). Multiple vendors provide the data
2. Data is replicated to locally managed databases. This would be a subject to commercial agreements between the NPSO and the vendor(s)
3. Authorised users of the data utilise the data via lookup APIs.

Financial Crime Analytics

A real-time feed of transaction information from the NPA clearing layer, in keeping with prevailing data protection laws, will be provided to the Financial Crime payments transaction data analytics capability. It is recommended that requirements for this data feed capability are further developed following the consultation period and once feedback has been obtained on the proposed clearing and settlement approaches.

2.2 Standards and Interfaces

The NPA uses a layered architecture. This section focuses on how the layers[3] would interact with each other. Data exchanged between layers will be based on the ISO 20022 standards. NPSO will define the services each layer has to expose and the associated SLA for them. Participants will have to make sure they meet the specification by going through required accreditation processes and will be continuously monitored by NPSO to meet service standards.

The NPA does not constrain the layers a particular market participant wants to operate in or how they deploy those layers. For example, a PSP that services customers' accounts can offer TPSP services such as account aggregation and payment initiation but would still need to have their account holding PSP layer exposed through the API gateway for another authorised TPSP to access its services.

2.2.1 ISO 20022 and JSON

The ISO 20022 messaging standard will be used for payment messages sent from the TPSP and the PSP layers, through to the clearing and settlement layers.

We are not mandating the use of ISO 20022 messaging standards between the participants in the End-User Overlay Services Layer or between the Customer (PSU) and the End-User Overlay Services Layer. We recognise, however, that a level of API definition may be required for certain core end-user services (such as Request to Pay and Confirmation of Payee) to enable interoperability, and therefore increased competition, between different service providers. It is envisaged that ISO 20022 would be the message standard adopted for any additions the NPA API catalogue. Furthermore, non-direct settling PSPs should be provided with ISO 20022 access to the NPA should they wish to obtain the benefits of using it, though using ISO 20022 would not be mandated for this category of participant.

The NPA will adopt a design approach that encompasses the following areas:-

- The NPA will implement end-to-end interoperability using the ISO 20022 messaging standard.
- ISO provides a catalogue of financial messages that will be utilised for the NPA end-to-end messaging flows.
- NPA messaging will deliver a positive response to all payment messages.

Detailed analysis of the ISO message catalogue will be required to determine which message definitions will form the message flows for NPA. Indicatively, the following have been identified:

- pacs - Payment Clearing and Settlement.
- pain - Payments Initiation.

The NPA requires that the status of a payment request is known throughout the payment processing lifecycle. To achieve this, the NPA will utilise ACK/NAK (Acknowledged/Not Acknowledged) messages. These are defined in ISO 20022 message definitions as;

- pain - Payments Initiation - pain.002.001.08 CustomerPaymentStatusReport
- pacs – Payments Clearing and Settlement – pacs.002.001.08 FIToFIPaymentsStatusReport

ACK/NAK will be utilised to provide a positive response regarding the acceptance or otherwise of a payment message for processing by the receiving participant. ACK/NAK are not used to indicate the successful transport of the payment file from point to point, this will be the responsibility of the managed file transfer software that will manage the secure transfer of data.

JSON - Post Consultation Update

In V1.0 of this document, it was proposed that JavaScript Object Notation (JSON) be used to provide the ISO 20022 data representations for the NPA. It was noted that JSON is a lightweight data interchange format and has been selected by the Open Banking Working Group for its ISO 20022 data representation and that the delivery of the NPA is not dependent on the use of JSON. At the time of writing, the use of

[3] Layers represent the roles and their associated capabilities provided. This allows the market to evolve and innovate based on the market needs.

JSON is dependent upon ratification of JSON encoding for ISO 20022 messages by the Registration Management Group (RMG).

Following further analysis, it is now being recommended that business requirements and models should be defined as the first stage in the decision-making process and as a result, there is no need to make a decision on XML and/ or JSON for the NPA at this stage. The decision-making process is consequently expected to be conducted by the NPSO during 2018.

Both XML and JSON can be used to represent the data required by the NPAs adoption of ISO 20022; however, there are some differences in the style of representation. Further considerations before concluding which option should be selected (see Appendix 2 for a potential set of options) are:-

- JSON is becoming more popular for FinTechs, however, there are large payment submitters that utilise XML (e.g. in the PSU and TPSP layers).
- Engaging a wider group of stakeholders (including the vendor community) will help to make an informed decision.
- Consideration should be given to how the choice(s) impact system roll-over (to CHAPS for example) in case of an NPA outage.
- Understanding the BoEs RTGS plans with regards to interoperability. The BoE has taken the decision to use XML for its ISO 20022 standard and this may impact decisions made.

It should be noted that the range of options include binary options (e.g. either JSON or XML) or blended approaches (e.g. the selection of data syntax option could be layer based).

2.2.2 APIs

Since the publication of the "Blueprint for the future of UK payments" in July 2017 further work has been undertaken to explore some of the potential APIs that may be required to enable the NPA to support open access and increased competition whilst protecting system integrity and resilience.

Appendix 3 provides an overview of the potential payment flows, API's and messages that are required to support the NPA design published in the July consultation documents. In doing this work it is recognised that there are a number of areas that will require further assessment, which may impact requirements and the final API catalogue. The areas identified for further investigation include settling the final design and architecture for Direct Debit and Credit processing and the re-direction of switched accounts.

The NPA design supports third-party payment service providers (TPSPs) playing an active role in NPA including those TPSPs acting as an AISP (Account Information Service Provider) or PISP (Payment Initiation Service provider). In addition to these roles, it is expected that third party service providers, likely to be accredited by the NPSO, could also provide further functions such as Request to Pay and Enhanced Data.

3 Clearing and Settlement

3.1 Background

In this blueprint, we have identified two main approaches to clearing and settlement, centralised and distributed. We have since performed further analysis of these two options to determine our preferred approach that must align with the following:

- The relevant capability within the BoE RTGS system.
- Settlement taking place in central bank money.
- Funds being available to ensure that settlement can complete.
- The ability to support:
    - Cap adjustments in real-time.
    - Flexible settlement options as agreed between the NPSO and the BoE.
    - Both attended (single) and unattended (bulk) payment types.
    - 24x7 clearing.
    - Settlement in line with BoE's RTGS.

The NPSO will apply to the BoE for NPA cap arrangements that are compliant with the BoE's settlement finality requirements.

Within the centralised and distributed clearing and settlement approaches, five options were identified. A summary of the evaluation has been provided below. The detailed analysis can be found in Appendix 4. Following our further analysis and feedback received through the consultation process, it remains our recommendation that a centralised model would provide the best solution for the NPA. The following criteria were used in suggesting a recommended approach to settlement and clearing.

Consideration	Description
Align to BoE RTGS system	The settlement risk model for NPA must be aligned to the relevant functionality within the BoE's RTGS system. The settlement model should be liquidity efficient for participants, without jeopardising settlement finality and Committee on Payments and Markets Infrastructure – International Organisation of Securities Commission (CPMI-IOSCO) principles (the optimal model using 1 or 2 accounts, is yet to be assessed along with the approaches being adopted in the US and Europe).
Settle in BoE money	A key requirement for NPA is that settlement must be completed using BoE money.
Increased funding available in real-time	Participants should be able to adjust the value of funds earmarked against NSCs as close to near real-time as practicable possible with minimal manual steps.
Flexible Settlement	Setting multiple settlement cycles by payment type must be supported unless continuous settlement is employed.
Attended (single) and unattended (bulk) payments	Settlement of attended and unattended payments must be supported, ideally via reference to a single risk position per participant. The exact model is subject to the unattended platform decision. Provision of a single common interface to the new RTGS platform.
24x7	The target architecture must enable real-time 24x7 settlement risk checking and periodic settlement output to the BoE.
Reversals and Returns	Must allow reversals and returns to be processed.

	Notification of payment status must be delivered to the involved participants so that the participant host system can be updated.

Table 3.1 Clearing and Settlement Criteria

The bilateral messaging options 3-5 that were analysed are shown in Appendix 4. These options were discarded on the grounds that, in the view of industry stakeholders, these options introduced unacceptable levels of risk. Details of the shortlisted options 1 and 2 are provided below.

3.1.1 Option 1: Centralised Model Overview

In the centralised model, the routing, settlement risk and settlement processing is managed centrally. The central clearing node will be responsible for the routing and clearing of payments. Participants do not need to exchange payment messages directly with each other.

Figure 3.1 below shows how the centralised model is intended to operate between individual PSPs and the central clearing node.

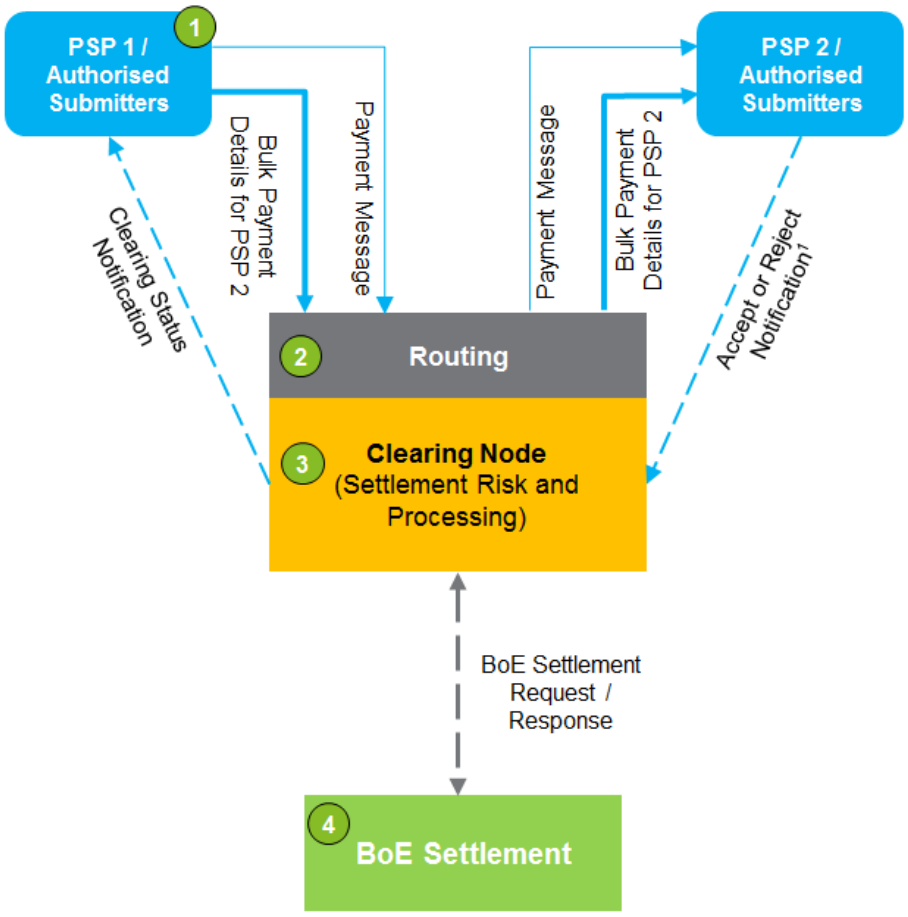


Figure 3.1 Centralised Model

All payment messages are routed via central participant messaging.

1. PSPs participating in a payment send payment messages to a central clearing node.
2. The routing is responsible for:
    - Receipt of payment message(s).
    - Routing of messages.
    - Relay of payment messages to other PSPs.
    - Clearing status notifications.
3. The clearing node is responsible for:
    - Maintenance and checking of the participating PSP's settlement risk position.
    - Creating settlement risk positions for cleared payments.
4. BoE settlement initiates settlement according to configured cycles.

The centralised clearing and settlement model is recommended, and has been broadly supported through consultation feedback, for the following reasons:-

- The centralised option provides a clear and manageable risk model that aligns the routing with the settlement risk.
- The reconciliation of transactions between participants is simplified compared with the peer-to-peer routing used in option 2.
- Systemic risk of participant failures is mitigated by insulating them from each other and provides consistent and accurate settlement information in real-time.
- This model is expected to provide lower overall cost and risk to the industry as the centre will handle the routing complexity.
- Operationally the governance and control are more efficient with a single point of contact for support.
- This model also offers a simpler mechanism to address a large number of direct submitters without requiring them to integrate with a registry/database before submitting payments.

3.1.2 Option 2: Distributed Model Overview

The distributed model (peer-to-peer participant messaging with centralised risk and settlement management) requires the participants to exchange payment messages with each other, with the sender accountable for ensuring settlement via a common settlement risk and settlement processing service (clearing node). The clearing node validates that the sending participant is operating within its NSC and adjusts the settlement positions for the cleared transactions.

Figure 3.2 below shows how the distributed model is intended to operate between individual PSPs and the clearing node.

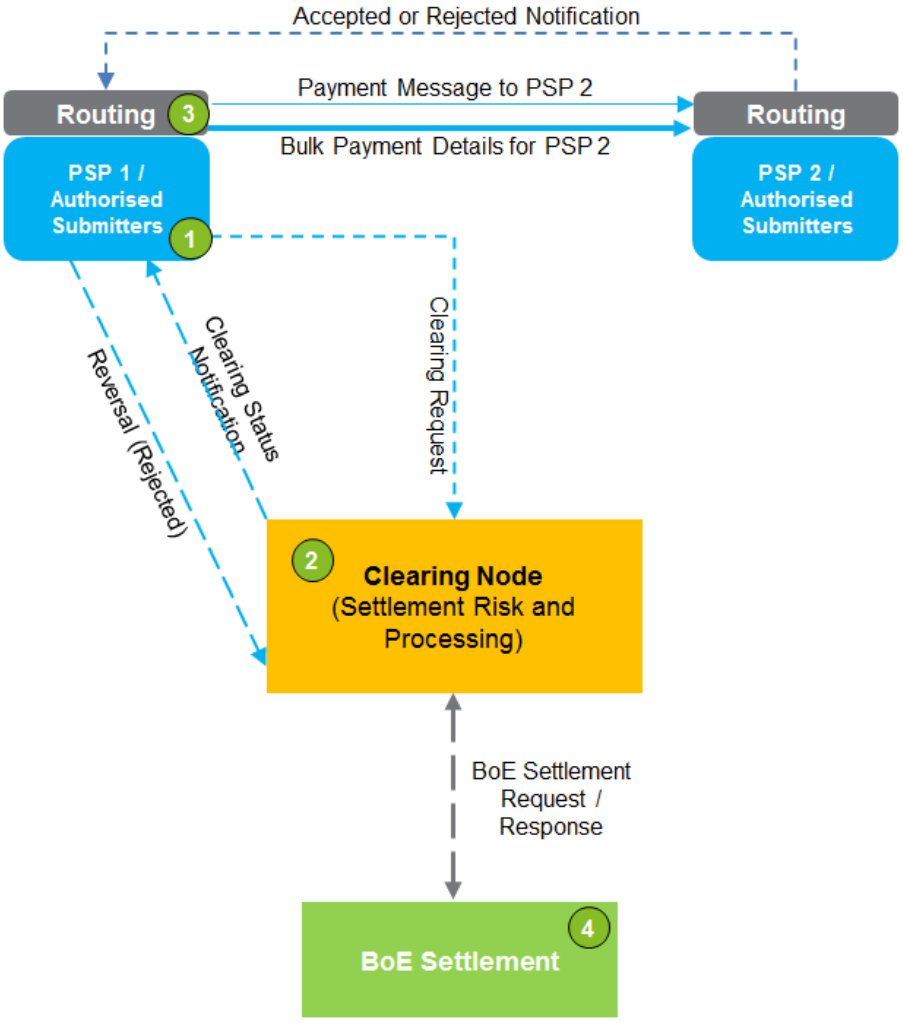


Figure 3.2 Distributed Model

Similar to centralised, the sender PSP initiates clearing and settlement but, each PSP will check redirection and separate files by receiving PSPs. This is unlike centralised where routing is centralised.

1. The PSP sending the payment (PSP 1) sends a clearing request to the clearing node.
2. The clearing node is responsible for:
   - Checking the risk position.
   - Creating a settlement obligation.
   - Sending a clearing status (with token) notification to the sender.
3. The sending PSP (PSP 1) sends cleared payments to the receiver (with a token) and the receiver (PSP 2) sends a response notification to the sender (PSP 1) - Accept or Reject.
4. BoE settlement initiates settlement according to configured cycles.

The distributed model was the next best option after Option 1. Following are the primary reasons for this option not being recommended.

- The distributed option was seen as adding costs and technical complexity to PSPs (routing) without demonstrable benefit to customers or the organisations themselves. It introduces a risk of PSPs not following message protocol and debiting/crediting accounts without confirmation of settlement. Additional message complexity is also added to manage receiver rejected payments.
- Although peer-to-peer routing creates a competitive market for technology, it adds significant complexity for PSPs. There is no evidence that suggests peer-to-peer routing is a key driver for a

competitive payments landscape. However, it does suggest that complexity is potentially increased for PSPs and therefore is more likely to discourage competition.

- Coordination of change will be complex with Option 2 and more controls will be needed to implement and mitigate cyber risk
- The distributed model does potentially offer more flexibility to scale with the addition of new PSPs, but this was outweighed by the challenges of certifying new PSP's and ensuring that they deliver a service that is fit for purpose.

3.1.3 Centralised and Distributed Models Comparison Summary

The pros and cons of each approach are summarised in below:

Approach	Pros	Cons
Centralised	• Multiple vendors can bid for each of the central components. • Provides a clear and manageable risk model that aligns the routing with settlement risk management. • Reconciliation of transactions between participants is simplified compared with the distributed model. • The insulating nature of the layered concept mitigates systemic risks associated with individual participant failures. • Provides consistent and accurate settlement information in real-time. • Expected to result in lower overall costs and risk to the payments industry as the centre will handle the routing complexity. • Expected to support greater levels of innovation through the reduction in PSP integration and management complexity compared to a peer-to-peer clearing approach. • Operational management, governance and control are more efficient with a single point of contact for support. • Offers a simpler mechanism for direct (payment) submitters as it does not require them to carry out directory look-ups before to route payments.	• Competition in the clearing and settlement layers will be 'for the market' only. • Precludes third-party from offering their own settlement routing services to individual PSPs. • Potentially exposes to participants to higher costs for routing since there may be fewer options to seek competitive pricing.
Distributed	• For routing, each PSP can scale to its required volumes, which introduces flexibility and makes the model commercially competitive. • Multiple suppliers can compete for providing routing services encouraging competitive pricing.	• Requires specific message flow implementation to enforce the requirement of the receiver only receiving cleared and settled payments. • Stakeholders saw the opening up of the clearing layer as adding to technical complexity and cost for PSPs (e.g. clearing message routing) without demonstrable benefit to customers or the organisations themselves. • Introduces a risk of PSPs not following message protocol and

Approach	Pros	Cons
		debiting/crediting accounts without confirmation of settlement. • Coordination of change was also considered to be more complex with this option since more controls would be needed to implement and mitigate cyber risk.

Table 3.2 Summary Centralised vs. Distributed Model Pros and Cons

Based on the analysis above, we believe that the centralised model is the best approach for the NPA.

3.2 Clearing and Settlement Deployment Models

The clearing and settlement model can be deployed as either a single or multi-vendor approach. The design of the NPA caters for both approaches. The NPSO will decide which approach to implemente and will facilitate the corresponding procurement process.

3.2.1 Single Vendor Deployment Approach

A single vendor deployment approach is one where a single vendor (node) provides settlement risk and settlement processing for attended and unattended payment types.

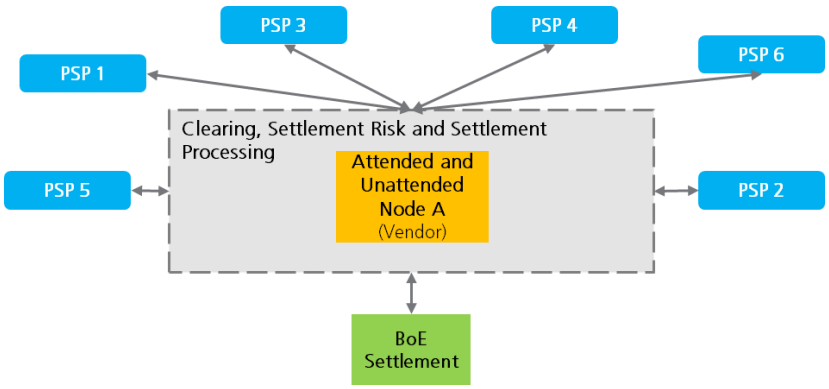


Figure 3.3 Single Vendor Deployment Approach

The single vendor option supports participant liquidity efficiency through the use of a single participant debit cap and multilateral netting between each participant for all their payment types. Simplified reconciliation and reporting are achieved with fewer settlement requests being sent to the BoE compared to the multi-vendor approach. Other advantages include the effective oversight and management by the NPSO ensuring simplicity, consistency and standardisation in the service and operational models.

However, reliance on a single vendor could make the migration to an alternative supplier for extended capacity (payment handling or PSP onboarding) or new services technically and commercially more challenging. The use of ISO 20022 along with the adoption of the layered model of the NPA and contract structure could be used to materially mitigate against these risks.

Opportunities

A single vendor approach presents the following opportunities:

- Less technical complexity – No sharing of data in real-time between multiple nodes to provide a single risk position for each participant or alignment of settlement cycles between nodes,
- Simplified reconciliation and reporting.

- Fewer settlement requests to the BoE than the multivendor approach.
- Allows for consistent and standardised service models.
- Introduces a single point of contact for operational issues.
- Allows efficient oversight by the NPSO.
- Maximising volume with a single vendor has potential to realise a lower unit cost per transaction.

Considerations

The following must be considered when choosing a single vendor approach:

- Reliant on a single vendor for scaling in line with increased demand.
- Migration to an alternative supplier in event of contractual issues may require retendering.
- No opportunities to direct traffic by market needs and provides no provisions for failure (node/vendor failure/downtime).
- Reliant on a single vendor to accommodate changes – may present resourcing constraints.
- PSPs are reliant on a single vendor for servicing all PSPs (onboarding and support).
- May lead to reduced negotiating power if there is a single vendor which could be mitigated by contract and break clauses.
- Limited opportunities to reduce transition risk among future vendors.

3.2.2 Multi-Vendor Deployment Approach

A multi-vendor deployment approach is one where clearing would be provided by different vendors (nodes). This can be one node per PSP – akin to the SEPA model or one node per payment type (e.g. attended or unattended). The per payment type multi-vendor approach is expected to offer advantages over the per PSP approach. It is expected to offer more flexible settlement options, enable the automation of cap management and support the ability to deliver new innovative payment services independently of the clearing and settlement layers, as well as allow for the delivery of new payment types with minimal disruption.

Opportunities also exist to provide a more sophisticated cap management approach in the future where nodes exchange data in real-time to enable dynamic debit cap adjustments according to the settling position of each node.

Based on stakeholder feedback, the option to assign a single clearing node to each payment type was considered to provide a good balance between technical implementation challenges and the enablement of competition for the market.

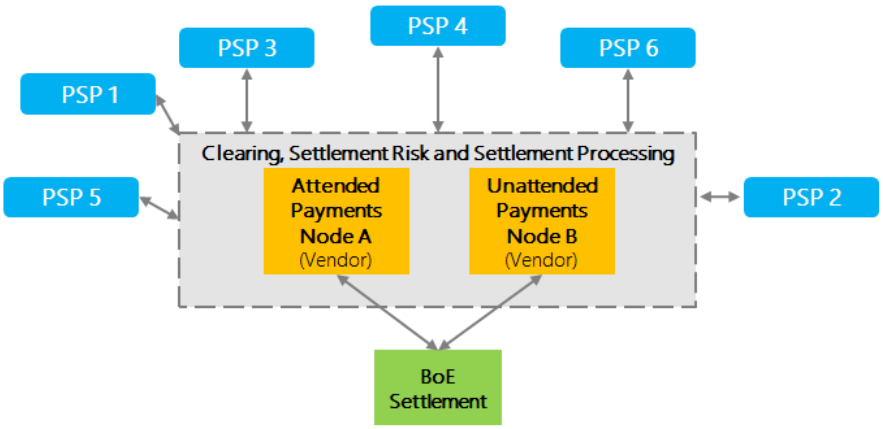


Figure 3.4 Multi-Vendor Deployment Approach

In this approach, it is envisaged that the NPSO would be responsible for managing an overall agreed NSC (i.e. the available balance) position for each participant and then allocating a debit cap for each of the clearing nodes. The settlement participant is responsible for determining the overall NSC and allocating it

between its sponsored non-settlement participants. To achieve optimal liquidity efficiencies with the multi-vendor approach, the economic and operational aspects of the settlement and clearing layers requires consideration.

The NPSO is also expected to be able to re-allocate debit caps for participants between the clearing nodes as long as the aggregate debit cap across all nodes remains within the participant's agreed NSC (available balance) position with the BoE.

The multi-vendor option is considered to be more challenging from an NPSO management perspective (e.g. cap allocation) as it requires a degree of technical inter-operation and management that is not required for the single vendor model.

Opportunities

A multivendor approach presents the following opportunities:

- Increased flexibility to scale – nodes can scale independently for increased demand.
- Traffic can be directed based on market needs – traffic separated by capabilities (e.g. unattended vs. attended, volumes, payment types etc.).
- Provisions for failure – simplified redirection in case of a node, vendor failure or downtime.
- Potential to accelerate changes/enhancements – one vendor may be able to deliver changes faster than the other.
- The potential for stronger negotiating power.
- Reduced transition risk (once model deployed).
- Simplified integration and migration to new master nodes.

Considerations

The following should be considered when choosing a multi-vendor approach:

- Operational (NPSO oversight) and technical (vendor communication) management is potentially more complex.
- Load balancing will need to be implemented across vendors.
- Nodes will need to share limited data in real-time to provide a single risk position for each participant.
- Settlement cycles need to be aligned.
- Reconciliation and reporting will be more complex.
- Each master node will (one for each PSP/Master Node) submit its own settlement requests to the BoE – it will need to process requests within the settlement cycle time window (each request may affect the same account).
- Less traffic per vendor may lead to a higher unit cost.

Design Principles

The following design principles should be considered when designing and implementing the NPA. It is recognised that it will be the NPSO's decision on how to deploy a clearing and settlement layer that meets its users' requirements whilst demonstrating that appropriate levels of competition have been achieved.

- There should be a unified clearing approach for both attended and unattended. (Reusable)
- Enable several vendor instances to operate concurrently without interference between them. (Concurrency Transparency)
- Enable multiple instances of the same vendor to be used to increase reliability and performance. (Replication Transparency)
- Allow the system and applications to expand in scale without change to the system structure or the application algorithms. (Scaling Transparency)
- Provide support for a common connection model covering attended and unattended.

4 Key Use Case Scenarios

The following use cases illustrate how the NPA will support some of the key payment scenarios. It should be noted that the supplementary document does not intend to cover every possible payment scenario, nor do we suggest the proposed solution is the only way for delivering the payment that is being described.

4.1 Direct Debit Payments

Direct Debits are a product offered by Bacs Payment Schemes Ltd (BPSL) that allows organisations to collect payments from their customers' accounts once a Direct Debit Instruction (DDI) has been authorised by the customer and lodged with their PSP. Organisations that use the existing Bacs Direct Debit payment system will still require the ability to automatically collect a payment from their customer's nominated account.

Under the NPA, the Direct Debit payment will continue, as today, to be initiated by the payee (Payment Service User). The Payment Service User (PSU) will still be responsible for providing the customer with a Direct Debit Instruction (DDI) to authorise the Direct Debit payment made by the customer's PSP on behalf of the PSU. When the DDI has been lodged with the customer's PSP, the PSU will continue to generate the Direct Debit collection file for payment to be made on a predetermined due date.

The PSU will still require a Direct Debit Submitter to transmit the DDI information and Direct Debit payment instructions to the customer's PSP. The PSU can submit directly using their existing approved software or indirectly through an existing bureau.

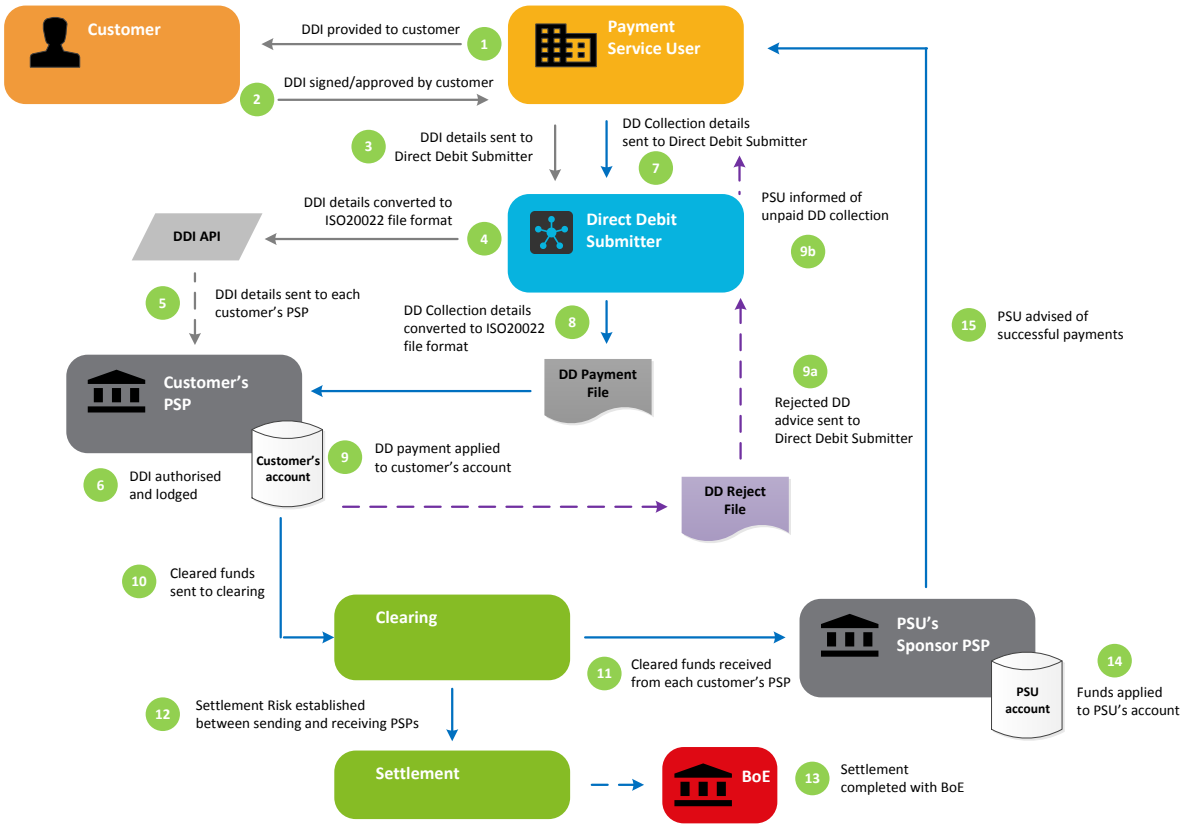
The customer's PSP will receive DDI requests from a Direct Debit Submitter. DDI requests will be submitted via a new DDI API. The customer's PSP will continue to set up the Direct Debit payment on the customer's account. Where an e-mandate has been generated it will be possible to use strong customer authentication to prevent fraudulent abuse where an electronic signature is required.

The PSP will continue to receive a Direct Debit payment request from the PSU via their Direct Debit Submitter. The PSP will execute the Direct Debit request on the payment due date and apply the payment to the customer's account. In a change from how the process works today, only cleared funds will be sent to the Clearing layer. As such, any payments that could not be applied to the customer's account will be returned to the PSU as an advice of non-payment and will not be sent to the Clearing layer.

PSUs will see a change in that they will only receive cleared funds into their account on the payment due date. Unpaid Direct Debits will no longer be reversed from the PSU's account post-settlement (as per the existing Bacs process). The PSU will be notified of any rejected payments and therefore cash flow can be accurately represented at the end of the day on the payment due date.

The NPSO will continue to perform a central role in maintaining, monitoring and facilitating settlement between the sending and receiving PSP. The NPSO will also have responsibility for the governance and compliance of the NPA layers over which Direct Debit services may run.

Under our proposed NPA, a Third Party Payment Service Provider (TPSP) may have the opportunity to provide mandate management services and Direct Debit collection services. The TPSP will be expected to be governed and be compliant with the Direct Debit scheme rules set by the NPSO.



Key:

Figure 4.1 NPA Direct Debit Overview

Process Steps

Onboarding

Step 1: The customer has agreed with the PSU to make payments via a Direct Debit arrangement. The PSU provides a Direct Debit Instruction (mandate) for the customer to complete. A customer's signature or electronic consent will be required.

Step 2: The customer returns the completed Direct Debit Instruction (DDI) to the PSU.

Direct Debit Instruction Set up

Step 3: The PSU sends the DDI to a Direct Debit Submitter e.g. their existing bureau, sponsor bank or a new third party providing a mandate management service. Note: the PSU could also continue to use their existing Bacs software to process the DDI.

Step 4: The Direct Debit Submitter will be required to capture the DDI information and convert the data into an electronic format, using a standard ISO20022 file format.

Step 5: The DDI data is transmitted to the customer's PSP via a new DDI API.

Step 6: The DDI authority is set up on the customer's account.

Direct Debit Collection

Step 7: The PSU generates a Direct Debit collections file and sends the file to their Direct Debit Submitter.

Step 8: The Direct Debit submitter will be required to convert the Direct Debit collection data into a standard ISO20022 file format if it is not already in an ISO 20022 format.

The customer's PSP will receive a Direct Debit collections file and will execute the payment on the required due date:

- The payment details are validated
- The account is checked for a valid DDI
- The account is checked for available funds
- The account is checked for any other reason not to make the payment e.g. closed account

Step 9: The PSP will send a file of successful payments to the NPSO for clearing and settlement. A total interbank settlement amount will be included.
Step 10: The PSU's PSP will receive a file of successful payments.
Step 11: A settlement obligation is created between the sending and receiving PSP.
Step 12: The NPSO initiates settlement with the Bank of England (BoE).
Step 13: The cleared funds are credited to the PSU's account.
Step 14: The PSU's PSP will be required to advise the PSU of all successful payments that have been applied to the PSU's account. The PSU will be able to reconcile successful payments with any unpaid collections received in Step 9b (see below).

Unpaid Direct Debit

Step 15: Step 9a: Where the PSP is unable to apply the payment, the payment is rejected. A rejected Direct Debit advice is sent to the Direct Debit Submitter.
Step 16: Step 9b: The Direct Debit Submitter informs the PSU of any payments that could not be applied on the payment due date.

4.1.1 Direct Debit Mandate Management

Mandate management describes the ability for the PSU to set up and lodge a valid DDI on behalf of its customer. The mandate management process includes the following functions:

- Set up and lodge a customer's DDI with the customer's bank.
- Amend and resubmit any DDI that could not be lodged by the customer's bank.
- Amend or cancel a customer's existing DDI.
- Redirect a DDI where the destination sort code has a redirection indicator.

The following scenarios illustrate how the NPA can support the set-up and lodgement of a customer's DDI, utilising both an electronic format (e-mandate) and a paper format.

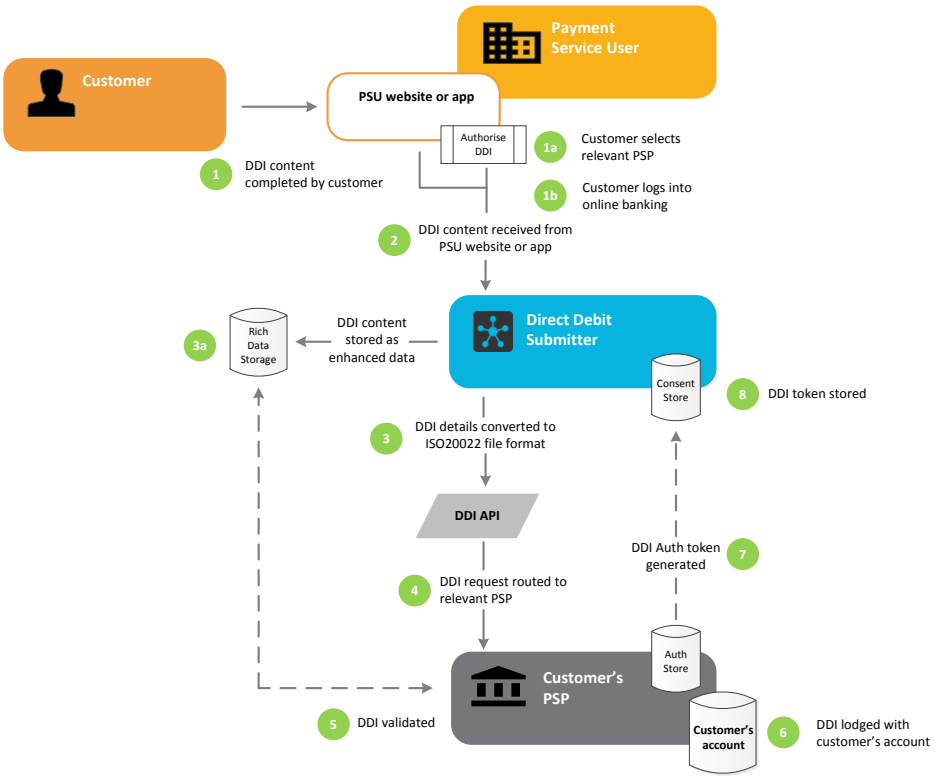
E-Mandates

The PSU will have the ability to provide a DDI through a remote channel such as the internet or a smartphone app.

Strong customer authentication is recommended for use by the customer's PSP in order to authorise the e-mandate. The PSP will generate an authorisation token in order to confirm that the customer has successfully completed strong customer authentication (i.e. logged into their online bank and entered their security details). The authorisation token will be unique to each customer's DDI. Without a valid authorisation token, the customer's PSP will be unable to process the Direct Debit collection.

Where the customer makes an amendment to the Direct Debit and a new DDI is required, a new authorisation token must be generated by the customer's PSP.

The strong customer authentication required to authorise the e-mandate will help to address one of the key detriments identified by the Payment Strategy Forum regarding the assurance of the payment being taken from the correct account. The successful log-in to the customer's own online account infers that the DDI being set up belongs to the intended payer (referred to as "Confirmation of Payer")



Key:

Figure 4.2 NPA E-Mandate Overview

Process Steps:

Step 1: Once the customer has agreed to pay by Direct Debit, the PSU informs the customer to complete a DDI either via their own website or through a smartphone app.

- The customer completes the details by entering the relevant bank account details that the Direct Debit collection will be taken from. The customer will be required to authorise the DDI with their PSP (Step 1a).
- The customer will authorise the DDI by successfully logging into their online banking account held with their PSP (Step 1b).

Step 2: The Direct Debit Submitter will be responsible for redirecting the customer to their relevant PSP in order to authorise the DDI in Step 1. Details of the DDI will also be passed from the PSU's e-mandate solution (i.e. either the website or smartphone app) to the Direct Debit Submitter once the customer has successfully logged into their online banking.

Step 3: The Direct Debit Submitter converts the DDI content into a standard ISO20022 file format, if it is not already in an ISO 20022 format.

- There is an opportunity for the Direct Debit Submitter to store the DDI content and/or other supporting payment information as enhanced data (Step 3a).

Step 4: The DDI data is routed to the customer's PSP via a new DDI API.

Step 5: The DDI is validated by the customer's PSP. The PSP has the opportunity to view any supporting information (held as enhanced data) to assist in validating the DDI e.g. customer details or payment related details that are not provided in the DDI API.

Step 6: Once the customer's PSP has successfully validated the DDI, the DDI is set up on the customer's account

Step 7: The customer's PSP generates a DDI authorisation token. The customer's unique DDI authorisation code is stored by the PSP.

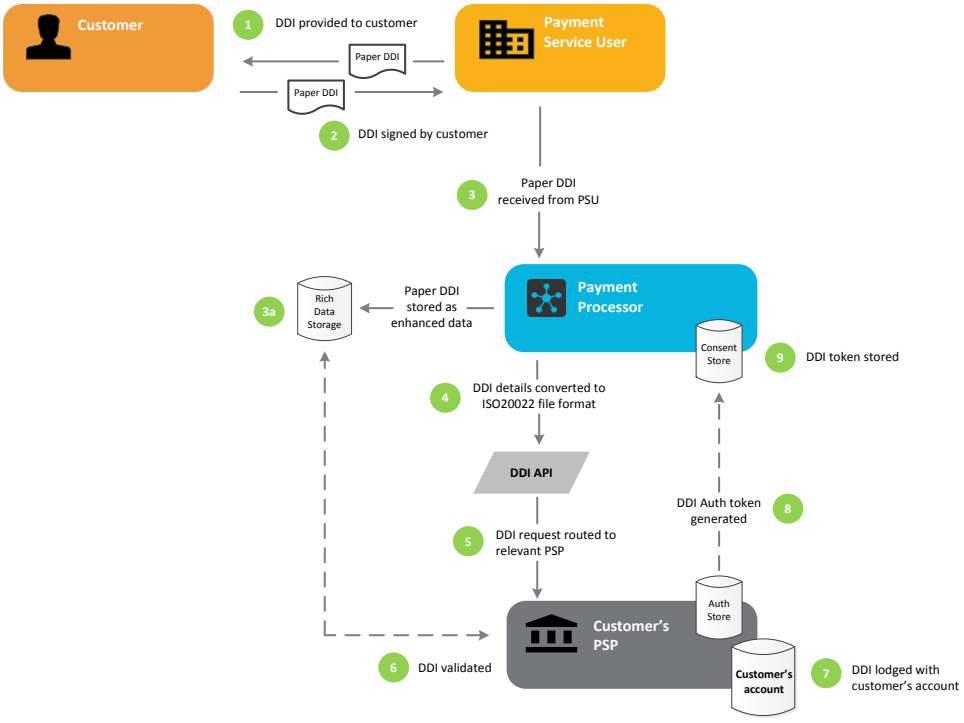
Step 8: The DDI authorisation token is passed to the Direct Debit Submitter and stored. The DDI authorisation token confirms the customer's consent for the PSU to initiate a Direct Debit payment.

Paper DDI

The PSU will still have the ability to provide a paper DDI to the customer. The customer's signature will continue to provide the required consent for authorising a Direct Debit collection.

Once the PSU has received a completed paper DDI, the Direct Debit Submitter will manage the processing of the paper DDI on behalf of the PSU. The Direct Debit Submitter will be required to dematerialise the paper content and create an electronic DDI request which will then be sent to the customer's PSP.

The NPA framework that supports DDI validation through the use of an Authorisation token (as in the case of an e-mandate) can also be applied to the paper DDI. The presence of the customer's signature would be sufficient for the customer's PSP to generate the authorisation token for a paper DDI. The use of an authorisation token for a paper DDI would ensure a consistent approach for processing Direct Debit collections where the PSP's customers have used either a paper DDI or an e-mandate to authorise their payment.



Key:

Figure 4.3 NPA Paper DDI Overview

Process Steps:

Step 1: Once the customer has agreed to pay by Direct Debit, the Payment Service User provides the customer with a paper DDI to complete.

Step 2: The customer completes and signs the paper DDI.

Step 3: The paper DDI is forwarded to the Direct Debit Submitter. The Direct Debit Submitter stores the original paper mandate. In addition, the paper DDI can be scanned and will be provided as enhanced data (Step 3a).

Step 4: The content of the paper DDI is dematerialised and an electronic DDI is created.

Step 5: The DDI details are passed to the customer's PSP via a new DDI API.

Step 6: The DDI details are confirmed by the customer's PSP e.g. verifying that the customer has a valid account held on their system. The DDI API could contain a link to view a copy of the customer's signed DDI as enhanced data. The customer's PSP is able to compare the Paper DDI signature with the signature held on their own system as a way of providing additional customer verification.

Step 7: Once the customer's PSP is satisfied that the customer's DDI details are valid, the DDI is set up on the customer's account.

Step 8: The customer's PSP generates a DDI authorisation token. The customer's unique DDI authorisation code is stored by the PSP.

Step 9: The DDI authorisation token is passed to the Direct Debit Submitter and stored. The DDI authorisation token confirms the customer's consent for the Payment Service User to initiate a Direct Debit payment.

4.1.2 Direct Debit Collection

Organisations are expected to continue to produce a bulk collections file as they do today. Under the NPA framework, the organisation will require a Direct Debit Submitter to process the bulk collections file. The organisation could either directly submit a bulk collections file (using approved software), or indirectly submit a bulk collections file (using a bureau service).

The validation of input files from the Direct Debit Submitter and the routing of payment instructions to each of the customer's PSPs can be provided within different layers of the NPA framework.

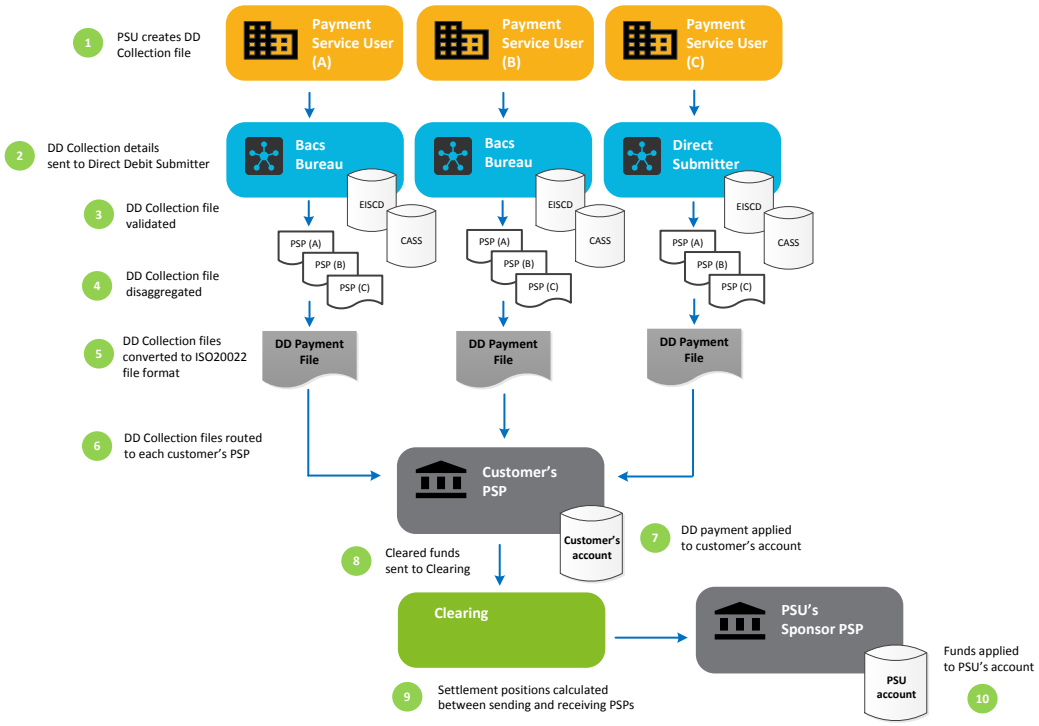
Direct Debit Submitter Processing

Each Direct Debit Submitter will provide the routing and output of the payment files to each destination PSP.

The Direct Debit Submitter will be responsible for the disaggregation of the Direct Debit collection file received from their PSU. Each destination PSP will potentially receive multiple Direct Debit collection files from multiple Direct Debit Submitters

Each Direct Debit Submitter will provide the validation and account redirection prior to outputting the Direct Debit collection file to each destination PSP. Each Direct Debit Submitter will require access to the CASS account switching database to effect any account redirection.

A TPSP has an opportunity to provide transaction processing services on behalf of the PSU. Transaction processing in the TPSP layer will provide competition in the market.



Key:

Figure 4.4 Direct Debit Submitter Processing Overview

Process Steps:

Step 1: Each PSU continues to produce their Direct Debit collections file.

Step 2: Each PSU sends their Direct Debit collections file to their Direct Debit Submitter. In this scenario, PSU A and B are indirect submitters and PSU C is a direct submitter.

Step 3: Each Direct Debit Submitter validates the input files and checks to see if any destination accounts are subject to redirection.

Step 4: Each Direct Debit Submitter disaggregates the Direct Debit collections file into each of the destination PSPs.

Step 5: Each Direct Debit Submitter ensures that the Direct Debit collections file is converted to the standard ISO20022 file format if it is not already in an ISO 20022 format.

Step 6: Each Direct Debit Submitter routes the Direct Debit collections file to each of the destination PSPs.

Step 7: The customer's PSP will receive the Direct Debit collection request and execute the payment on the payment due date.

Step 8: The customer's PSP will send a file of successful payments to the NPSO for clearing and settlement. A total interbank settlement amount will be included.

Step 9: A settlement obligation is created between the sending and receiving PSP.

Step 10: The cleared funds are credited to the PSU's account.

Please refer to Appendix 3 for further details on how the process steps 3, 4 and 6 are expected to work.

Further Analysis

It has been identified through the consultation process that further analysis on understanding how BPSL products and services will run over the NPA and the impact this might have on service users is a necessary and important next step. To this end, this next level of analysis and design is expected to be undertaken by the NPSO during 2018.

It is suggested that a range of options be considered including there being one or more organisations offering a clearing layer overlay service that could offer a range of capabilities such as:-

- receiving input files from each of the Direct Debit Submitters and provide the routing and output of the payment files to each destination PSP.
- being responsible for the disaggregation of Direct Debit collection files received from a Direct Debit Submitter.
- providing a single Direct Debit collections file to each destination PSP.
- providing the validation and account redirection prior to outputting the Direct Debit collection file to the destination PSP.

4.2 Direct Credit Payments

Organisations that use the existing Bacs Direct Credit payment will still require the ability to make payments by electronic transfer directly into their customer's PSP account.

Organisations are expected to continue to produce a bulk credit file as they do today. The organisation will require a Direct Credit Submitter to process the bulk collections file. The organisation could either directly submit a bulk credit file (using approved software), or indirectly submit a bulk credit file (either through a bureau service or a sponsor PSP service.)

Under the NPA framework, there will be the ability to address one of the key detriments identified by the Payment Strategy Forum regarding the assurance of the payment being taken from the correct account. A new "Confirmation of Payee" API will allow the PSU to confirm with the customer's PSP that the account belongs to the intended customer prior to submitting the Direct Credit file to the Direct Credit Submitter.

The processing of the Direct Credit payment follows a similar approach to Direct Debit collections process described in Section 4.1. The PSU's PSP will receive a Direct Credit payment request from the PSU via their Direct Credit Submitter. The PSP will execute the Direct Credit request on the payment due date and apply the payment to the PSU's account. The Customer's PSU will only receive cleared funds into their account on the payment due date.

The PSU will be notified of any unapplied Direct Credits on the payment due date.

The NPSO will continue to perform a central role in maintaining, monitoring and facilitating settlement between the sending and receiving PSP. The NPSO will also have responsibility for the governance and compliance of the NPA layers over which Direct Credit services may run.

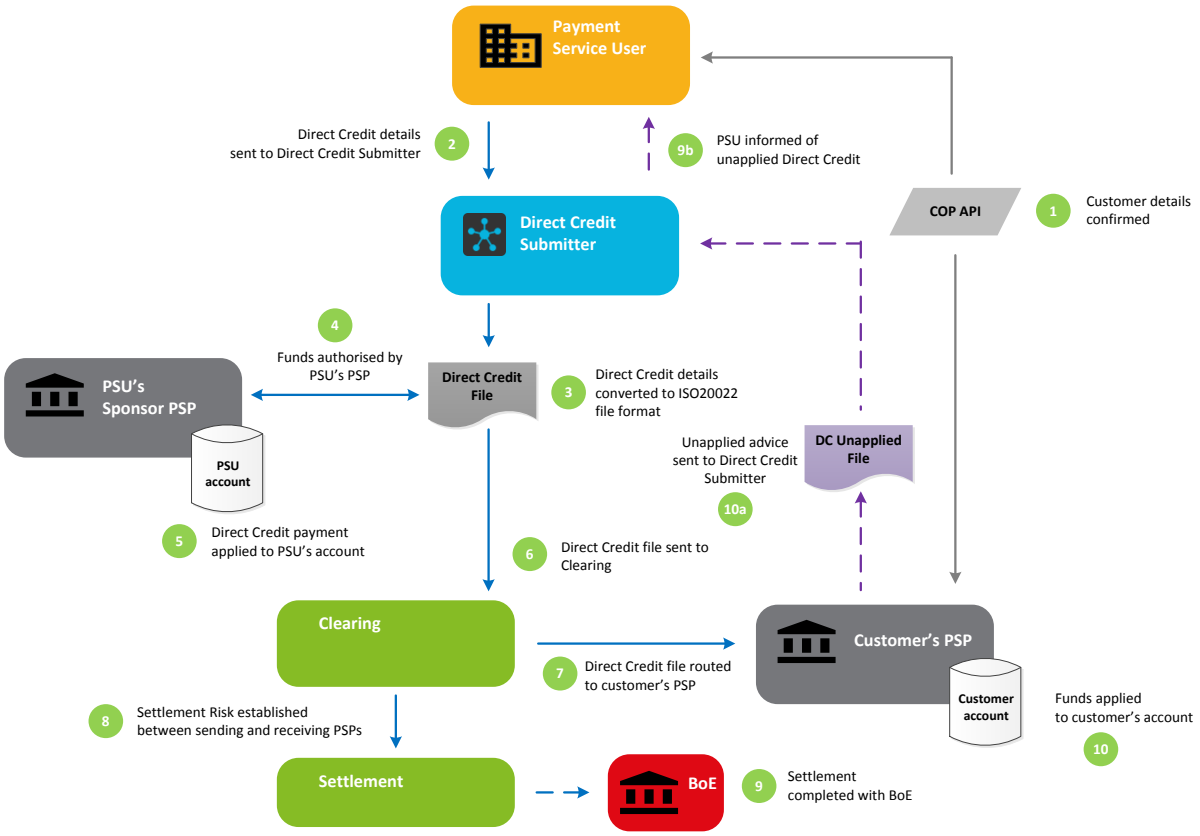


Figure 4.5 NPA Direct Credit Overview

Process Steps:

- Step 1: The PSU initiates the Confirmation of Payee API to confirm the customer's details with the customer's PSP.
- Step 2: The PSU creates a Direct Credit file and sends the file to their Direct Credit Submitter.
- Step 3: The Direct Credit Submitter ensures that the Direct Credit file is converted to the standard ISO20022 file format if it is not already in an ISO 20022 format.
- Step 4: The PSU's PSP receives the Direct Credit payment request and funds are authorised.
- Step 5: The Direct Credit payment is applied to the PSU's account.
- Step 6: The Direct Credit file is sent to the Clearing layer.
- Step 7: The Direct Credit file is routed to the customer's PSP.
- Step 8: A settlement obligation is created between the sending and receiving PSP.
- Step 9: The NPSO initiates settlement with the Bank of England (BoE).
- Step 10: The cleared funds are credited to the customer's account. Any unapplied payments are returned to the Direct Credit Submitter.

As described in Section 4.1, the validation of input files from the Direct Credit Submitter and the routing of payments to each of the customer's PSPs can be provided within different layers of the NPA framework.

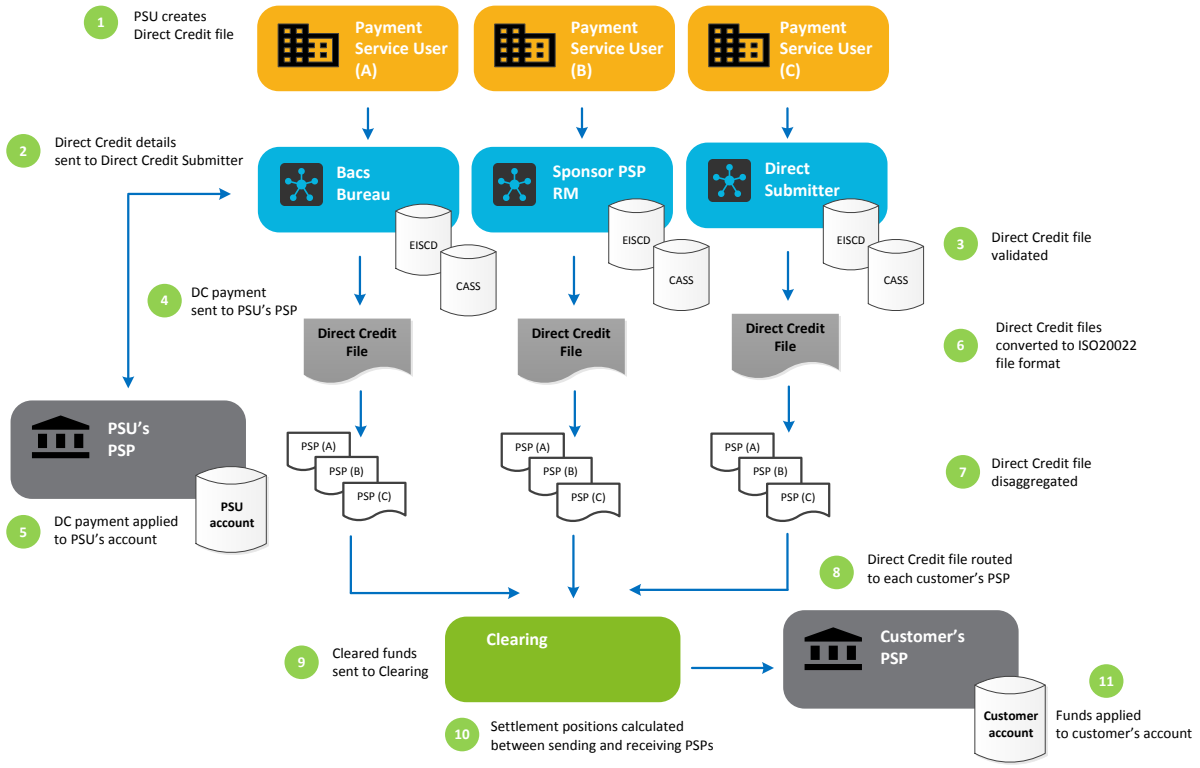
4.2.1 Direct Credit Submitter Processing

Each Direct Credit submitter will provide the routing and output of the payment files to each destination PSP.

The Direct Credit submitter will be responsible for the disaggregation of the Direct Credit file received from their PSU. Each destination PSP will potentially receive multiple Direct Credit files from multiple Direct Credit submitters.

Each Direct Credit submitter will provide the validation and account redirection prior to outputting the Direct Credit file to each destination PSP. Each Direct Credit Submitter will require access to the CASS account switching database to effect any account redirection.

A TPSP has an opportunity to provide transaction processing services on behalf of the PSU. Transaction processing in the TPSP layer will provide competition in the market.



Key:

Figure 4.6 Direct Credit Submitter Processing Overview

Process Steps:

Step 1: Each PSU continues to produce their Direct Credit file.

Step 2: Each PSU sends their Direct Credit file to their Direct Credit submitter. In this scenario, PSU A is an indirect submitter using a bureau, PSU B is an indirect submitter using their sponsor PSP's business banking Relationship Manager (RM) and PSU C is a direct submitter using their own approved software.

Step 3: Each Direct Credit submitter validates the input files and checks to see if any destination accounts are subject to redirection.

Step 4: Each Direct Credit submitter sends a Direct Credit request to the PSU's PSP.
Step 5: The sponsor's PSP receives each Direct Credit request and debits the PSU's account on the payment due date.
Step 6: Each Direct Credit submitter ensures that the Direct Credit file is converted to the standard ISO20022 file format if it is not already in an ISO 20022 format.
Step 7: Each Direct Credit submitter disaggregates the Direct Credit file.
Step 8: Each Direct Credit submitter routes the Direct Credit file to the customer's PSP.
Step 9: Each Direct Credit file is sent to the NPSO for clearing and settlement.
Step 10: A settlement obligation is created between the sending and receiving PSP.
Step 11: The customer's PSP applies the funds to the customer's account.

Please refer to Appendix 3 for further details on how the process steps 3 & 7 are expected to work.

Further Analysis

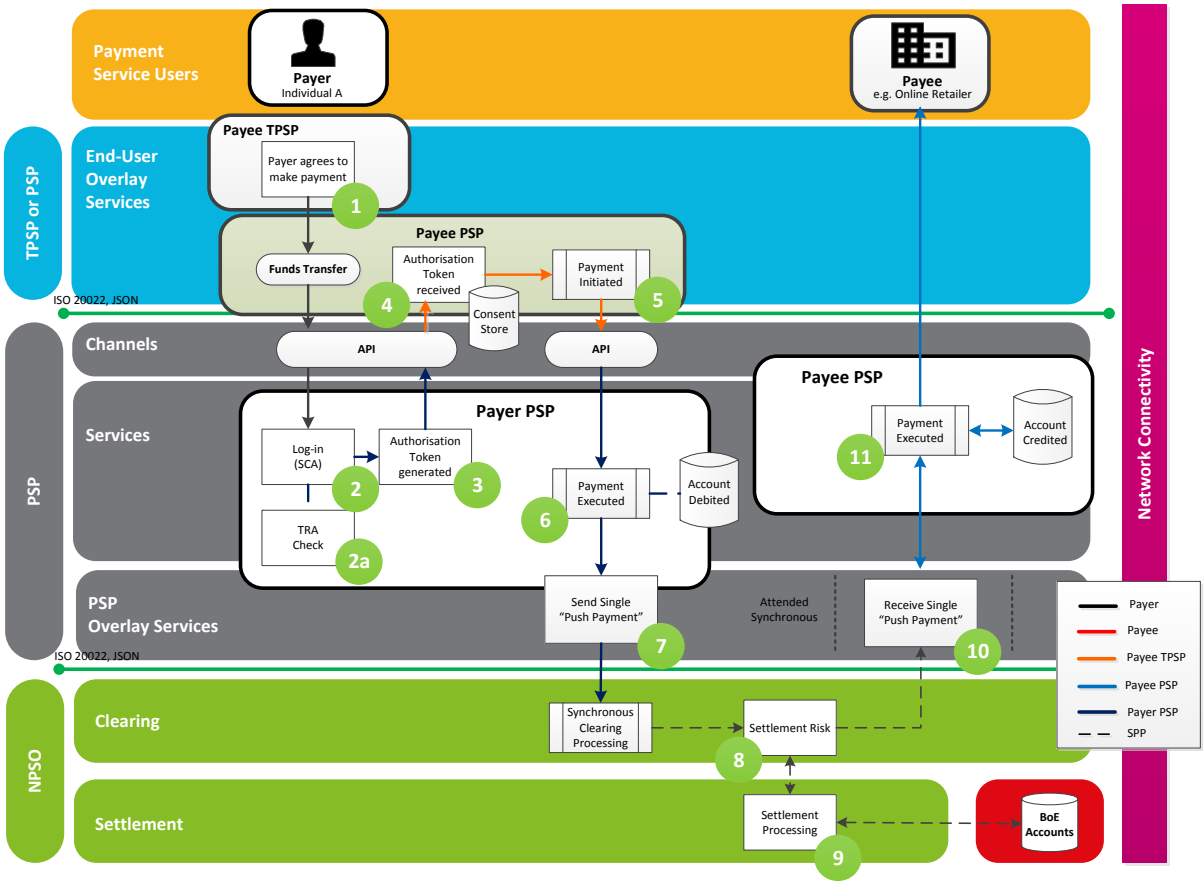
As has been identified above, further analysis is being suggested. In the context of Direct Credits, consideration could be given to how a clearing layer overlay service, offered by one or more organisations, could be used to deliver some or all of the capabilities shown above but for Direct Credit submissions.

4.3 Single Immediate Payment

Payment Service Users (PSUs) that use the existing Faster Payments service will still require the ability to make SIPs.

The following scenario illustrates how an organisation could utilise a SIP as a means of payment for a product or service offered via their online channel. Organisations could incorporate a SIP into their payment options, supplementing their existing payment methods such as Debit Card, Credit Card and PayPal.

Under the NPA framework, the organisation will require a TPSP to manage the transfer of funds between the individual (payer) purchasing the product or service and the organisation receiving the payment (payee). The TPSP role could be provided by a third party or a PSP. Consent will be required by the payer to initiate the transfer of funds and in this scenario, the individual is redirected to their PSP to authorise the payment.



Key:

Figure 4.7 Single Immediate Payment

Step 1: The online retailer includes a funds transfer payment option which will allow the customer to pay for their product or service directly from the PSP account.

Step 2: The customer selects the fund's transfer option and is redirected to their online PSP where they are required to log into their account with their security credentials. The customer's PSP will also perform a Transaction Risk Assessment (Step 2a).

Step 3: The customer's PSP will authorise the payment and an authorisation token is generated.

Step 4: The online retailer's TPSP receives the authorisation token to confirm that consent has been given to initiate the payment.

Step 5: The payment is initiated via the online retailer's website.

Step 6: The customer's PSP executes the payment and checks for available funds.

Step 7: Cleared funds are pushed to the clearing and settlement service.

Step 8: A settlement obligation is created between the sending and receiving PSP.

Step 9: The clearing and settlement service initiates settlement with the BoE.

Step 10: Payment details are sent to the online retailer's PSP.

Step 11: The online retailer is credited with the payment. The online retailer receives confirmation that the payment has been completed successfully.

4.4 Regular Payments

Individuals will still require the ability to arrange for a payment to be made from their PSP account on a date in the future. The NPA framework supports both a single forward dated payment and a recurring forward dated payment (Standing Order).

4.4.1 Standing Order Set up

The authority to execute a forward dated payment is typically set up by an individual via their own PSP. The ability to set up and manage forward dated payments could be provided by a new payment provider in a competitive market. In the following scenario (Figure 4.8), a TPSP (or PSP acting as a TPSP) has developed a mobile app for individuals to set up a Standing Order.

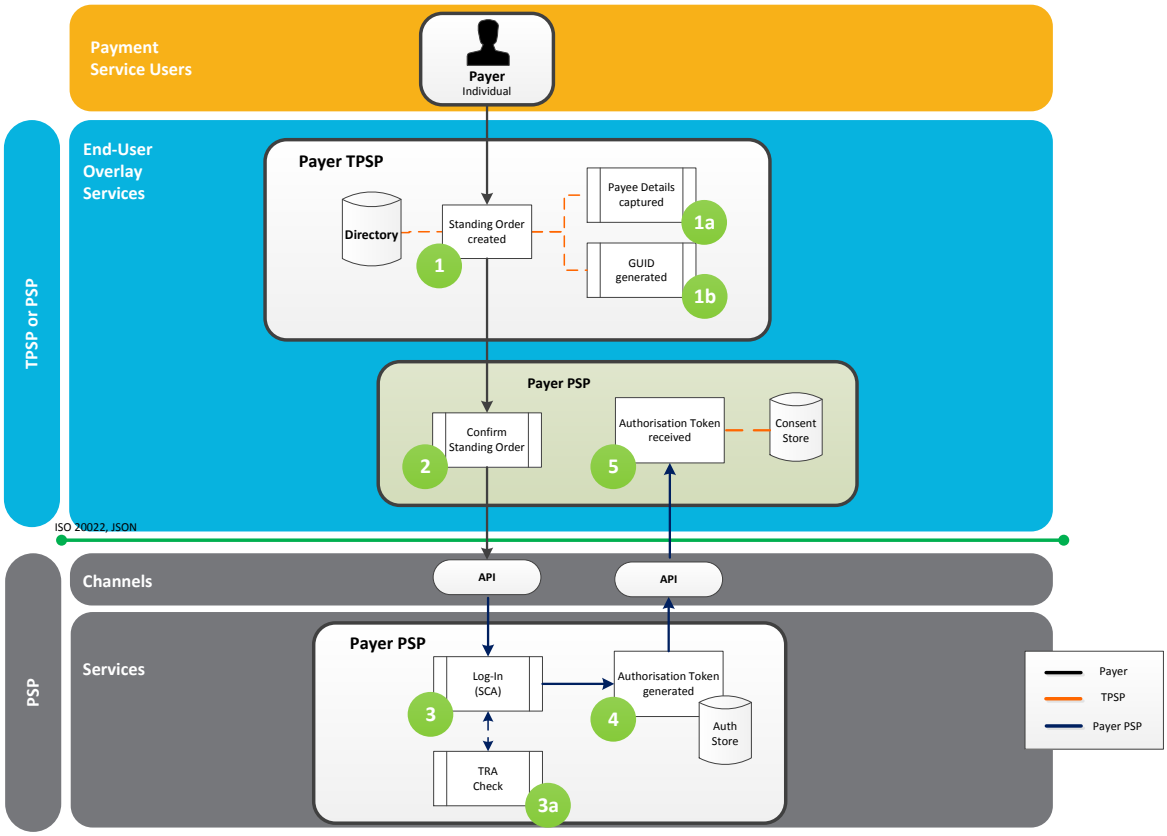


Figure 4.8 Standing Order Set-up

Step 1: A TPSP allows an individual to create a Standing Order via a mobile app. Payee details are captured (Step 1a) and a unique reference ID will be generated for each Standing Order created (Step 1b).

Step 2: The individual confirms the Standing Order details and is redirected to their PSP account to authorise the payment.

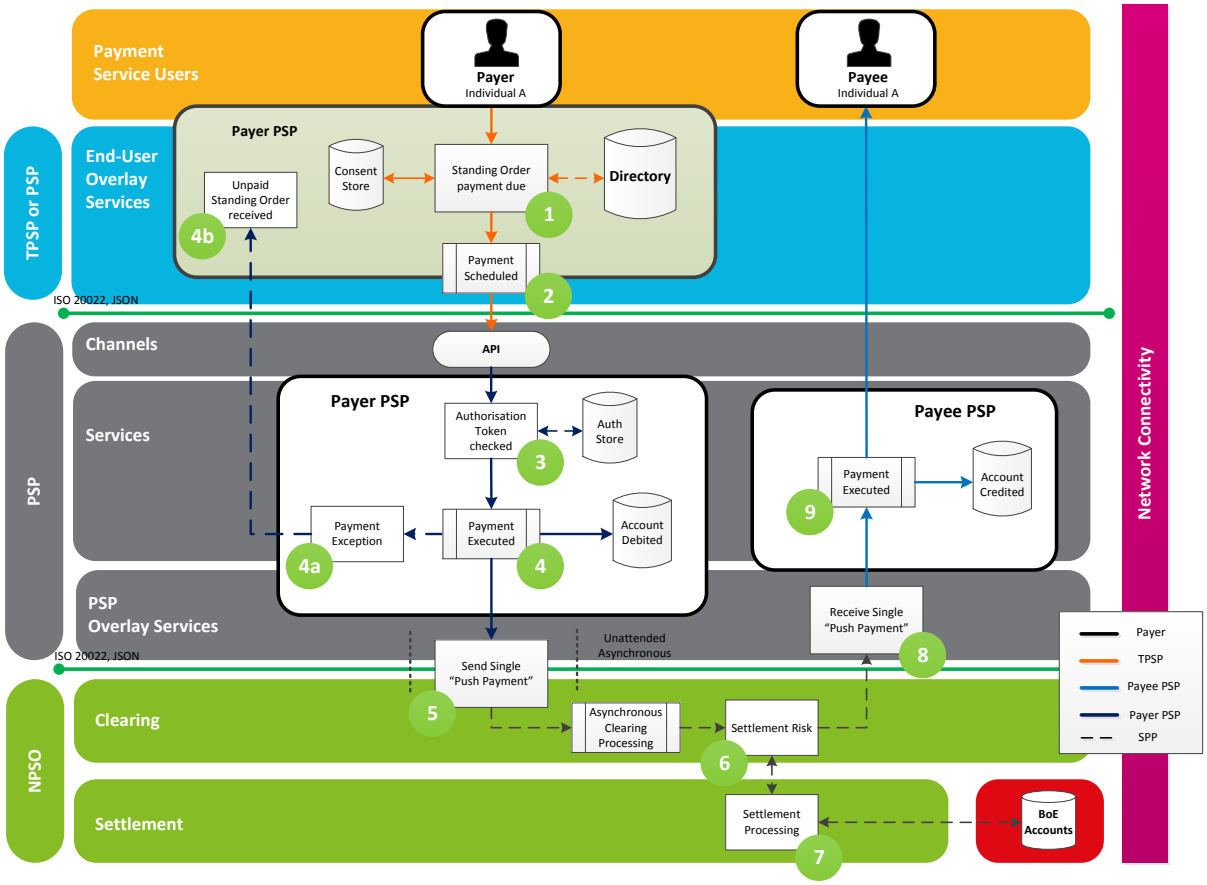
Step 3: In this example, the organisation's app has allowed the individual to choose their online PSP and log into their account using their online credentials. The payer's PSP will also perform a Transaction Risk Assessment (Step 3a)

Step 4: The customer's PSP will authorise the payment and an authorisation token is generated.

Step 5: The TPSP receives the authorisation token to confirm that the Standing Order has been set up.

4.4.2 Standing Order Payment

Figure 4.9 shows how a Standing Order payment can be executed on behalf of an individual. The role of the TPSP is to initiate the payment on the date that has been predetermined by the Standing Order set up as described in Section 4.4.1. The TPSP could execute the Standing Order as either an individual payment or as a collection of Standing Order payments, (i.e. a single bulk payment), to improve efficiency in payment processing.



Key:

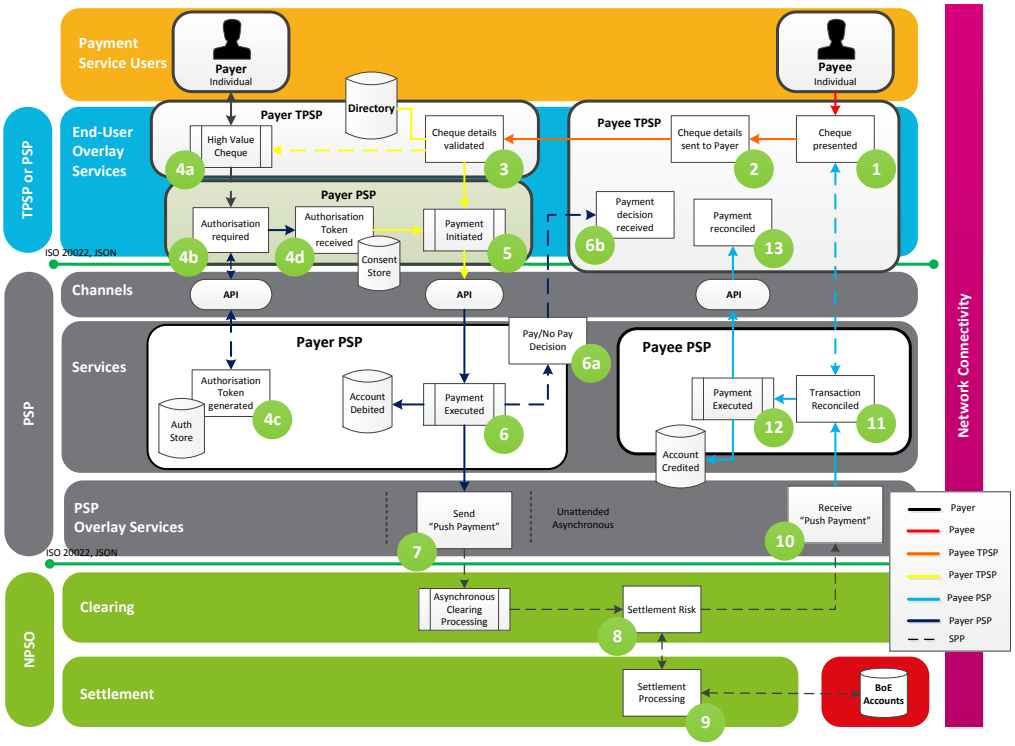
Figure 4.9 Standing Order payment

Step 1: The Standing Order has been set up and the payment is due on a predetermined date.
Step 2: When the due date arrives, the payment is initiated by the TPSP and the individual's PSP is notified.
Step 3: The individual's PSP checks that the Standing Order has been authorised.
Step 4: The PSP executes the payment and a funds check is performed. Where a payment could not be applied to the account (Step 4a), the TPSP is notified of the unpaid Standing Order (Step 4b) who in turn will notify the payer.
Step 5: Cleared funds are pushed to the clearing and settlement service.
Step 6: A settlement obligation is created between the sending and receiving PSP.
Step 7: The clearing and settlement service initiates settlement with the BoE.
Step 8: Payment details are sent to the payee's PSP.

Step 9: The payee is credited with the payment on the due date.

4.5 Cheque Payments (ICS)

Individuals will still require the ability to make a payment via cheque. The NPA framework supports the Image Clearing System (ICS) currently operated by Cheque and Credit Clearing Company Limited. Figure 4.10 shows how an individual could present a cheque via their PSP's branch network. In this scenario, the individual's PSP assumes the role of the TPSP in order to initiate the request for a cheque payment.



Key:

Figure 4.10 Cheque Payment

Step 1: The individual (payee) presents a cheque to their local branch to be deposited into their account.

Step 2: The payee's TPSP scans the cheque and sends the details to the payer's TPSP. Note: conceivably, the cheque image will not be routed via the ICS central system as per existing cheque processing.

Step 3: The payer's TPSP validates the cheque details e.g. duplicates, fraud or high value.

Step 4: In this scenario, a high-value cheque payment requires the payer to authorise the cheque before further processing (Steps 4a through to 4d). Note: the authorisation process is consistent with the Standing Order set-up process described in Section 4.4.1

Step 5: The cheque payment is initiated by the payer's TPSP.

Step 6: The PSP executes the payment and a funds check is performed. Where the payment cannot be executed, the payee's TPSP is notified via the Pay/No Go message (Step 6a and 6b).

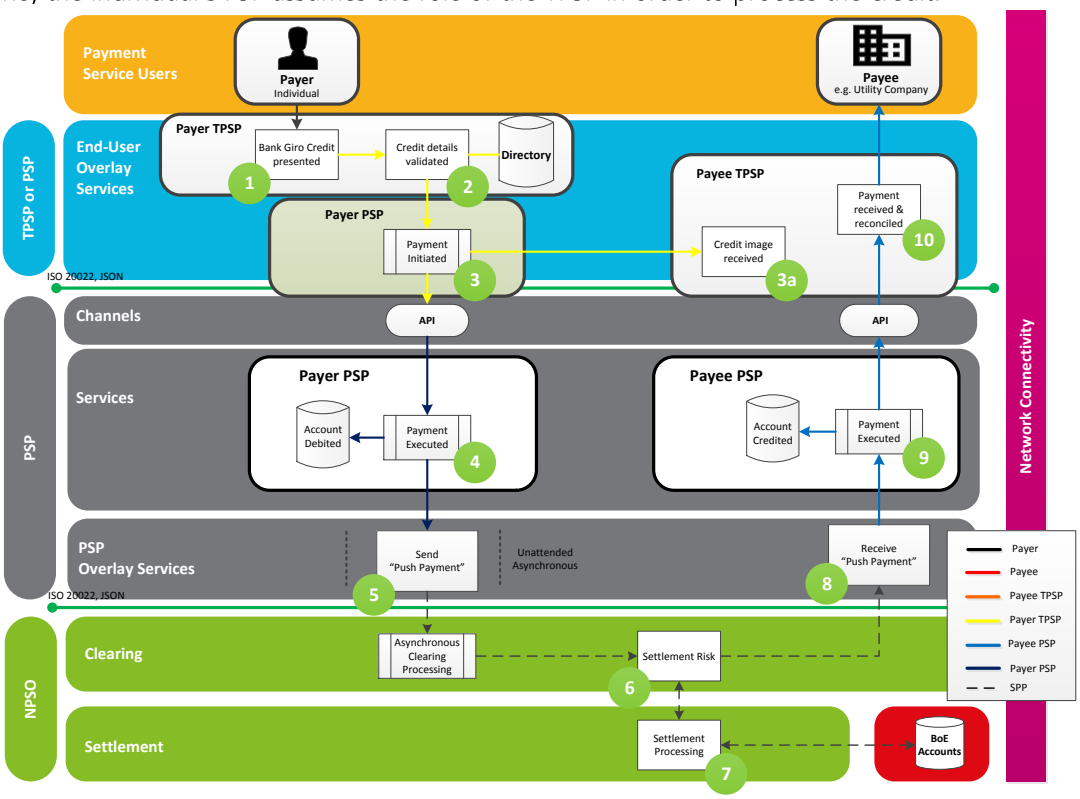
Step 7: Cleared funds are pushed to the clearing and settlement service.

Step 8: A settlement obligation is created between the receiving and sending PSP.
Step 9: The clearing and settlement service initiates settlement with the BoE.
Step 10: Payment details are sent to the payee's PSP.
Step 11: The payment is reconciled against the cheque received from the payee's TPSP.
Step 12: The payee is credited with the amount.
Step 13: The payee TPSP's reconciliation process ensures that the payment has been cleared.

4.6 Paper Credit Payments

Individuals will still require the ability to present a Bank Giro Credit (BGC) as a means of transferring funds from their account to make a payment e.g. a utility bill or invoice.

Figure 4.11 shows how an individual could present a credit via their PSP's branch network. In this scenario, the individual's PSP assumes the role of the TPSP in order to process the credit.



Key:

Figure 4.11 Paper Credit Payment

Step 1: The individual (payer) presents a credit to be paid, for example, a Bank Giro Credit associated with a utility invoice.
Step 2: The payer's TPSP validates the credit details.
Step 3: The payment is initiated by the payer's TPSP. An image of the credit is made by the payer's TPSP and sent to the payee's TPSP once the payment has been successfully applied (Step 3a). Note: the enhanced data capability could also be used to send an image of the credit
Step 4: The PSP executes the payment and a funds check is performed.
Step 5: Cleared funds are pushed to the clearing and settlement service.

Step 6: A settlement obligation is created between the sending and receiving PSP.
Step 7: The clearing and settlement service initiates settlement with the BoE.
Step 8: Payment details are sent to the payee's PSP.
Step 9: The payee is credited with the amount.
Step 10: The payee TPSP's reconciliation process ensures that the payment has been cleared.

5 NPA Support of the End-User Needs Solutions

5.1 Introduction

Since the publication of the original document more work has been undertaken on developing the requirements for the End-User Needs services. We would recommend the reader refers to the documents 'Collaborative Requirements and Rules for the End User Needs Solutions Blueprint' and 'Request to Pay Technical Solution Blueprint' for the most up to date information on these services.

For completeness, the original section with additional Enhanced Data use cases is provided below.

5.2 Request to Pay

Request to Pay (RtP) is a communication mechanism that will allow a payee (government, businesses, charities and consumers) to send a message to a payer requesting a payment.

Through Request to Pay, a payee will be able to notify a payer of a payment that requires their attention and in return, the payer will be able to respond to the payee. For example, the payer will be able to accept the request and make full or partial payments; decline it; request an extension of the time period in which they can make the payment; or request more information. When a payer accepts the request, they will be able to pay using a choice of available methods, and the acceptance will automatically trigger the payment being made.

End-to-End Journey for Request to Pay

The overall end-to-end Request to Pay journey will take the form shown in Figure 5.1:

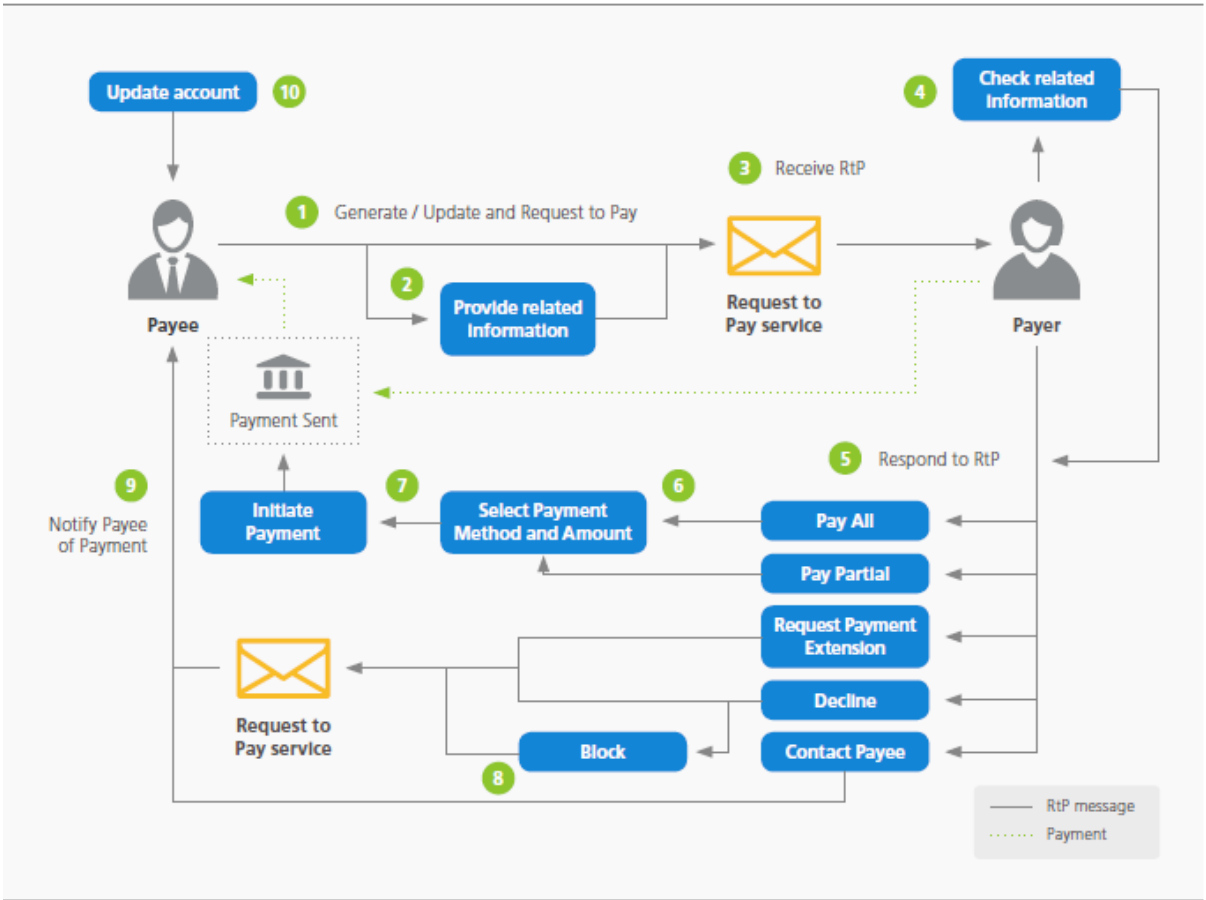


Figure 5.1 Request to Pay End-to-End Journey

Step 1: A payee generates a new Request to Pay (or updates an existing Request to Pay), which is then sent to the payer.

Step 2: A payee has the option to provide additional information for the payer. This could take the form of a hyperlink to related information stored elsewhere or an attached document for example.

Step 3: The payer receives the Request to Pay through their preferred channel.

Step 4: The payer reviews additional information related to the received request – if the payee has provided this

Step 5: The payer responds to the Request to Pay, at which point they have a number of options for payment; pay all, pay partial, request payment extension, decline or contact payee.

Step 6: The payer selects the payment method they want to utilise from the payment options supported by the payee and their PSP. The payer can set the amount that they want to pay for a single instalment.

Step 7: The payer initiates payment.

Step 8: The payer can block a payee from sending requests to them. The payee will be notified, and any future requests will not be received by the payer (unless they choose to unblock the payee).

Step 9: The payee receives a notification with the payer's response.

Step 10: Once the payment period is complete, the payee updates the payer's billing account based on the information that has been received and any relevant back-office processes.

How will the NPA support Request to Pay?

The NPA will provide the architectural framework on which Request to Pay will be implemented as an overlay service. Common standards through APIs and messaging will be in place to ensure interoperability.

Figure 5.2 provides an example[4] of a utility company requesting a bill payment from one of its customers. The payer chooses to make an electronic payment over the NPA through their TPSP.

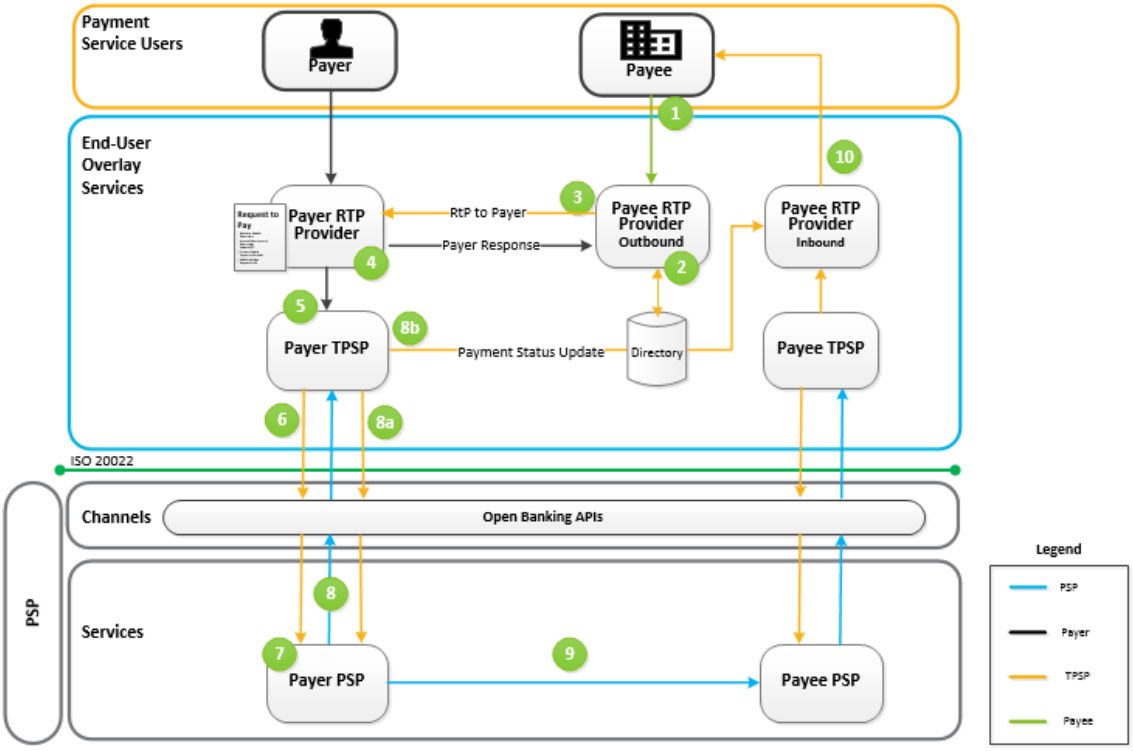


Figure 5.2 Request to Pay Potential Solution

In this example, the main steps involved are:

Step 1: The payee's billing system would initiate a Request to Pay (RtP) and pass this on with the appropriate information to the RtP Service provider.

Step 2: The payee's RtP provider generates a 'Request to Pay' instruction. The necessary data is populated. Recipient, Description, Amount, Reference ID etc. The provider would also look up the payer's RtP address from a directory.

Step 3: The payee's RtP provider sends the RtP to the payer's RtP provider.

Step 4: Upon receipt of the RtP, the payer would respond (Pay all, Partial pay, Request Contact etc.). The response would be sent back to the payee's RtP provider.

Step 5: If payer intends to make a payment (Full or Partial), a payment process would be initiated via their TPSP, who may also be their PSP.

Step 6: The payer's TPSP authenticates the payer and initiates the payment.

Step 7: The payer's PSP authorises the transaction.

Step 8: The payer's TPSP receives the payment authorisation (via a token) from the payer's PSP and initiates payment (Step 8a). The payee would also be updated on the payment initiation outcome. (Step 8b).

Step 9: Funds are transferred to the payee's PSP.

Step 10: The payee's RtP provider updates the request status and passes this on to the payee.

[4] Please note that the following is just one example, and therefore, not the only way Request to Pay could be deployed on the NPA.

5.3 Assurance Data

Assurance data will provide key facts about a payment, e.g. the availability of funds to make a payment, the correct destination of the payment prior to paying, the status of the payment while 'en route' to the payee[5], and the delivery status. Providing this information increases end-users' confidence.

Assurance data has been proposed as a suite of tools:

1. Provision of real-time balance information (supported by PSPs and therefore not covered in this section).
2. Confirmation of Payee (NPA based feature).
3. Payment status and tracking (NPA based feature).

In combination, these 3 tools will provide assurance over the lifecycle of the payment: initiation, processing and receipt.

5.3.1 Confirmation of Payee (CoP)

Confirmation of Payee (CoP) will provide a payer with information to give them assurance that the account to which they are making the payment belongs to the intended payee. This will help to address the detriment associated with misdirected payments.

As a special case, CoP will also include a Confirmation of payer capability. Confirmation of payer addresses the need for a payee setting up a payment mandate (direct debit) to verify that the account, from which they will be initiating the payment, belongs to the intended payer.

End-to-End Journey for CoP

Figure 5.3 illustrates the end-to-end journey for CoP.

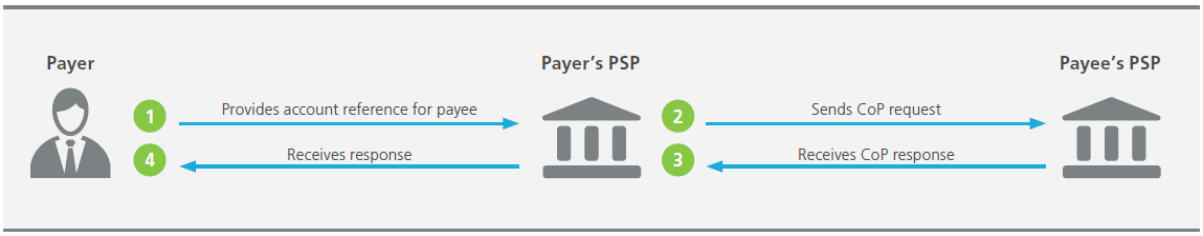


Figure 5.3 Confirmation of Payee End-to-End Journey

Step 1: The payer provides the account reference details (e.g. sort code and account number) to their PSP.
Step 2: The payer's PSP sends CoP request to the payee's bank.
Step 3: The payee's PSP sends a response back to the payer's PSP.
Step 4: The payer's PSP presents the response to the payer. The payer makes a decision based on the CoP response.

How would the NPA support CoP?

The NPA will be designed to provide an architectural framework, set of standards and APIs that will enable Confirmation of Payee (CoP) providers to interoperate.[6]

It is considered essential that all PSPs participating in CoP provide a near real-time CoP response to registered PSPs requesting payee information. Figure 5.4 illustrates an example[7] where the payer is

[5] The level and nature of status tracking varies across the payment methods.
[6] We support the work of PayM to deliver a 'Confirmation of Payee' capability on the current architecture, and we recognise the potential of this activity to inform the final design of the overall Assurance Data Solution in the NPA.
[7] Please note that the following is just one example (and therefore not the only way possible) of how Confirmation of Payee could work over NPA.

making a first-time payment to a new payee with their bank account details that were received via a text. The payer wants to be sure that the details he received are correct and that the account actually belongs to the payee when he makes the payment. The payer is making an electronic payment over the NPA.

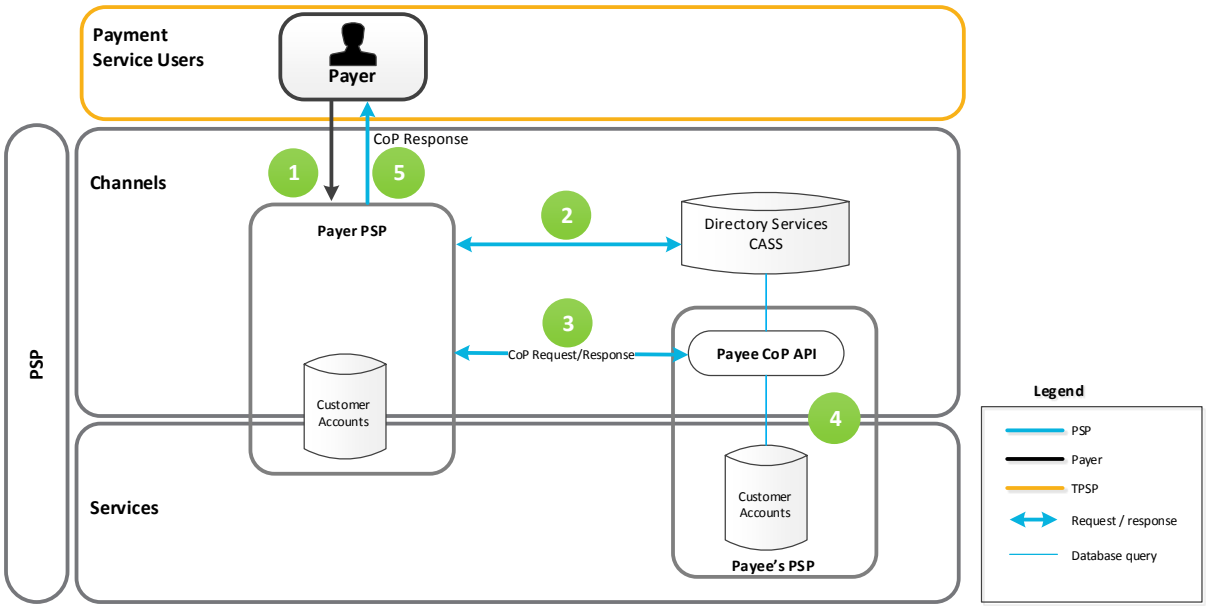


Figure 5.4 Confirmation of Payee Potential Solution

In this example, the main steps involved are:

Step 1: The payer provides the payee's account details.

Step 2: The payer's PSP looks up these details in a directory to determine the payee's PSP. The payer's PSP is then able to determine the correct API endpoint.

Step 3: The payer's PSP makes a Confirmation of Payee request to the payee's PSP CoP service through an API call.

Step 4: The payee's PSP upon receipt of the CoP request looks up the payee's details in its customer account store (Step 4a). The payee's PSP returns the CoP response back to the payer's PSP (Step 4b).

Step 5: The payer is presented with the response by their PSP. The user makes a decision based on the information provided.

Confirmation of payer scenario can be supported by the e-mandate set up the process. See Section 4.1.1 for an example of how a utility company allows an individual to confirm the payer using the e-mandate process for Direct Debits.

5.3.2 Payments Status and Tracking

Once a payment is initiated, the payer will want to know the status of the payment and, if not in real-time, its position on its journey to the payee.

Payments Status Tracking End-to-End Journey

Figure 5.5 summarises the main parts of the payment journey and what is being tracked.

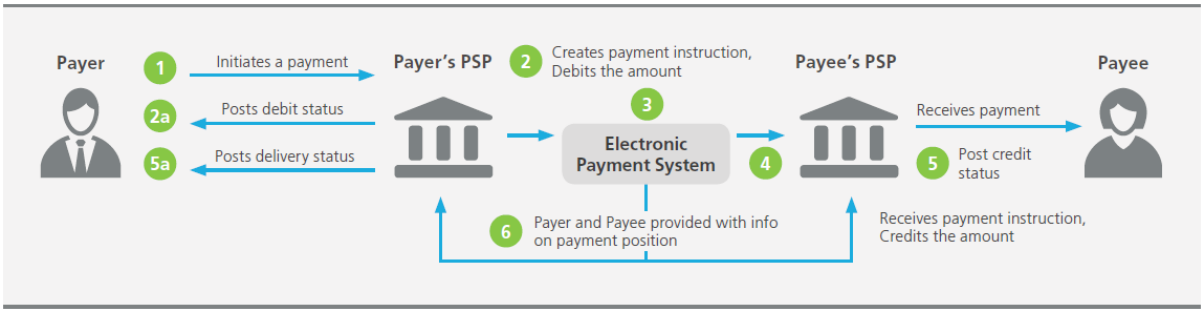


Figure 5.5 Payments Status Tracking End-to-End Journey

Step 1: Payer initiates a payment by providing PSP with payment details and instructions.
Step 2: Payer's PSP creates payment instruction and initiates it. The payer is provided with information on the debit status of the payment (2a).
Step 3: Payment passed on to the payment systems.
Step 4: Payee's PSP receives payment instruction and credits payment to payee's account.
Step 5: Information on credit status provided to the payee. The payer is provided with information on the payment being credited to the payee (5a).
Step 6: Throughout the journey, the payer and payee are provided with information on the payment's position.

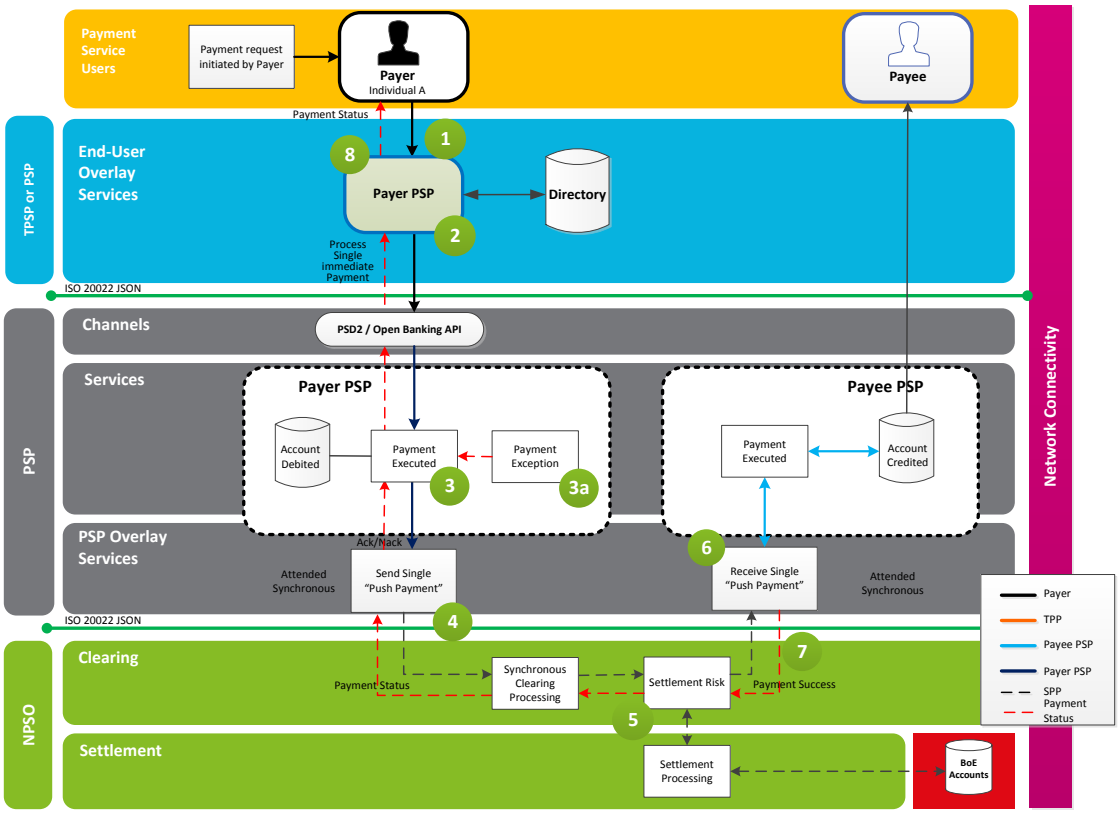
How will the NPA support Payment status tracking?

NPA will support two types of push payments: attended and unattended push payments. It will support the provision of payment status messages to a customer's PSP / TPSP throughout the payments lifecycle.

Single immediate payments have the advantage of being processed in near real time resulting in immediate feedback. For unattended payments, status messages are not provided in real-time.[8]

Figure 5.6 illustrates payment status tracking for a Single Immediate Payment.

[8] In the case of 2nd tier accounts the payer will be notified immediately once the payment is received in the collecting account. They will receive notification once the payment
has been forwarded. This type of payment is expected to represent a fraction of the overall payments volume going through NPA.



Key:

Figure 5.6 Payments Status Tracking Potential Solution

In this example, the main steps involved are:

Step 1: Payment is initiated via Open Banking APIs through the payer's TPSP.

Step 2: The payer's PSP executes the payment request and payer's account is debited. Where the payment cannot be executed, a payment exception message will be returned to the payer (Step 3a).

Step 3: The payer's PSP sends the payment details to the clearing and settlement service using a push payment and receives back an acknowledgement.

Step 4: The clearing and settlement risk management checks the PSP's risk position and creates a settlement obligation. The clearing and settlement service initiates settlement with the Bank of England (BoE).

Step 5: The clearing and settlement service sends the cleared settlement payment details to the payee's PSP and simultaneously confirms the payment status. The payee's PSP checks the account status and credits the payee's account.

Step 6: The payee's PSP confirms payment credited and provides the payment success status to the payer's PSP.

Step 7: The payer will be notified that the payment has been completed successfully via their TPSP.

5.4 Enhanced Data

An electronic payment is broadly composed of two parts: a payment instruction and remittance information. The payment instruction initiates transfer of money between the payer and payee. The remittance information provides context on the underlying commercial transaction.

Enhanced Data is the technical capability to add, associate, retrieve, and access increased amounts of remittance information to a payment instruction in a form that is structured[9] and standard.

End-to-End Journey – Enhanced Data

The overall end-to-end Enhanced Data journey will take the form shown in Figure 5.7.

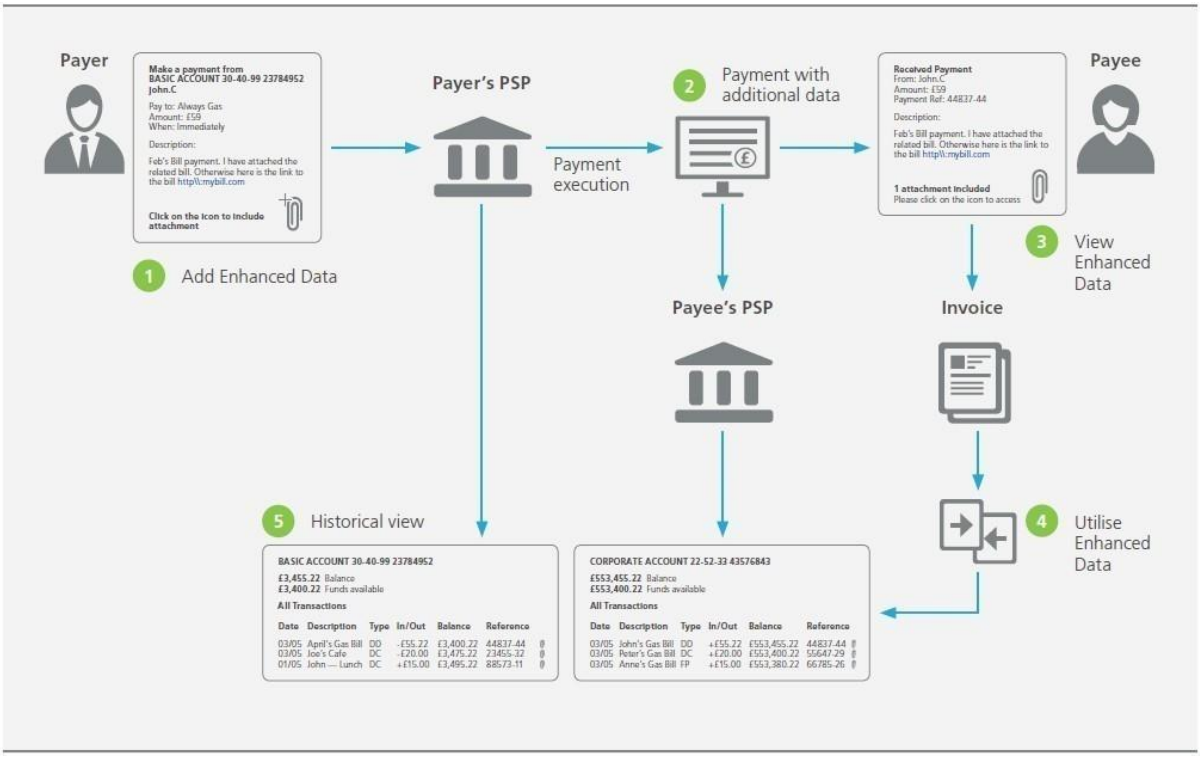


Figure 5.7 End-to-End Journey Enhanced Data

Step 1: The payer adds Enhanced Data to a payment. E.g. gas bill or hyperlink.
Step 2: Payment travels to the payee's PSP with Enhanced Data included by the payer.
Step 3: Payee accesses the Enhanced Data provided through APIs or PSP interfaces.
Step 4: Payee utilises Enhanced Data to reconcile the payment to the payer's account.
Step 5: Both payer and payee are able to access Enhanced Data added to historic payments made or received through APIs or interfaces provided by PSPs.

How will the NPA support Enhanced Data?

Enhanced data is expected to be delivered on the following design principles:

- Storage agnostic – The data could be stored in the user's system or in the cloud. However, the storage should conform to NPA security requirements.
- The entity that stores the data is not expected to be a regulated body, however, it is expected that the entity that retrieves the data will be a governed or regulated body i.e. a PSP or an RtP TPSP.

[9] Structured data is data that is highly organised, and strictly defined in its form and nature. Structured data has the advantage of being easier to enter, store, query and analyse using a computer.

- The payment or request to pay message that contains the enhanced data should not be truncated at any of the NPA layers i.e. all participants should pass the enhanced data without truncation.
- As in SEPA, the remittance information field (140 character length) in ISO20022 could be used to store the enhanced data as the URL link to the enhanced data or as structured data where required (e.g. benefit payment breakdown).

The New Payment Architecture will adopt the ISO 20022 messaging standard. ISO 20022 will inherently provide the capability to carry additional data as well as the framework to ensure data added is structured. The use of ISO 20022 is a key assumption in the delivery of Enhanced Data in the New Payments Architecture.

TPSPs (or PSPs) are expected to offer the storage service with each enhanced data item being uniquely identifiable in the external cloud through a unique identifier. The solution supports multiple enhanced data items per transaction.

Enhanced data TPSPs are expected to be registered entities with the directory holding routing data for each enhanced data TPSP. Taking this approach will allow multiple enhanced data TPSPs and external cloud providers to compete in providing enhanced data services/storage.

The data required (e.g. Globally Unique Identifier (GUID), document ref, enhanced data token, enhanced data TPSP Identifier) to allow the payee's TPSP to access the enhanced data items will be sent with the cleared payment and API specifications will be provided where required. The solution supports multiple enhanced data items per transaction.

Encryption will ensure that the enhanced data token issued by the enhanced data TPSP can only be used by the intended recipient to access the enhanced data items.

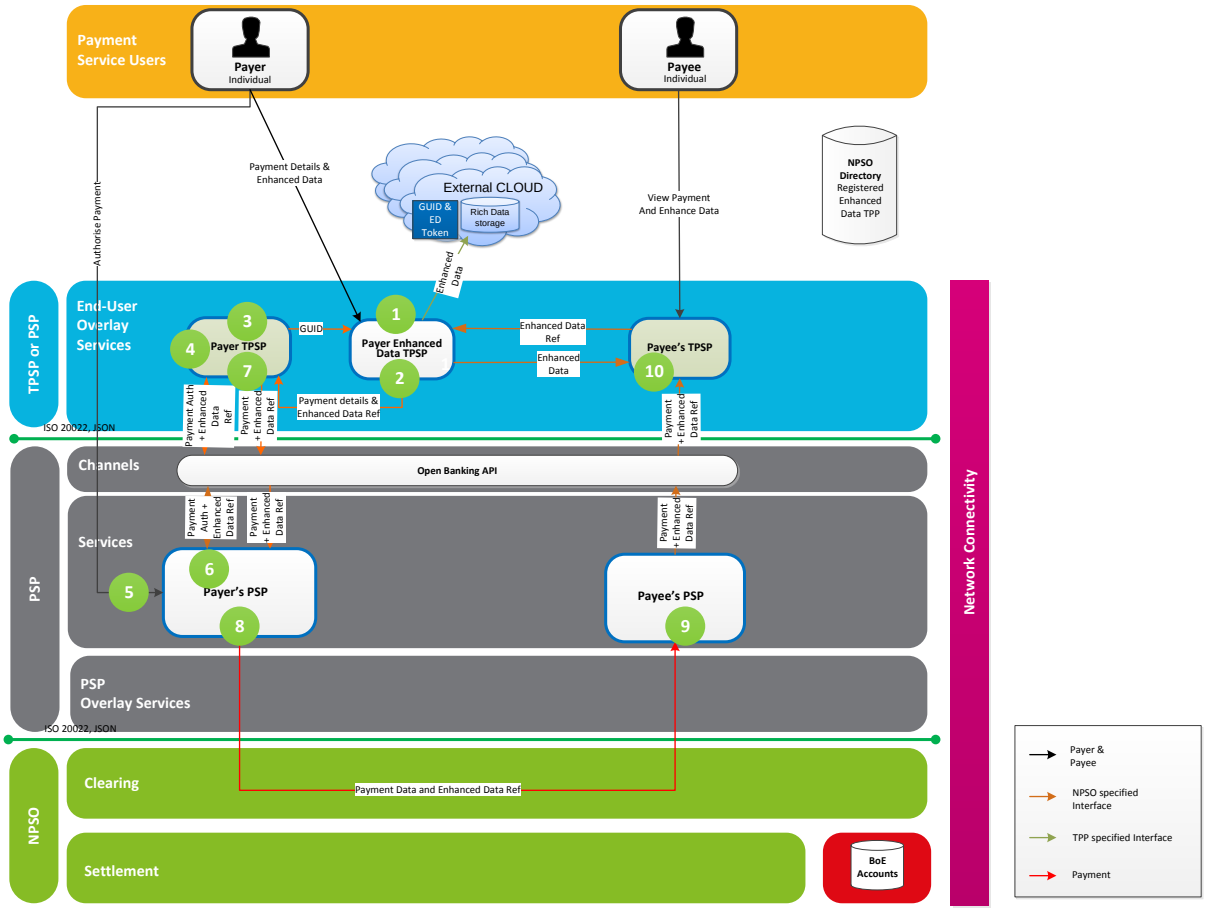
An enhanced data TPSP will:

- Authenticate and authorise the requester before providing access to enhanced data
- Maintain the required audit trails of the access provided with the associated security audit
- Fully comply with GDPR and ensure that access to enhance data will be as per the data regulations defined at a given point in time.

It is recognised that as enhanced data solutions are developed consideration will need to be given to the following areas:-

- Anti-Money laundering regulations and how these will include the vetting of enhanced data.
- Security standards around accessing the data.
- GDPR implications on the use of external data.
- Duration for which the data needs to be stored.
- Standards for data sent with payments to enable auto reconciliation.
- While HMRC has specified the minimum data required for e-invoicing, (See VAT Notice 700/63: electronic invoicing) the complete set of data will require further definition and agreement.

It is also recommended that the NPSO undertake consultation with service users to ensure that any proposed solutions will meet their requirements.



Key:

Figure 5.8 Potential Solution for Enhanced Data for payments

The main steps involved are:

Step 1: The payer's Enhanced Data TPSP receives payment instructions and Enhanced Data Unique Identifier from the payer.

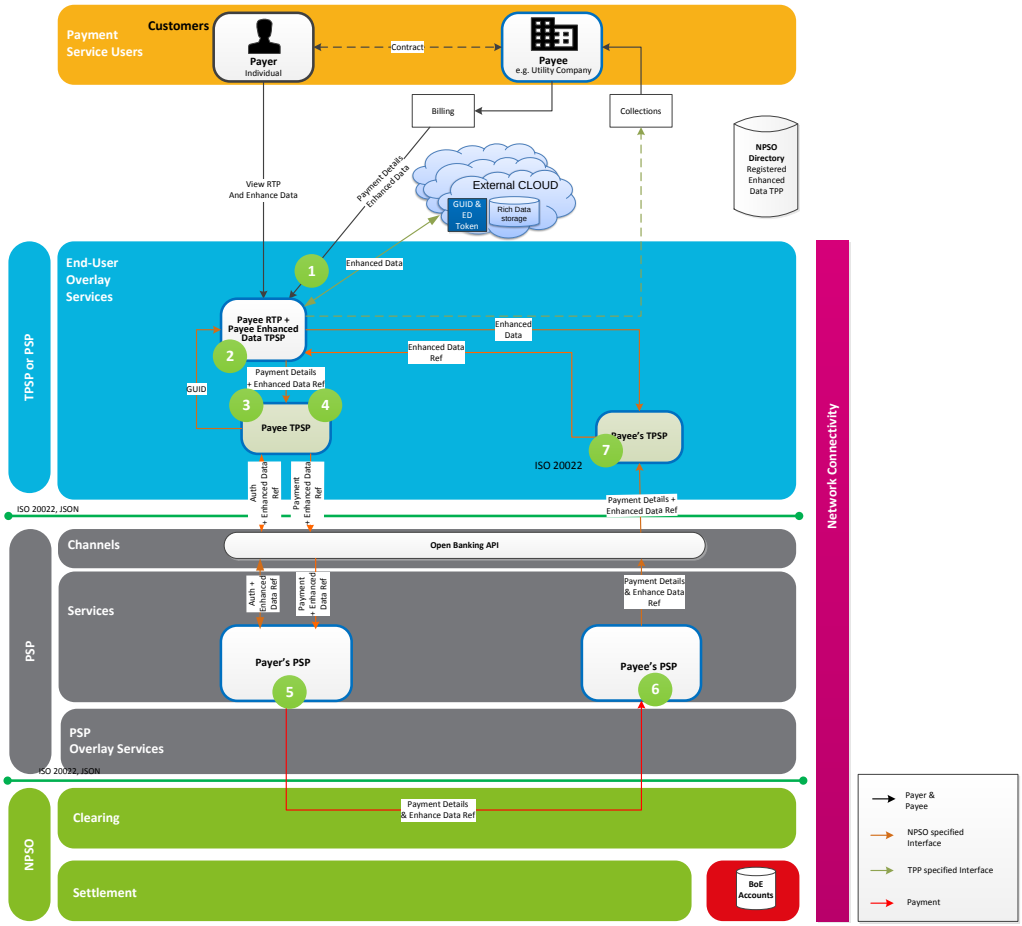
Step 2: The payer's TPSP stores the Enhanced Data items and sends the payment instruction including the Enhanced Data Unique Identifier to the payer's payment initiation TPSP.

Step 3: The payer's TPSP (payment initiation) sends the payment details (including the Enhanced Data Unique Identifier details) to the payer's PSP.

Step 4: The payer's PSP creates and sends the payment (with the Enhanced Data Unique Identifier details) for clearing and settlement.

Step 5: The payee's PSP receives the cleared payment (with the Enhanced Data Unique Identifier details) and sends them to the payee's TPSP.

Step 6: The payee accesses the cleared payment and Enhanced Data via their TPSP, which looks up the location of the payer's Enhanced Data TPSP from the directory and retrieves the Enhanced Data.



Key:

Figure 5.9 Potential Solution for RtP Enhanced Data

The steps below are only for the Enhanced Data solution and assume that the requests to pay steps still apply. As per the request to pay solution, the payer will still view and respond to the request to pay, which will include the Enhanced Data supplied by the payee. It is assumed that the Enhanced Data TPSP and payee RtP roles are performed by the same provider.

The main steps involved are:

Step 1: The payee's Enhanced Data TPSP receives payment details and Enhanced Data item/s from the payee's host system.

Step 2: The payee's Enhanced Data TPSP stores the Enhanced Data items and sends the payment details (and Enhanced Data reference details (e.g. Enhanced Data TPSP participant ID, document ID/s and ED token) to the payer's TPSP.

Step 3: The payer's TPSP generates a Globally Unique Identifier (GUID) and sends the GUID to the payer's 'Enhanced Data TPSP'

Step 4: The payer's TPSP sends the payment details (including the Enhanced Data reference details) to the payers PSP.

Step 5: The payers PSP creates and sends the payment (with the Enhanced Data reference details) for clearing and settlement.

Step 6: The payee's PSP receives the cleared payment (with the Enhanced Data reference details) and sends them to the payee's TPSP.

Step 7: The payee accesses the Enhanced Data reference via their TPSP, which looks up the payer's Enhanced Data TPSP from the directory and retrieves the Enhanced Data using the Enhanced Data reference from the cleared payment.

5.4.1 Enhanced Data Use Cases

E-invoicing

The figure below illustrates an example of how Enhanced Data could be used for e-invoicing.

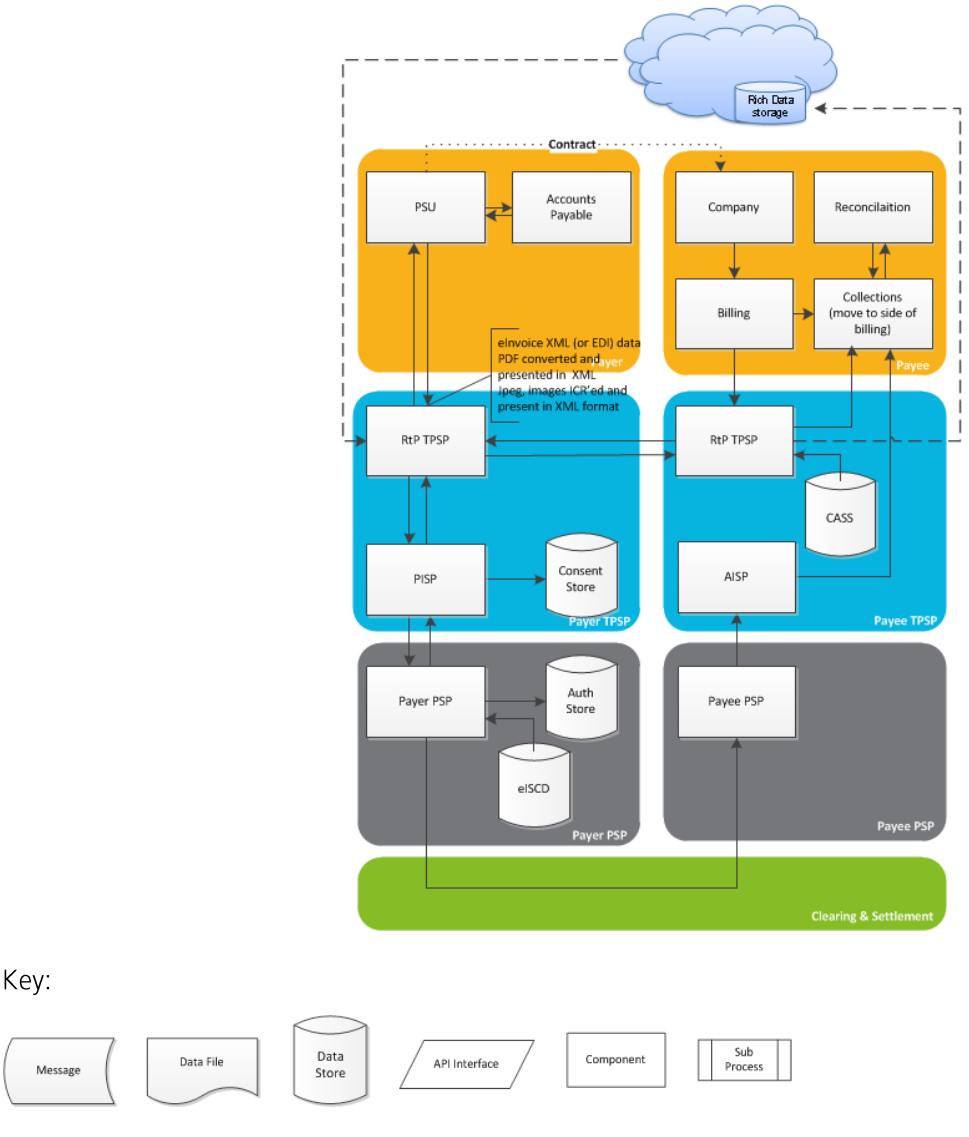


Figure 5.10 Illustrates use of Enhanced Data for e-invoicing

- The payer (company) enters into a contract with a payee (company) for execution/supply of a service and provides the details of his request to pay TPSP.
- On completion of the work, the payee sends a request to pay with the invoice as enhanced data.
- Storage of the invoice as enhanced data can be undertaken by the payee or the TPSP associated to the payee.
- On receiving the request to pay message, the payee's TPSP extracts the enhanced data and submits it to the payee. Where required, the data received is converted it into the format required by the payee.
- The e-invoice is routed to the payee's accounts payable for validation and payment without operator intervention.

- e-invoices approved are submitted for payment following the direct credit or single immediate payment model.

Auto-reconciliation

The figure below illustrates an example of how enhanced data could be used for auto-reconciliation.

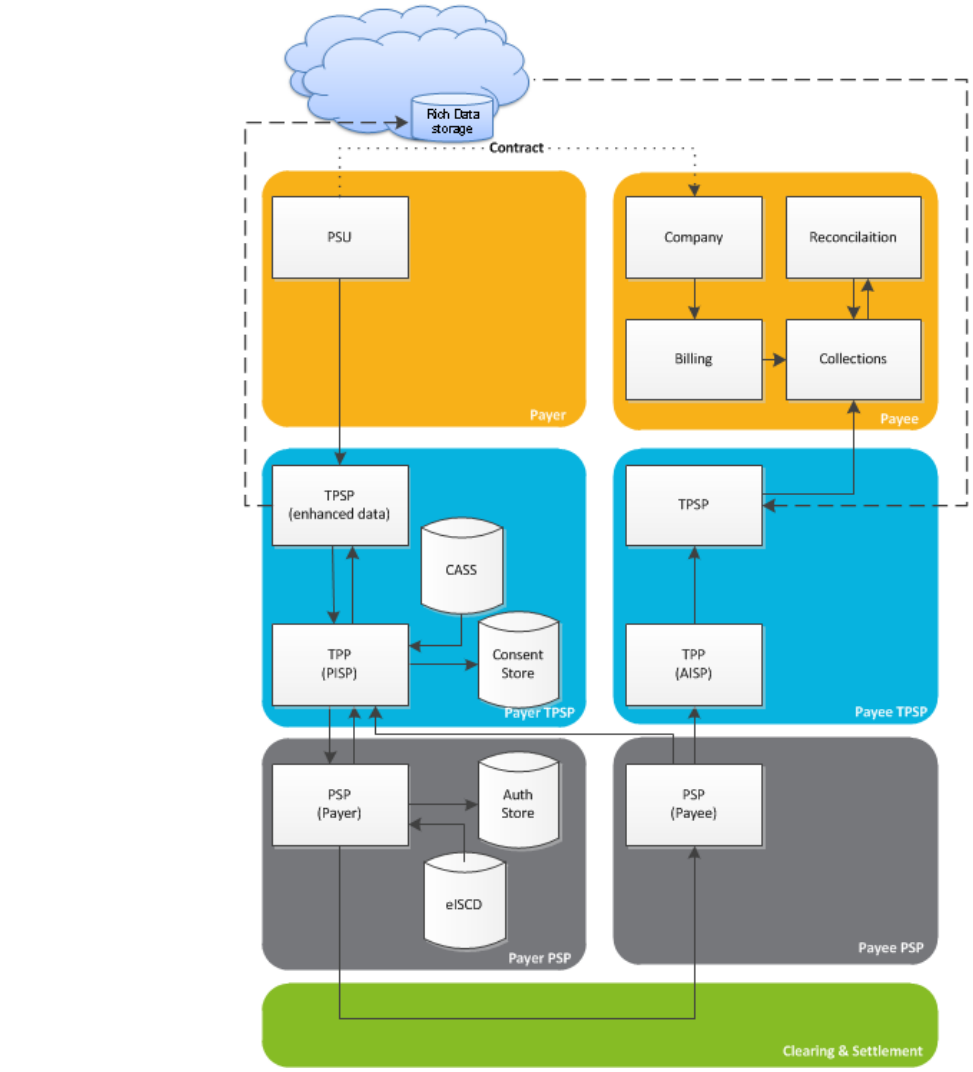


Figure 5.11 Example of how enhanced data could be used for auto-reconciliation.

- The payee or their TPSP stores additional details on the payment made as enhanced data.
- The payee's TPSP extracts the enhanced data and passes them in XML/EDI format along with the payment details to the payee.
- If the data supplied is not in XML/EDI format, they will be converted by the TPSP e.g. image files could use OCR to extract the data.
- The payee uses the additional data supplied for auto-reconciliation.

Enhanced data can also be used to provide basic supporting data such as providing credit information with the payment. Supporting data with enhanced data could work as follows:

- If the payment message data is in the form of a URL, then the URL to the data could be stored by the PSP as a link along with the customer's debit or credit information. When the customer requests additional details for the credit or debit the data could be extracted by the PSP and displayed to the customer.
- If the payment message data is a structured data, then the data could be made available for the user to download themselves. For benefit payments, this data could be used by the PSP to restrict what the funds are used for, for example.

6 Transition Approach

6.1 Introduction and Principles

In developing the transition approach, we have taken into account the PSR's recent market review report 'Ownership and Competitiveness of Infrastructure Provision'. The transition approach proposed is designed to ensure interoperability, continuity of service and minimal disruption.

In addition, the transition to the NPA must achieve the primary goal of ensuring that the migration does not introduce instability or excessive risks. To achieve this goal a number of transition principles have been established. The transition approach should:

- Be phased, as this is less disruptive to the market, reduces transition risk and the likelihood of failures and introduces a transitionary period that allows PSPs to develop or upgrade their systems over time.
- Keep transition periods as short as possible, without creating unnecessary risks to keep the costs low and reap the benefits as early as possible.
- Avoid detrimental impact on the integrity of UK electronic payments during the migration to, and adoption of, ISO 20022; avoid detrimental customer impact (across all customer segments) and avoid introducing uncontrolled risks.
- Facilitate the transition of PSPs from the current payment models to the NPA.
- Ensure that the current and new systems run independently of each other for clearing.
- Minimise the impact of the existing payment schemes during the transition.
- Permit an orderly and prompt closure of the existing schemes, to ensure optimal benefits realisation.

6.2 Options Evaluated

The following options for transition were considered:

6.2.1 All Receive 'Day 1' - Option 1 (Recommended)

All PSPs will be capable of receiving NPA transactions at the start of the transition period. The key features of this approach are:

- All PSPs will be able to receive the payments types as shown below in each of the listed transition states:
    - Single Payments at the start of transition state 1.
    - Bulk Payments at the start of transition state 2.
    - ICS transaction at the start of transition state 3.
- Sending of NPA transactions will be phased within each transition state by type of payment.

6.2.2 Phased Receive - Option 2

PSPs will be phased to send and receive NPA transactions. The key features of this approach are:

- PSPs will be phased to send and receive NPA transactions.
- PSPs are not expected to receive NPA transactions on 'Day1'.

The phased receive model was discounted as all the PSPs sending data from the new to old schemes will result in data truncation and development effort being expended for a limited benefit.

6.2.3 'Big Bang' Approach - Option 3

The key feature of the big bang approach is that each payment type is migrated as a 'big bang' on the same day. This model was discounted due to the inherent risk in adopting this approach and is against the recommendation in the PSR "Market Review into the Ownership and Competitiveness of Infrastructure Provision" report.

6.2.4 Recommended Transition Approach

Our analysis discounted a 'big bang' approach due to potential uncertainties around risk and stability. It also discounted a phased send and receive approach on the grounds that there are additional complications of sending data between the NPA and the current payment systems that would result in data truncation and create the need for too many disposable transition development states.

The analysis led to the conclusion that all participants should be able to receive SIPs on the day of the NPA launch ('Day 1'), resulting in Option 1 being recommended as the preferred approach. The approach outlined above, which relies on all PSPs being ready on 'Day 1', has been adopted by the Image Clearing Service (ICS) and is considered to best meet the requirements as set out.

6.3 Phasing Overview

We have defined four transition states for the phasing in of the NPA. Together they will deliver a successful implementation of the NPA and migration of legacy payment volumes, as well as subsequently ensuring that existing scheme processing capability can be closed down.

The phases use a series of architectural positions known as transition states to describe the particular layers and components that need to be delivered to provide the functionality described within each state. Further detail on each of the transition states and what each will mean to end-users can be found in the Implementation Plan document.

Along with PSP participants being able to receive SIPs on the day of the NPA launch ('Day 1'), it is also a requirement that directory services have been implemented and that the relevant capability in the BoE RTGS system is also available. The implication of this approach is that PSPs may need to run existing, as well as new, payment systems in parallel and cover such setup costs until the old payment scheme is shut down.

The four proposed transition states are as follows:-

- Transition State 1: Single Payments (all PSPs capable of receiving SIPs):
  - Phase 1: sending of SIPs.
  - Phase 2: sending forward-dated payments.
- Transition State 2: Bulk Payments (all PSPs capable of receiving bulk payments):
  - Phase 1: sending of bulk payments – Bacs, direct credit, direct corporate access and Standing Orders.
  - Phase 2: sending payments for Direct Debits.
- Transition State 3: Image Clearing System:
  - Phase 1: Processing of credits (transit credits received with on-us debits).
  - Phase 2: Processing of cheques (transit cheques receive with on-us or transit credits).
- Transition State 4: Close down of legacy services completed (a parallel activity aligned to the status of the other transitions).

The first three transition states will coincide with the delivery of the layers of the NPA. The final fourth transition state will coincide with the close down of the existing infrastructure once all payments have migrated to the NPA. This process is expected to start with FPS.

Please refer to the NPA Implementation Document for the updated NPA timelines.

6.4 Transition States

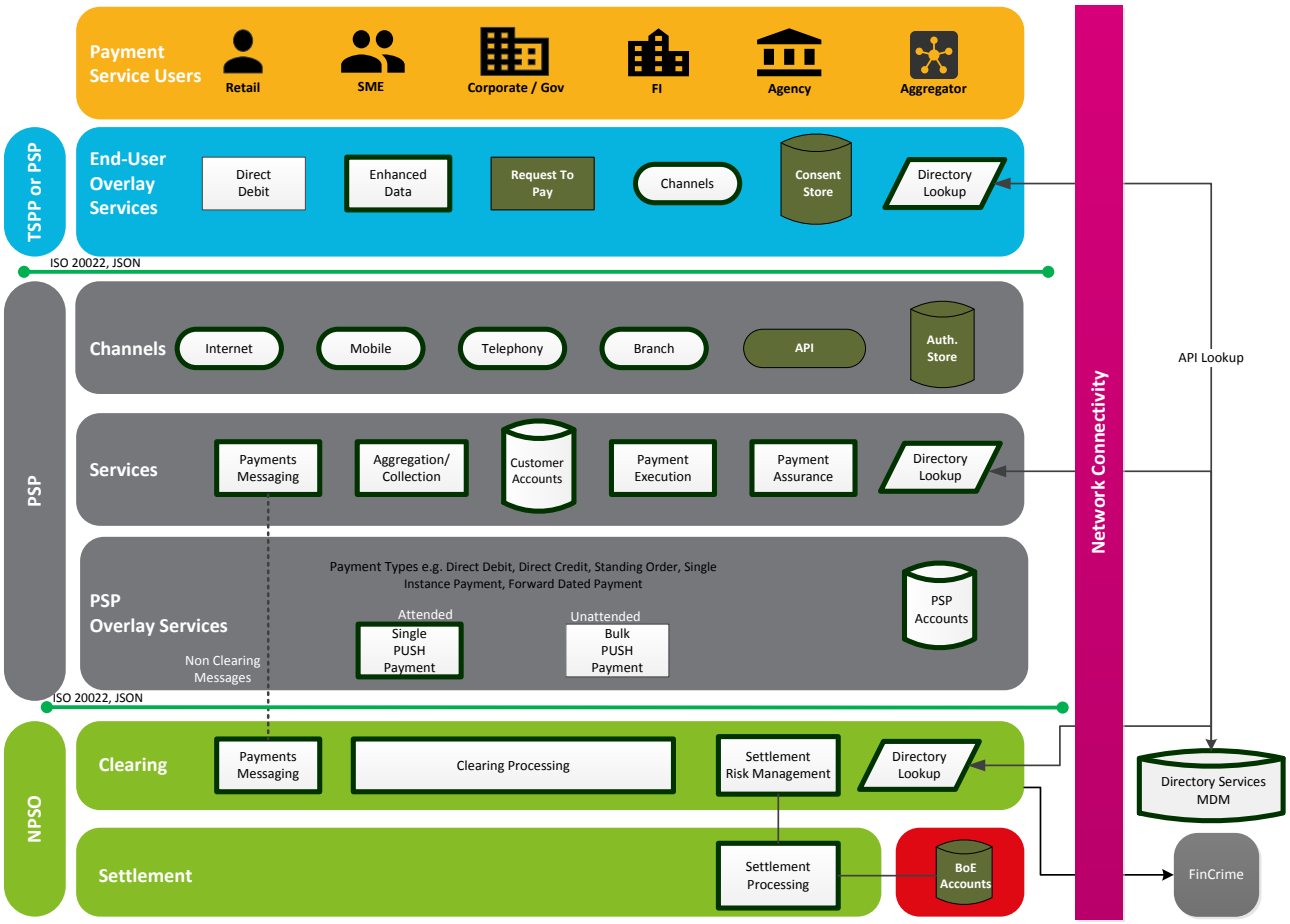
With the on-going industry initiatives, the following features are expected to be implemented before commencing NPA transition:-

- Relevant capability being available within the BoE RTGS system or equivalent which provides:
    - Single settlement account for each participating PSP.
    - Liquidity available for each payment scheme apportioned from the PSP's funds maintained in BoE.
- Open Banking APIs in use.
- TPSPs or PSPs Request to Pay and Consent Store deployed.
- PSP authorisation store is live.
- Existing services such as CASS, Bulk redirection etc. are in place.

Note: If the above features are not implemented prior to NPA, it is expected that the implementation will take place within Transition State 1.
The dark green boxes in the following diagrams indicate the components of the NPA that are required to be functional to support each of the transition states.

6.4.1 Transition State 1 – Attended (Single) Payments

For the first transition state, all PSPs must be capable of receiving attended single payments.



Key:

Figure 6.1 NPA Components: Transition State 1

Receiving attended (single) payments - In addition the following components are required to be implemented at the start of Transition State 1:

- NPSO
  - Payment messaging
  - Clearing processing
  - Settlement risk management and settlement processing
  - Directory services e.g. routing including CASS, participant and payment reference
- PSP
  - PSP Account
  - Payments Messaging
  - Aggregation/Collection
  - Customer Account
  - Payment Execution

The sending of new SIPs will be migrated in phase 1 followed by the sending of forward-dated payments in phase 2.

Sending attended (single) payments - In addition to the components implemented for receiving single payments, the following components are required to be implemented for sending single payment messages:

- TPSP or PSP
  - Channels
  - Directory lookup
  - Enhanced data
- PSP
  - Single push payment
  - Tracking of payments as a part of Payment Assurance.

6.4.2 Transition State 2 - Unattended (Bulk) Payments

For the first transition state, all PSPs must be capable of receiving unattended payments.

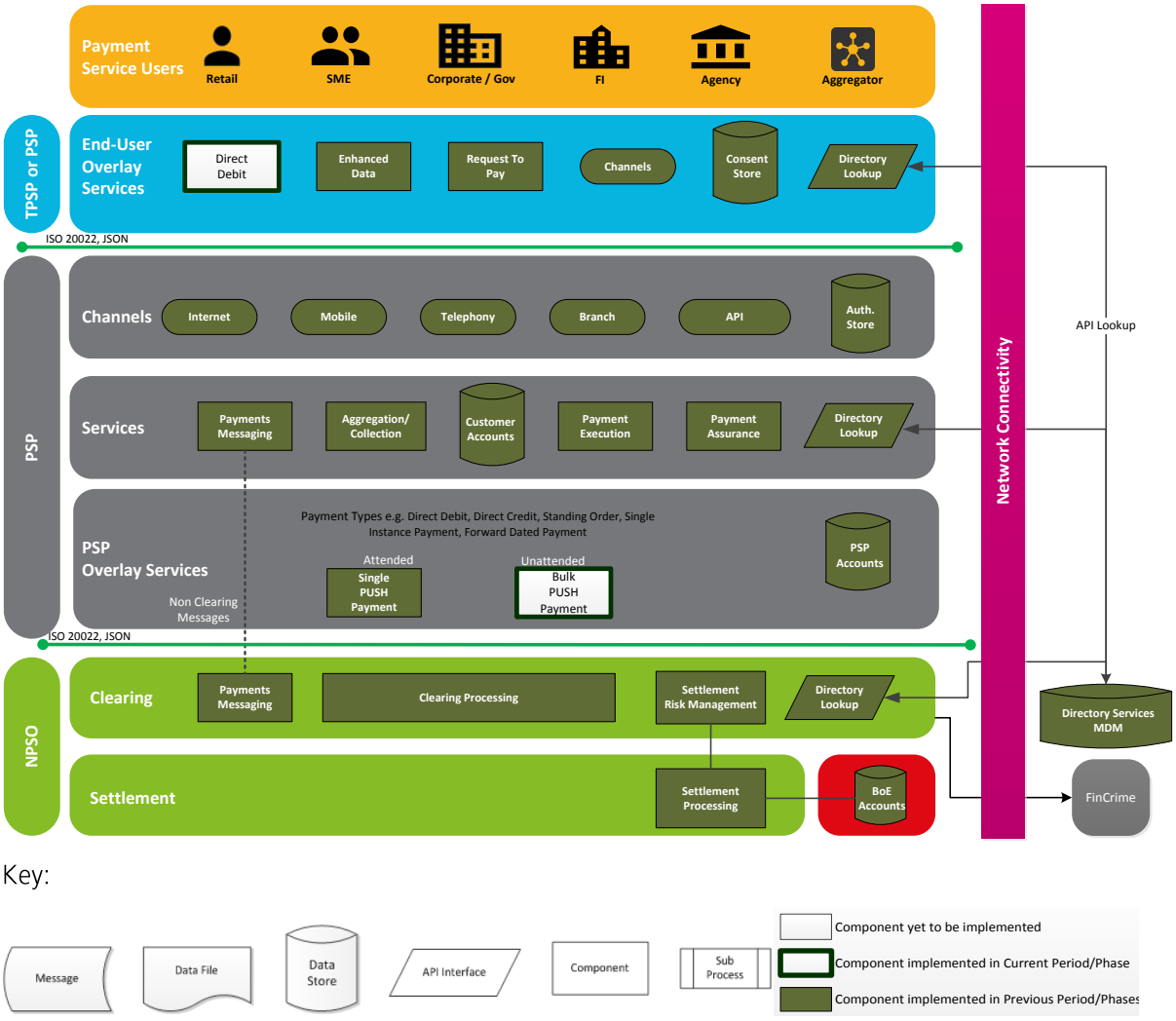


Figure 6.2 NPA Components: Transition State 2

Receiving unattended bulk payments:

Other than the components implemented in the previous phases, there are no additional components required for receipt of bulk payment. Sending of unattended payments will be implemented in phase 1 with the sending of Direct Debit payments taking place in phase 2.

Sending unattended bulk payments:

In addition to the components implemented in the previous periods, the bulk push payment and Direct Debit components are expected to be implemented to enable the sending of bulk payment messages.

6.4.3 Transition for Direct Submitters

During Transition State 2, corporates, FI and the government who submit work directly to Bacs and FPS will be required to migrate to NPA. In order to minimise the impact on direct submitters, there will be no requirement for them to change their existing file. As a transition solution, these files will be sent to a TPSP (similar to sending them to a bureau service, Bacstel-IP or direct corporate access) who will complete the pre-processing, for example, disaggregating the file, changing the format to ISO 20022 etc., before submitting the file to clearing and settlement for Direct Credits or to the payer's TPSP for Direct Debits.

6.4.4 Direct Credits

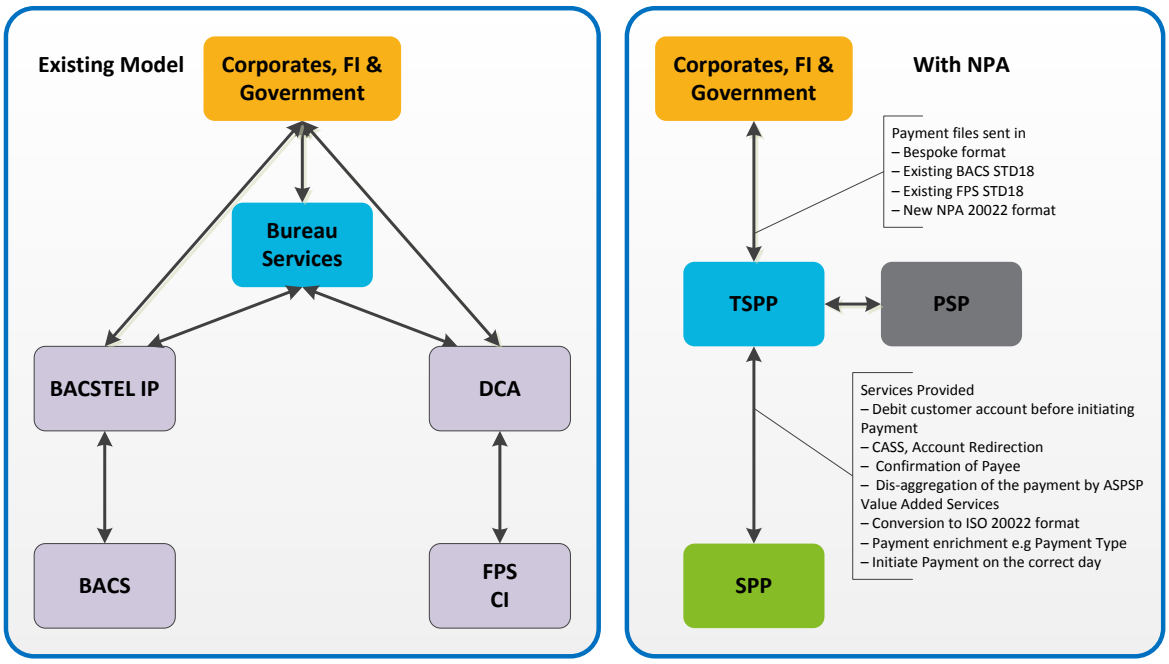


Figure 6.3 NPA Components: Transition – Direct Credit Submitters

Direct Credit files will be submitted in their existing format to the TPSP. The TPSP as a part of their service will perform:-

- Confirmation of Payee (where required).
- CASS Account redirection.
- Disaggregation of the file by PSPs.
- Convert the data into ISO 20022 format.
- Enrich the data where required e.g. include the type of payment.
- Initiate the payment on the correct day.
- Secure funds before initiating the payment.

6.4.5 Direct Debits

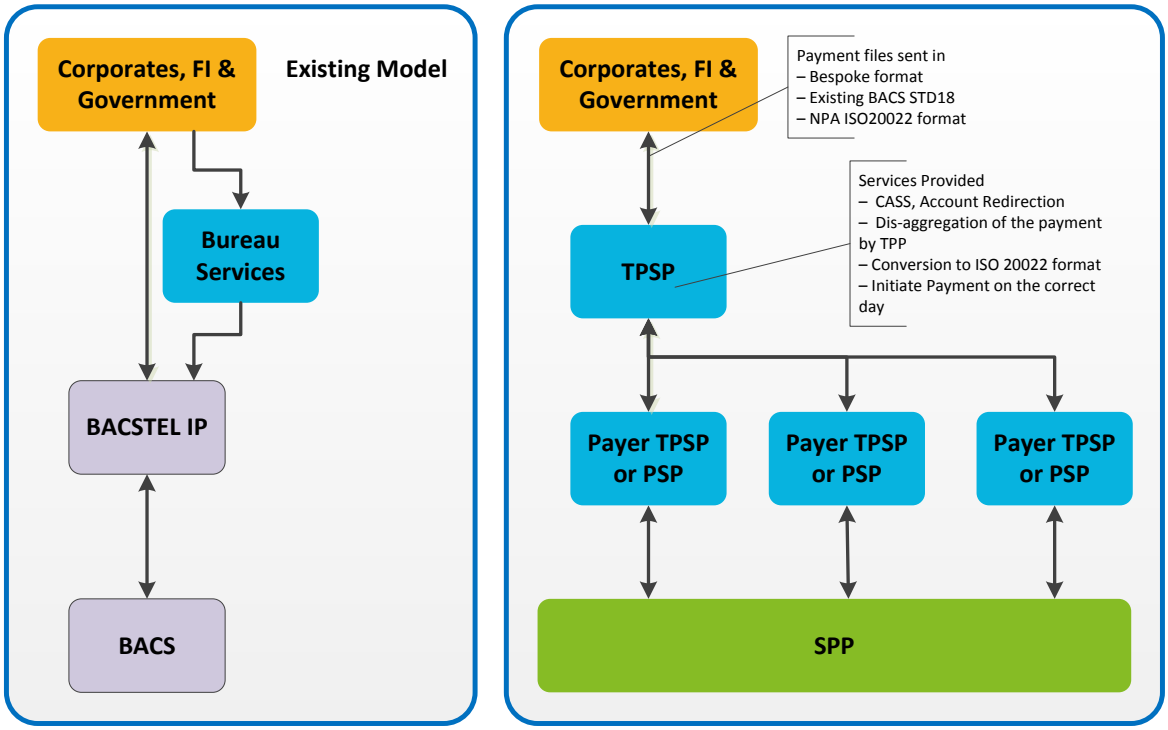


Figure 6.4 NPA Components: Transition – Direct Credit Submitters

Direct Debit files will be submitted in their existing format to the TPSP. The TPSP as a part of their service will perform:-

- CASS Account redirection.
- Disaggregation of the file by payer TPSP or PSPs.
- Convert the data into ISO 20022 format.
- Initiate the payment on the correct day.
- Secure funds before initiating the payment.
- Reconcile the payments received.

Migration to ISO 20022

The direct submitters have the opportunity to adopt the ISO 20022 file format in order to provide additional information i.e. enhanced data that is not supported in the current file format. Adopting the ISO 20022 file format could be implemented during or after a transition period. Similarly, there is no requirement to change the existing Direct Debit Instructions (mandates) during the transition period. Adopting a new Direct Debit Instruction approach for payer verification could be implemented during or after the transition period.

6.4.6 Transition State 3 – ICS

All PSPs must be capable of receiving ICS Payments at the start of this transition state.

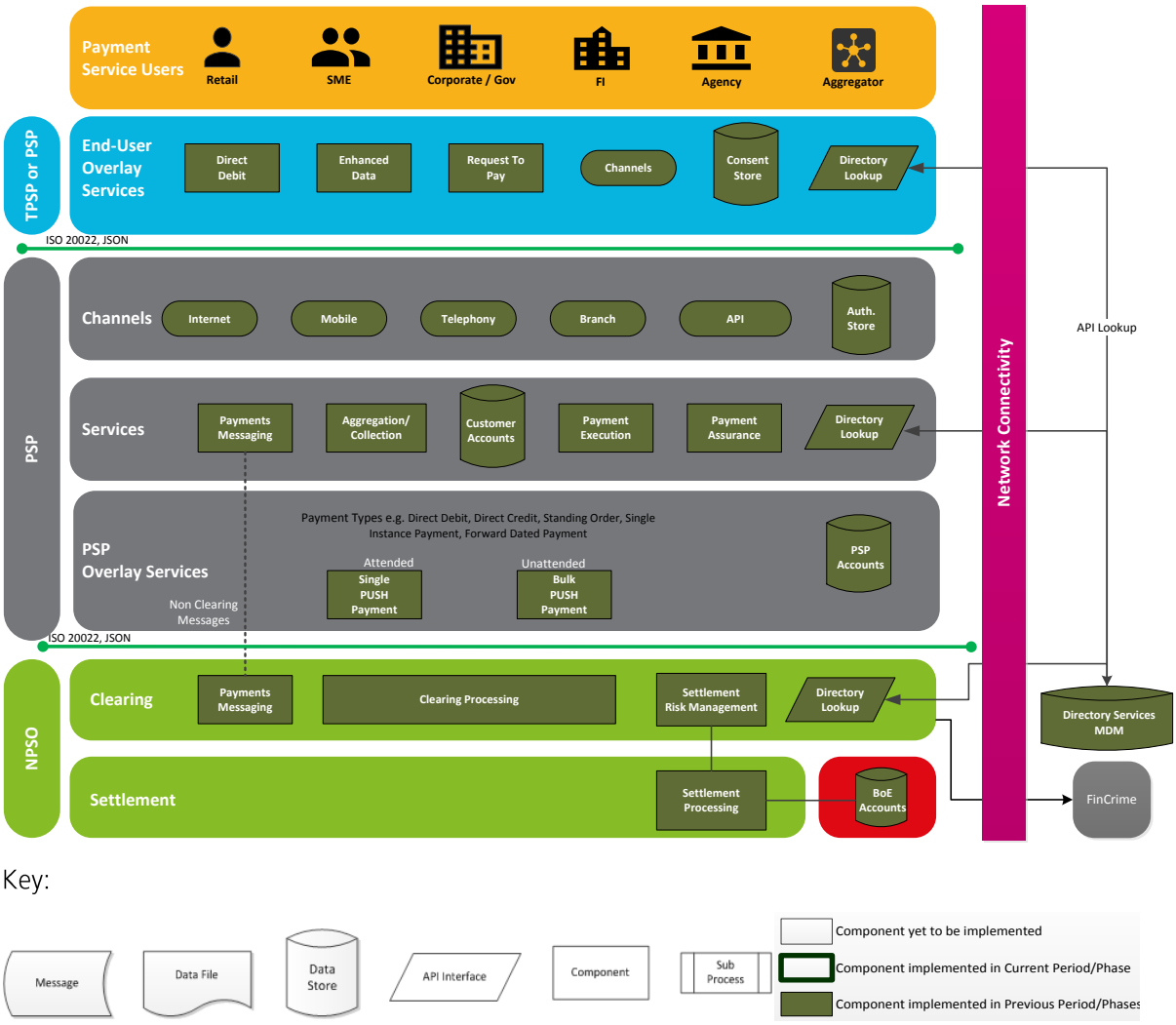


Figure 6.5 NPA Components: Transition State 3

Receiving ICS Payments: Other than the components implemented in the previous phases, there are no additional components required for receipt of an ICS payment.

Migrating ICS Payments: Processing of credits, i.e. transactions that contain an interbank credit with cash, electronic or on-us cheques will take place in phase 1 with the processing of cheques and credits i.e. all the types of transactions occurring in phase 2.

Sending ICS Payments: In addition to the components implemented in the previous phases, sending of ICS transactions would require ICS messages being transferred between the payer's TPSP and the payee's TPSP.

6.4.7 Transition State 4 – Closedown

Transition state 4 is the final state when legacy systems are closed down as the NPA will be fully operational and transactions from all the payment schemes will be being processed through the NPA. Decommissioning of the existing schemes will be progressed to completion. While this is the final stage, decommissioning will commence as soon as the traffic has been migrated to NPA from a particular scheme resulting in some of the schemes being decommissioned before this phase.

6.5 Optional Consideration

During transition state 1, if we do not have sufficient PSPs sending NPA transactions, a migration service could be implemented to re-route the FPS SIPs to NPA. The migration service could run in the FPS central switch or within PSPs infrastructure.

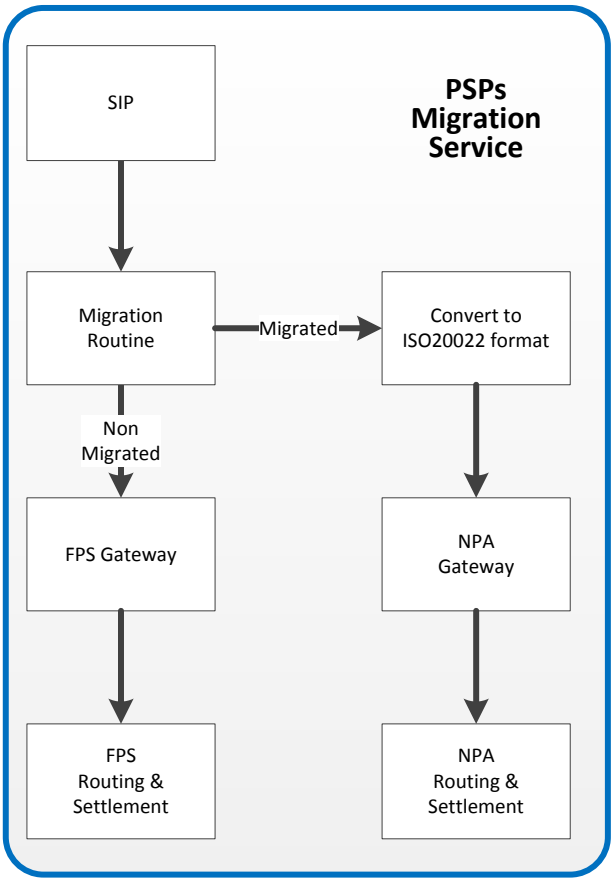


Figure 6.7 Potential PSP Migration Service

Example of a migration service within PSPs.

The suggested migration service within PSPs would intercept SIP transactions and route the migrated transactions to the NPA gateway. These transactions will have a cut down version of the NPA data. Non-migrated transactions would continue to be routed to the FPS gateway, as in the current model.

7 NPA Participation

7.1 Participation Model

The NPA design has adopted three recognised types of participants for organisations that are involved in the initiation of payments. The following engagement models have been developed using these definitions:-

Direct Settling access	Direct Non-Settling access	Indirect access
• BoE Settlement Account is mandatory. • Direct technical connection to the NPA infrastructure. • Mandatory to receive payments 24x7. • Expected to offer send payment capability 24x7. • Funds authorised prior to submitting transactions to clearing (as per the current model). • Liquidity and Risk management tools required.	• Bank of England settlement account is not required – settlement provided by the Direct Settling Participant acting as a sponsor PSP. • Direct technical connection to the NPA infrastructure. • Mandatory to receive payments 24x7. • Expected to offer send payment capability 24x7. • In the NPA model, funds will be authorised by the PSP before submitting the transactions to clearing.	• Bank of England settlement account is not required – settlement provided by the Direct Settling Participant acting as a sponsor PSP. • No direct technical connection to the NPA infrastructure – the technical connectivity is between the indirect participant and their sponsor PSP. • Fully reliant on the NPA service offering to the sponsor PSP. • Not mandatory to receive or send payments 24x7.

Table 7.1 Participant Role Definitions

The reference to 24x7 in the table above relates to clearing and not settlement functionality.

NPA participants can use any of the participation models mentioned provided they can meet the criteria mentioned.

Direct Non-Settling access participants can also be called a connected non-settling participant and indirect access participants can be called non-connected non-settling participants.

7.2 Depiction of Participation Models

7.2.1 Direct Settling Participant – PSP

PSPs that are eligible to hold a settlement account with the Bank of England can build their own connectivity to the clearing and settlement or SPP layers or they can work with the multiple connectivity providers or technical aggregators that are expected to be available to them.

It is envisaged that PSPs may wish to implement their own payment initiation and account aggregation capability. It is assumed that PSPs capability will meet the required interoperability standards as determined by the regulator and the NPSO.

A PSP could, if required, sub-contract the delivery of payment initiation and other TPSP capabilities to a third party if they did not want to build their own capability.

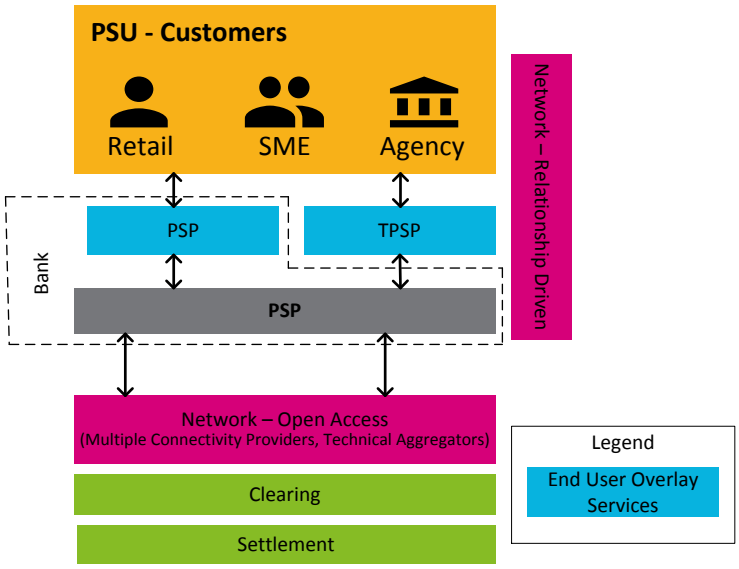


Figure 7.1 Direct Settling Participant

7.2.2 Direct Non-Settling Participant - Agency, Financial Institution or PSP

In this scenario, an agency PSP, financial institution or PSP has decided to connect directly with NPA but not to self-settle. Taking this approach would mean that they would be reliant on a sponsor (PSP) to perform settlement and to set NSCs. The sponsor (PSP) would have to be a direct settling participant of the SPP as described above.

A PSP could, if required, sub-contract the delivery of payment initiation and other TPSP capabilities to a third party, or rely on their sponsor if they did not want to build their own capability.

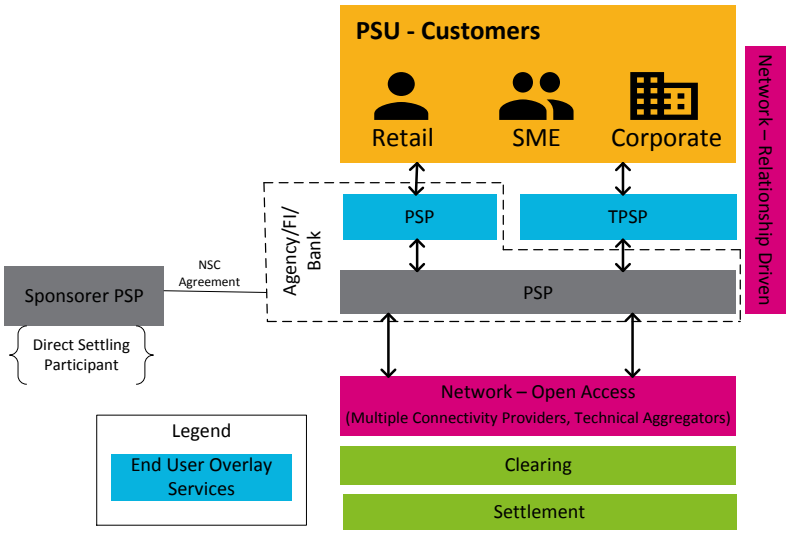


Figure 7.2 PSP Non-Direct Settling Participant

7.2.3 Direct Submitters - Corporate Government and Financial Institutions

Today, Government, financial institutions and some corporates use Bacstel-IP software to submit payment files directly to Bacs Central Infrastructure. The Bacs Central Infrastructure carries out the payment routing and initiates the debit request to the payer's PSP. Bacs makes use of a corporate level cap to then clear the funds on Day 3 following the submission.

Between now and the delivery of the NPA there are a number of industry and regulatory initiatives that will require changes to be made with the current payments infrastructure such as the mandating of ISO 20022 and the need to provide additional payments message data under the Fourth Money Laundering Directive.

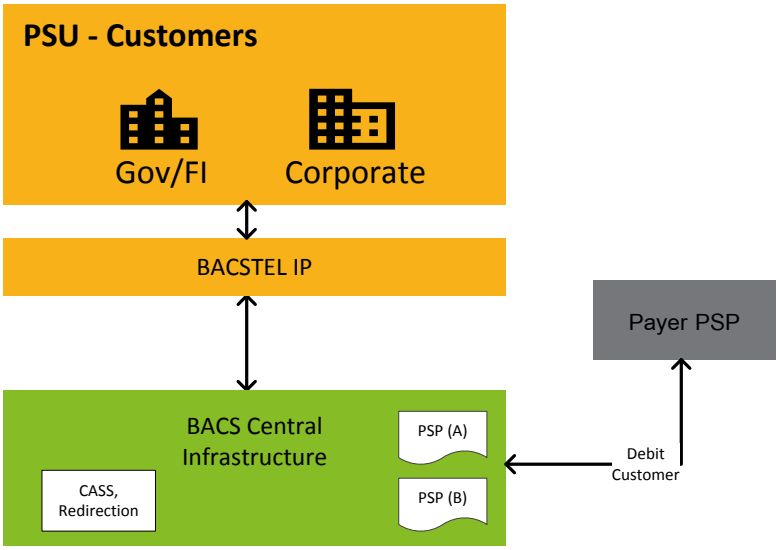


Figure 7.3 Current Bacs Flow

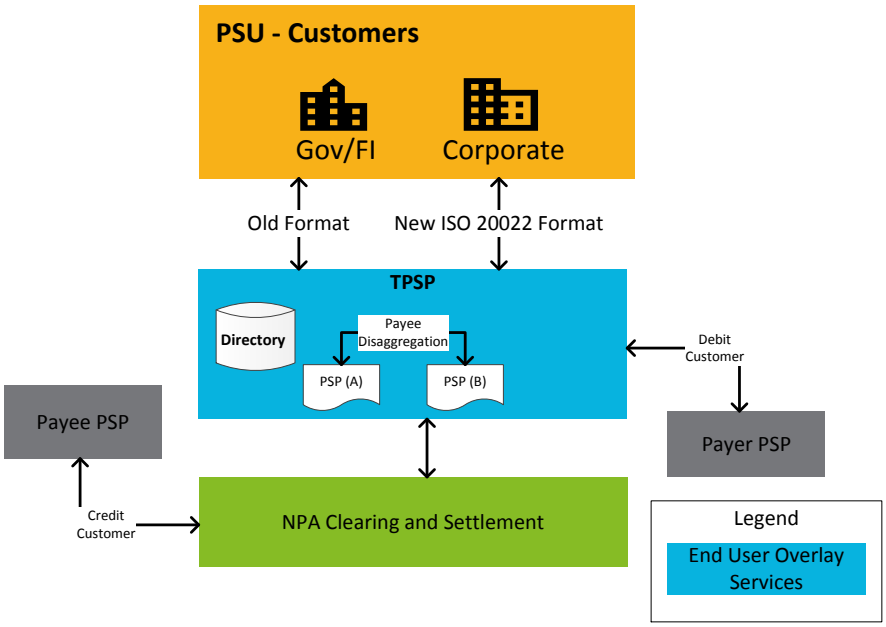


Figure 7.4 Direct Submitter – Bacs Direct Credit flow

Corporates, financial institutions and Government currently can submit direct payment files which contain direct credits (push payments) as well as collection (pull payments) request. With the NPA the clearing layer will support push unattended (bulk) payments using singular clearing processing (detailed in Section 2.1.6)

Taking this participation approach would mean direct submitter for Bacs Direct Credit payment type will have to use a TPSP (or PSP) to submit files to the NPA clearing layer. The TPSP will be required to provide the following functionality before submitting the payment file to clearing:-

- Directory Services – CASS, account redirection.
- Confirmation of Payee (Payment Assurance).
- Dis-aggregation of the payment file by payee PSP
- Optionally they may offer value-added services to enable transition such as:
    - Provide a conversion service to ISO 20022 from the old messaging format
    - Provide a payment enrichment service such as adding payment type.

For Bacs Collection (Direct Debit – DD) payment type, direct submitters will continue to generate their collection file (e.g. utility bills, council tax) as they do today and pass it to the TPSP. The remainder of the process flow is similar to the DD collection process detailed in Section 4.1.2.

The types of organisations that might offer direct submission services are believed to be a matter for further post consultation exploration as at one level they can be easily offered by multiple entities (as competition in the market) or conceivably by the NPSO (as a market catalyst or competition for the market).

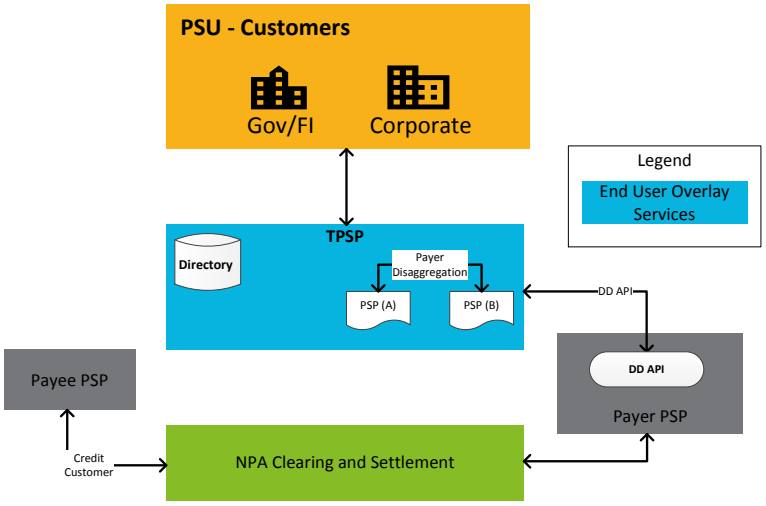


Figure 7.5 Direct Submitter– Bacs Direct Debit flow

8 Appendices

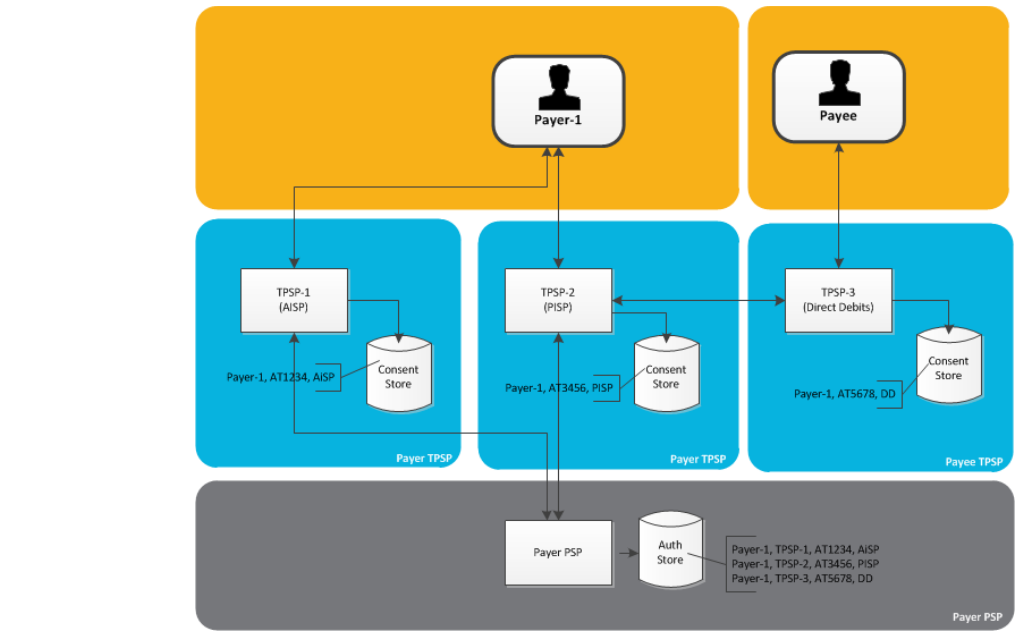
8.1 Appendix 1: Consent & Auth Store Definition

TPSPs require authorisation to perform the following for a PSU:

- Payment initiation
- Access to customer data
- Direct Debit collections

These authorisations are normally provided by the PSU logging into their PSP account with their secure credentials and authorising the TPSP's authorisation request (e.g. via a mobile banking app).

The authorisations provided by the PSU will be used to create a unique security token 'auth token' by the PSP. This unique authorisation token is stored in the PSPs Authorisation (Auth) store and the initiating TPSPs Consent store. Any subsequent transactions carried out by the TPSP on behalf of the PSU should carry this 'auth token' for the PSP to act on the request.



Key:

Figure 8.1 Consent and Auth Store Interaction

The diagram above shows how the authorisation token could be stored in the PSPs Auth store and the TPSP consent store. However, implementation of this could differ in each TPSP/PSP.

Authorisation (Auth) store

The authorisation store is held in the PSP and it holds the unique security tokens created when a payer authorises a TPSP to perform a specific function. Some of the details that could be stored in the Auth store depending on the authorisation type are:

- Customer details – Sort code and account number

- Authorisation type – PISP, AISP, Direct Debits etc.
- TPSP details – TPSP ID
- Authorisation token
- Authorisation date
- Authorisation valid date range
- Payee Details – Sort code, account number, name etc.
- Authorised amount
- Maximum amount of Single payments
- Amount range for Direct Debits etc.

Consent store

Consent store is held by the TPSP and it holds the 'auth token' created by the PSP for its PSU. The details stored in the consent store are similar to that of the Authorisation store.

Payment

For a TPSP to execute a payment or access the customer account details, they should have a valid 'auth token'. When the TPSP initiates a payment or request access to the customer account details, the 'auth token' for the transaction is retrieved from the TPSP's consent store and included with the request sent to the PSP. The PSP verifies the 'auth token' received against the 'auth token' in its 'auth store' and only processes the request that has a valid 'auth token' and the request conforms to the parameters associated with the token i.e. the amount is in the specified range, the beneficiary details are the same etc.

8.2 Appendix 2: JSON – XML Options

Below are a set of initial options that may be taken into consideration by the NPSO when determining their JSON and/ or XML policy. It is recommended that, as a minimum, the following assessment criteria should be considered:-

- Ease of 'connection to the NPA' (low technical barriers to encourage competition) and with it the ability to provide innovative services.
- End-to-end interoperability – ensuring that data is interpreted in the same way (e.g. RTGS uses SWIFT messages and it is XML based)
- Network and processing implications (e.g. protocol, volumetrics and capacity)
- Stability/maturity of the data format standard (inc. security standards)
- Existing Infrastructure and Investments and the ability of vendors to support NPA requirements

Option	Pros	Cons

Option 1: JSON as data format across all layers	• Open Banking supports JSON
	• Developer friendly
	• REST/JSON aligns well technically
	• Consistent syntax across the layers
	• JSON is (potentially) the future direction of travel
		• Standard maturity of JSON is low
		  • Multiple standards, OB has gone with one
		  • Security standards are considered as low
		• JSON is not commonly used in the clearing layer

Option 2: XML as data format across all layers	• Consistent syntax across the layers
	• XML is a mature standard
	  • Security
	  • ISO20022 definitions
	• Very prevalent in the Clearing layer
		• Open Banking supports JSON
		• JSON is (potentially) the future direction of travel
		• XML is not commonly used in APIs, developers have moved/ are moving on to JSON

Option 3: JSON or XML as data format across all layers	• Provides flexibility	• More standards to maintain • Difficult to govern • Increases complexity of the ecosystem
Option 4: JSON for top layers and XML data format for Clearing and Settlement layer	• Tries to strike a balance based on the syntax acceptance	• Not aligned with future direction of travel for around the more widespread adoption of JSON
Option 5: JSON for top layers and XML or JSON for Clearing and Settlement layer	• Tries to strike a balance based on the syntax acceptance • Allows the Clearing layer to evolve over time to industry acceptable syntax	• Potentially more standards to maintain • Increases complexity of the clearing and settlement layer (slightly)

Table 8.1 JSON and/ or XML Options

8.3 Appendix 3: Payment Flows & APIs

8.3.1 Payment Flows

Introduction

This appendix shows how the following payment flows could work across the NPA design, as set out in this document, and the APIs/messages required to support them:-

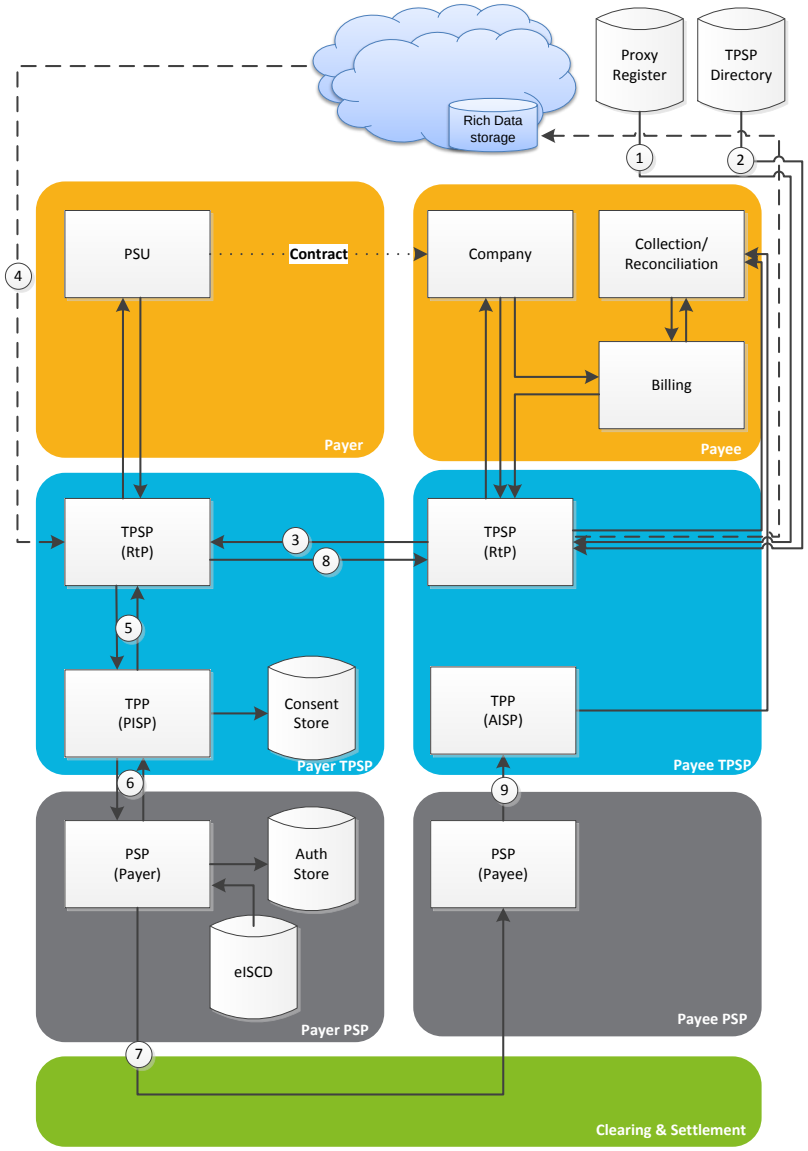
- Request to Pay (RtP).
- Single Immediate Payment.
- Direct Debit Instruction (DDI)
- Direct Debit Collection
- Direct Credit
- Standing Order setup
- Cheque Clearing
- Paper Credit (BGC) clearing
- Refund Requests

In the following descriptions, a TPP is used to describe a TPSP that may conceptually deliver functions governed by PSD2 (e.g. AISP & PISP) and a TPSP is a Third Party Service Provider involved in delivering NPA related functions that are likely to be accredited by the NPSO. Under the NPA TPSP capability can be delivered by any suitably regulated organisation (e.g. a PSP) and as such are functions not tied to just third party organisations.

It should be noted that further work, led by the NPSO, is required to establish the appropriate level of regulatory control required for TPSPs that are engaged in delivering certain functions within the NPA. It is expected that all TPSPs will operate under a governance scheme set out by the NPSO.

It is also recognised that the next phase of requirements gathering work, to be carried out by the NPSO, may impact the final API requirements and catalogue for the NPA.

8.3.2 Request to Pay



Key:

Figure 8.2 Request to Pay – Payment Flows

Interfaces

Request to Pay Interfaces			
Name	**Description**	**Type**	**Source**
1. Proxy registry Interface	To get the payers TPSP and account details	API	New
2. TPSP Directory Service	To get the list of RtP service providers	Directory Service	New
3. RtP Message	RtP message to the payer RtP	API	New
4. Enhanced Data Extract	To extract enhanced data from cloud storage	API	New
5. Payment Initiation to PISP	Payment initiation request to PISP	API	New
6. Payment Initiation to PSP	Payment initiation request to PSP	API	Open Banking
7. Payment Initiation	Single Immediate payment	File	New
8. RtP Response	Response to the RtP request	API	New
9. Account Information	To get account transaction details from the PSP	API	Open Banking

Table 8.2 Potential Request to Pay Interfaces

Solution Overview

A potential solution for Request to Pay (RtP) is as follows:

Step 1: The payer enters into a contract with the payee and provides their TPSP, sort code and account number details using one of the following options:

- Telephone number, email etc. – These details will be checked against the proxy registry to identify the payer's TPSP, payer sort code and payer account number.
- QR codes – Scanned QR codes will identify the payer's TPSP, payer sort code and payer account number.
- The payer enters or selects the TPSP from a list provided. The list of TPSPs will be retrieved from the RtP TPSP list stored in the directory services for validation or display.

Step 2: The payee initiates the RtP Request and passes this on with the appropriate information to their RtP TPSP.

Step 3: The payee TPSP stores the supporting documents in cloud storage with a token. The TPSP then creates a RtP message and sends it to the payer's TPSP.

Step 4: Upon receipt of the RtP message, the payer's TPSP submits the request to the payer for their approval. If the payer wishes to see the supporting document, it can be extracted from cloud storage and displayed to the payer by their TPSP.

Note: The RtP message could be sent to the payer as a QR code via email/post and the payer could use the RtP TPSP app to scan the QR code to make the payment.

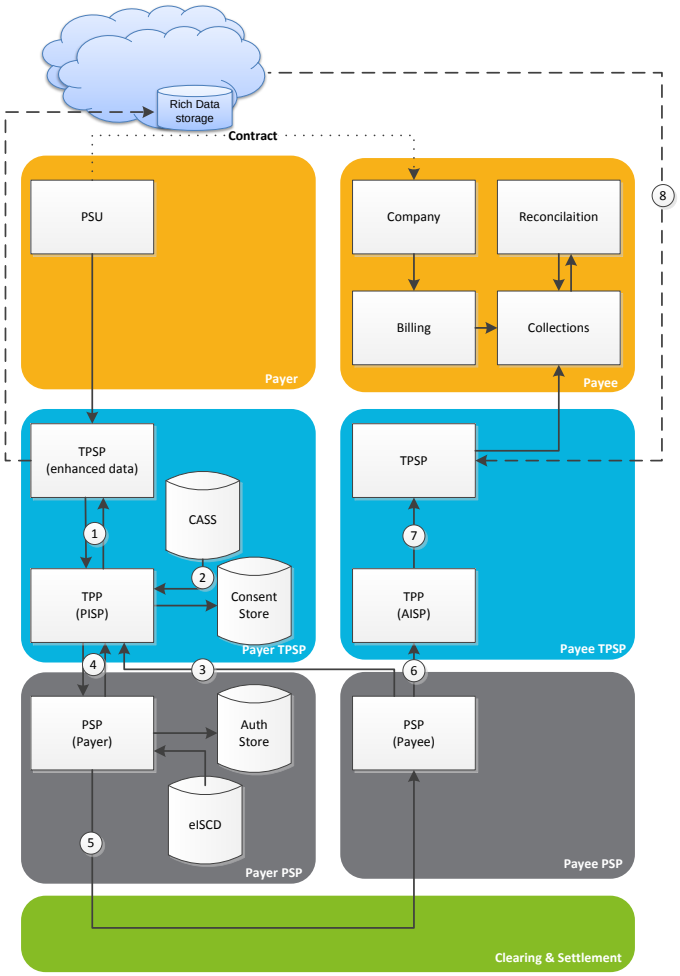
Step 5: The payer could choose to pay, pay partial or pay none and request the payee to contact them. In addition, the payer may be able to choose to specify the date of the payment.

Step 6: If the payer intends to make a payment (full or partial), the payment process will be initiated:

- The payer could then be redirected to their online PSP via the PISP where they are required to log into their account with their secure credentials.
- The payer's PSP will authorise the payment and create an authorisation token which will be stored in the authorisation store.
- If the payment is for the same day, the payer's PSP will initiate the payment after checking for the availability of funds.
- If the payment is future dated, the payer's PSP will store the transaction as a future dated payment.
- The payer's PISP (or TPSP) will receive the authorisation token to confirm that consent has been given for the payment as well as the status of the payment i.e. initiated or scheduled for the future. The authorisation token from the payer will be stored in the consent store.
- The PISP can then forward the status to the payer's TPSP.

Step 7: The payer's TPSP can now respond to the payee's TPSP with the payer's response and where applicable provide the status of the payment.
Step 8: When the response is received, the payee's TPSP will update the request status and pass it on to the payee.
Step 9: When the payment is received the payee's PSP will update the payee's account(s). This information will be retrieved by the payee's AISP and passed on to the payee for reconciliation.

8.3.3 Single Immediate Payment



Key:

Figure 8.3 Single Immediate Payment – Payment Flows

Interfaces

Single Immediate Payment			
Name	Description	Type	Source
1. Payment Initiation - PISP	Payment initiation request to PISP	API	New
2. CASS lookup	CASS lookup to determine switched accounts	API	New
3. Payee name	Payee Name Verification	API	New
4. Payment Initiation - PSP	Payment initiation request to PSP	API	Open Banking

5. Payment Initiation	Single Immediate Payment Initiation	File	New
6. Account Information - PSP	To get account transaction details from PSP	API	Open Banking
7. Account Information - AISP	To get account transaction details from AISP	API	Open Banking
8. Enhanced Data Extract	To extract enhanced data from cloud storage	API	New

Table 8.3 Single Immediate Payment Interfaces

Solution Overview

A potential solution for Single Immediate Payment or Future dated payment with enhanced data is as follows:

Step 1:

The payer initiates a payment along with the supporting data through their TPSP.

Step 2:

The payer's TPSP receives the payment request with the enhanced data and stores the supporting documents in a place where the payee can access it e.g. in the cloud with a token.

Step 3:

The PISP (or TPSP) receives the payment request and processes the payment request as follows:

- The PISP checks the CASS database to determine if the account has switched and get the switched account details.
- The payee's name is verified to ensure that the payment is being made to the intended party.
- It then passes the transaction on to the payer's PSP.

Step 4:

The payment process in the PSP will be initiated as follows:

- The payer will be redirected to their online PSP where they are required to log into their account with their secure credentials to authorise the payment.
- Once the payer authorises the payment, the payer's PSP will authorise the payment and create an authorisation token which will be stored in the authorisation store.
- The payee's PSP routing details will be obtained from the eISCD.
- If the payment is for the same day, the payer's PSP will initiate the payment after checking for the availability of funds.
- If the payment is future dated, the payer's PSP will store the transaction as a future dated payment.
- The status of the payment along with the "auth token" will be returned to the PISP.

Step 5:

The payer's PISP will receive the payment status from the PSP and

- Store the authorisation token in the consent store.
- Inform the payer on the status of the payment via their TPSP.

Step 6:

The payee's PSP will receive the transaction and update the payee's account with the funds received.

Step 7:

The payee's AISP will extract the transaction details and pass it to the payee's TPSP.

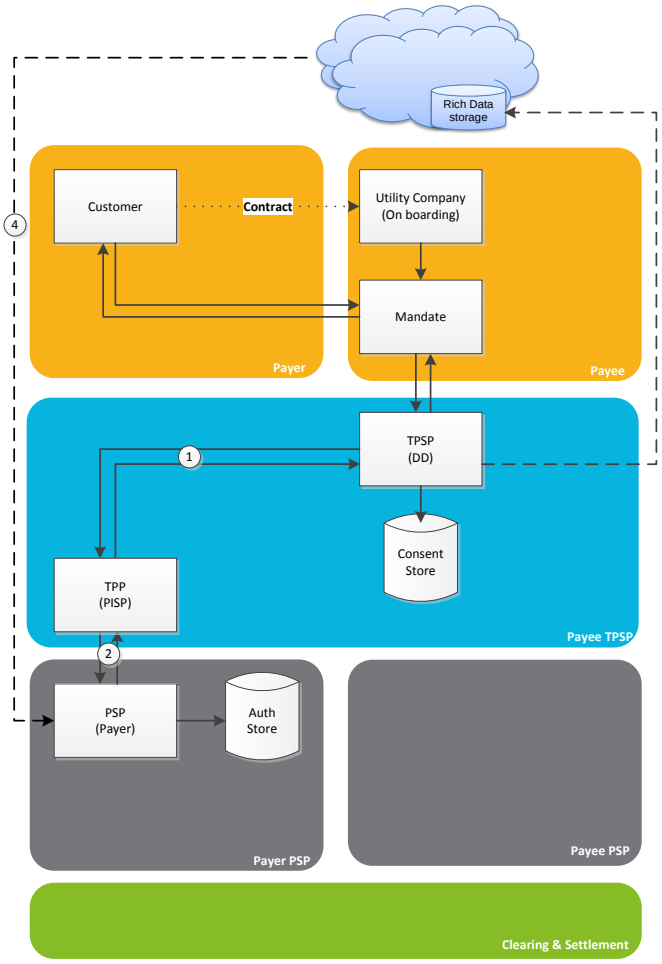
The payee's TPSP will extract the enhanced data and pass it along with the payment details in a format required by the payee. If the payee requires the data in XML/EDI format for auto-reconciliation, it will be converted to the format required e.g.

- PDF files will be converted to XML/EDI format
- Image files will use OCR to extract the data and send them in XML/EDI format

Step 8:

The payee's collection system will receive the payment details and enhanced data. The enhanced data will be used for automated reconciliation of the account receivables.

8.3.4 Direct Debit Instruction (DDI)



Key:

Figure 8.4 Direct Debit Instruction – Message Flows

Interfaces

Direct Debit Instruction Setup			
Name	**Description**	**Type**	**Source**
1. DDI - PISP	DDI request to PISP	API	New
2. DDI - PSP	DDI request to PSP	API	New

Table 8.4 Potential Direct Debit Instruction Interfaces

Solution Overview

A potential solution for Direct Debit Instruction set up is as follows:

Step 1:

The payer enters into a contract with the utility company and provides their sort code and account number. These details could be provided:

- in writing, verified by a signature.
- by telephone.
- on a secure password-protected website e.g. authenticated by logging into online banking.

Step 2:

The utility company sends the DDI details to their TPSP along with the copy of the paper DDI where applicable.

- If the authorisation is in writing and verified by a signature the utility company's TPSP can store the supporting documents in the cloud storage with a token and pass the DDI details to the payer's PSP via the PISP.
- If the payer has given their details online, they will be redirected to their online PSP via the PISP, where they will be required to log into their account with their secure credentials to authorise the DDI.

Step 3:

If the payer has approved the DDI in writing with a signature, the PSP can use the DDI as received or can perform additional validation as follows:

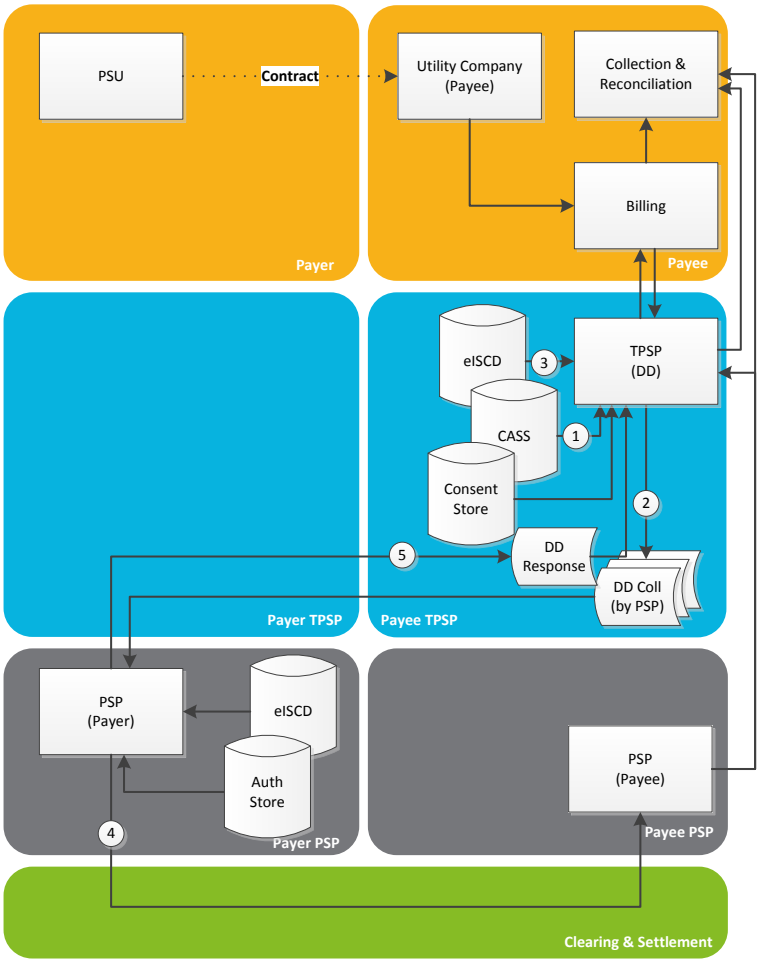
- Extract the DDI from the enhanced data and verify the signature to confirm the payee's authorisation.
- The payer's name in the DDI will be checked against the payer name in the account for confirmation of payer.

Step 4:

Once validated, the payer's PSP will authorise the DDI and create an authorisation token which will be stored in the authorisation store. The authorisation token will be returned to the payer's TPSP.

The payee's TPSP will store the "auth token" in its consent store and use it for subsequent Direct debit collections. The "auth token" will be used as a unique id to identify the DDI.

8.3.5 Direct Debit Collection



Key:

Figure 8.5 Direct Debit Collection – Payment Flows

Interfaces

Direct Debit Collection			
Name	Description	Type	**Source**
1. CASS lookup file	CASS lookup to determine switched accounts	File	New
2. DD Collection file	DD collection file by a PSP	File	New
3. eISCD lookup	eISCD lookup for routing details	Directory Service	New
4. Unattended (bulk) payment initiation	Unattended (bulk) payment files	File	New
5. DD Response file	DD response file	File	New

Table 8.5 Potential Direct Debit Collection Interfaces

Solution Overview

A potential solution for Direct Debit collection is as follows:

Step 1:

The utility company creates a bulk collections file of the payment due from its customers who have signed up for Direct Debit.

Step 2:

The payee's utility company's TPSP receives the bulk file and processes it as follows:

- The TPSP checks the consent store and to ensure that there is authorisation for the payment and the payment is in line with the parameters for the authorisation.
- Validates the payer's sort code and account number against the CASS database and substitutes them with the switched account details where required.
  Note:
  - Validating CASS for switched accounts could be a file-based submission with a response file of switched accounts.
  - Where the customer has switched, the switched account details will be sent to the utility company to update their records.
- Creates a separate file for each PSP and, where required, enriches the data and converts it to ISO20022 format.
- A collection file is submitted to each of the individual PSPs the day before the collection.

Step 3:

The individual PSP will receive the collections file and check the "auth code" received against what is stored in their authorisation store to ensure that a valid mandate exists and that the transactions are in line with the authorisation provided. On the due day;

- Cleared funds are pushed to the clearing and settlement service as unattended transactions early on the day of the collection date. A settlement obligation is created between the sending and receiving PSP.
- Accounts that fail posting due to insufficient funds may be re-tried by the payer's PSP as per the FCA guidelines and the payment generated will be sent as an attended or unattended payment.
- A rejection file will be created for items that were not posted due to insufficient funds, that are not in accordance with the authorisation or for closed accounts – deceased, switched etc. and then forwarded to the payee's TPSP.

Step 4:

The payee's TPSP will receive the rejections file from all the PSPs and amalgamate them and then send a single rejections file and send it to the utility company. Where required the TPSP could access all payments received from the payee's PSP via the AISP and reconcile the payment request submitted to the payment received.

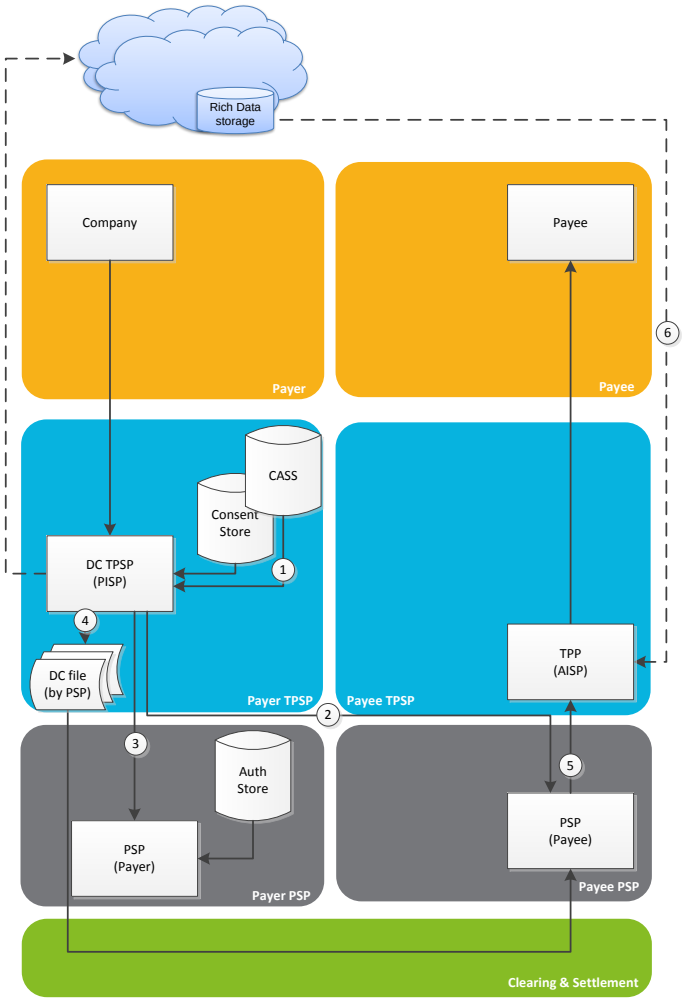
Step 5:

The payee's PSP will receive payment from each PSP, aggregate the payments and apply a single credit to the utility company's account. A file containing details of the payments received is sent to the payee or the payee's TPSP for reconciliation.

Step 6:

The utility company uses the payments file from its PSP to reconcile the collection raised against the payments received.

8.3.6 Direct Credit



Key:

Figure 8.6 Direct Credit – Payment Flows

Interfaces

Direct Credit			
Name	**Description**	**Type**	**Source**
1. CASS lookup	CASS lookup to determine switched accounts	API	New
2. Payee name	Payee Name Verification	API	New
3. Payment Initiation - Debit account	Debit payee account and credit NPA account	API	Open Banking (enhanced)
4. DC file	DC file by PSP	File	

5. Account Information PSP	To get account transaction details from a PSP	API	Open Banking
6. Enhanced Data Extract	To extract enhanced data from cloud storage	API	New

Table 8.6 Potential Direct Credit Interfaces

Solution Overview

A potential solution for Direct Credit is as follows:

Step 1:

The utility company creates a direct credits file along with the supporting documents (e.g. payslip) for the payment and forwards it to its (the payer's) TPSP for processing.

Step 2: .

The payer's Direct Credit TPSP (who is also a PISP) receives the bulk file and processes it as follows:

- Stores the supporting documents in cloud storage with a token.
- Checks the consent store to ensure that there is authorisation for the payment and the payment is in line with the parameters for the authorisation.
- Where required checks the payee name.
- Validates the payer's sort code and account number against the CASS database and substitutes them with the switched account details where required.
- Creates a separate file for each PSPs.
- Where required, converts the file ISO20022 format and enriches the data.
- On the day of the payment, the payers PISP will debit the payers account as detailed in Step 4 and submit the Direct Credit file (6) on behalf of the PSP to the clearing and settlement layer.

Step 3:

When the PISP initiates the debit to the customer's account, the PSP will perform the following checks before debiting the account.

- Check the "auth code" received against what is stored in their authorisation store (5) to ensure that a valid "auth code" exists and the transaction is in line with the authorisation provided.
- There are no blockers on the account.
- The account has sufficient funds.

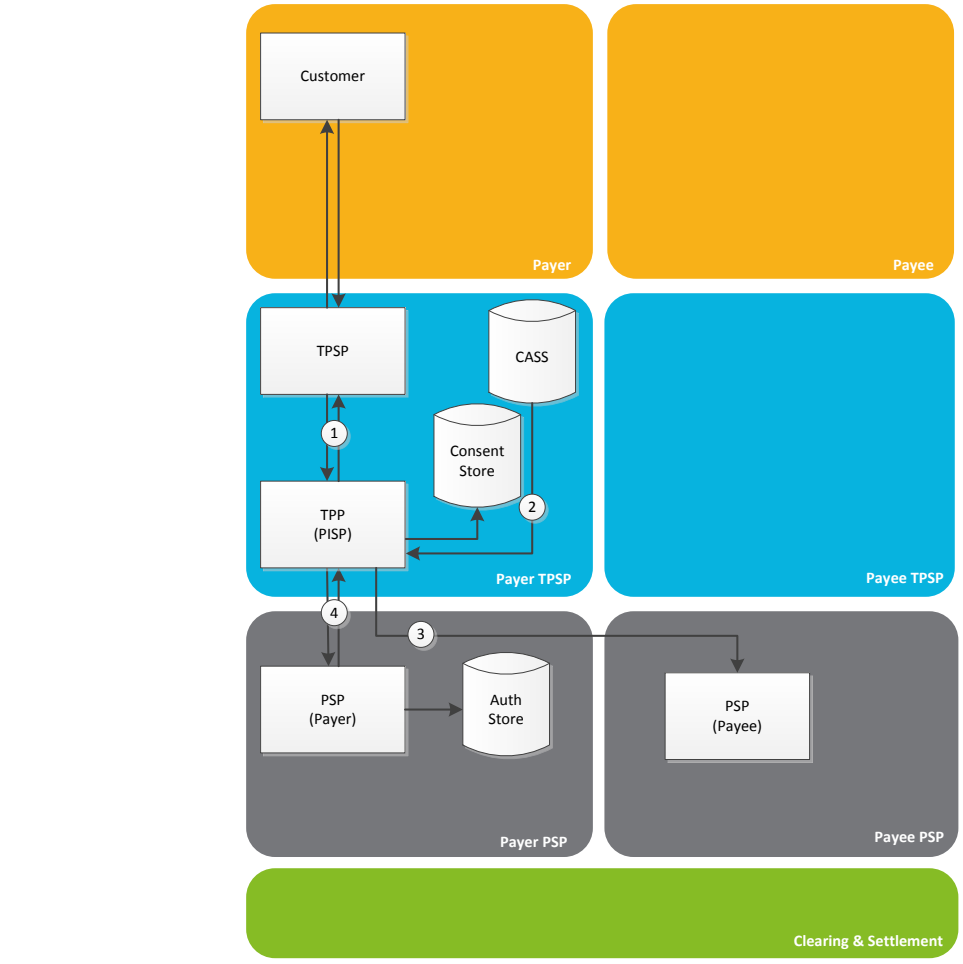
Step 4:

On receiving the Direct Credit file, the PSP updates the payee's account with the funds received.

Step 5:

Details of the payments received will be extracted by the customer's AISP and, where required, the enhanced data from the cloud storage, and passes the transaction details along with the enhanced data to the payee. Where required the TPSP could convert the enhanced data received to the format required by the payee e.g. XML/EDI format.

8.3.7 Standing Order Setup



Key:

Figure 8.7 Standing Order Set-Up – Messaging Flows

Interfaces

Standing Order Set-up			
Name	**Description**	**Type**	**Source**
1. Standing Order	Standing Order details to the PISP	API	New
2. CASS lookup	CASS lookup to determine switched accounts	API	New
3. Payee name	Payee name verification	API	New
4. Standing Order	Standing Order details to the PSP	API	New

Table 8.7 Potential Standing Order Set-Up Interfaces

Solution Overview

A potential solution for Standing Order set-up through the TPSP is as follows:

Step 1:

The customer initiates a standing order:

- Online - by logging on to their TPSP and entering the Standing Order details or
- Manually – by contacting their PSP to set up the Standing Order.

Step 2:

When the customer sets up the standing order online, the payer's TPSP validates the data received and passes the details to the payers PISP.

The PISP processes the request received as follows:

- Validate the payee's sort code and account number against the CASS database and substitutes them with the switched account details where required.
- Validates the payee's name with the payee PSP.
- Redirects the payer to their online PSP where they are required to log into their account with their secure credentials to authorise the standing order setup.

Step 3:

The PSP receives and processes the files as follows:

- Once the payer authorises the payment, the payer's PSP will authorise the mandate and create an authorisation token which will be stored in the authorisation store.
- The authorisation token returned to the payer's PISP.
- If the payer does not have an online presence
  - The customer could call the PSP or go to the PSP branch to set up the standing order.
  - The PSP can then set up the standing order after validating the details supplied (including the payee name).
- The "auth token" will be stored in the authorisation store.

Step 4:

The payer's PISP will store the "auth token" in their consent store and respond to the payer's TPSP.

Step 5:

The payer's TPSP will confirm the Standing Order set-up to the payer.

8.3.8 Cheque Clearing

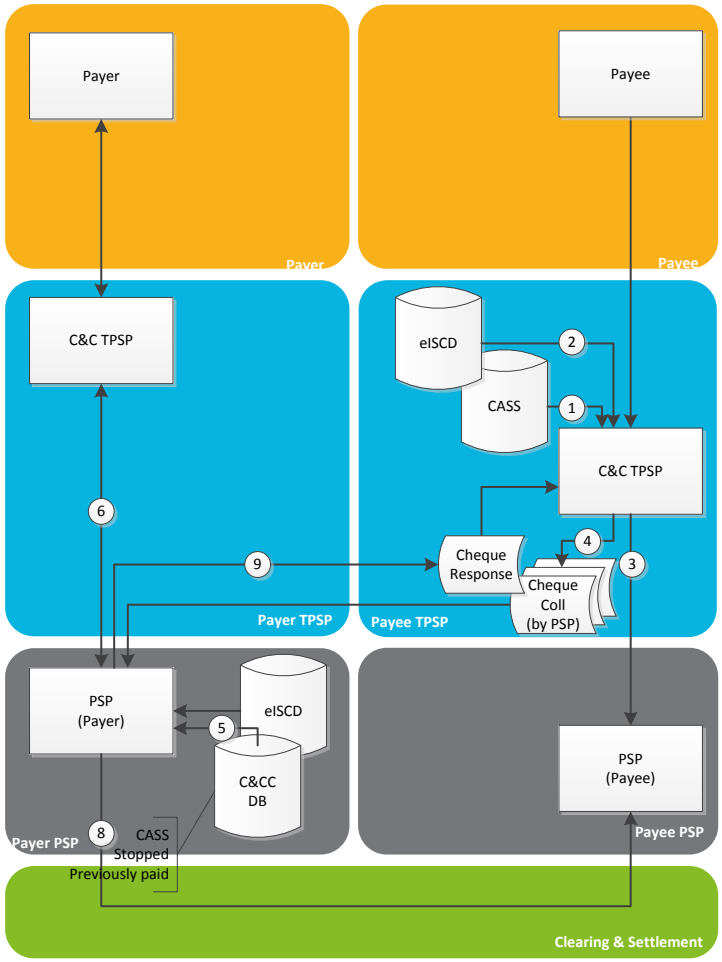


Figure 8.8 Cheque Clearing – Payment Flows

Interfaces

Cheque Clearing			
Name	**Description**	**Type**	**Source**
1. CASS lookup	CASS lookup to determine switched accounts	API	New
2. eISCD lookup	eISCD lookup for routing details	Directory Service	New
3. Transaction details	Transaction details to payee PSP	API	New

4. Cheque collection	Cheque collection file (similar to current ICS)	File	**New**
5. C&CC DB lookup	C&CC DB lookup for switched accounts	API	
6. Payee authorization	Cheque details to payee TPSP for payee authorization	API	**New**
7. Cheque response	Clearing status of cheques to TPSP	File	**New**
8. Unattended (bulk) payment initiation	Unattended (bulk) payment files	File	**New**

Table 8.8 Potential Cheque Clearing Interfaces

Solution Overview

A potential solution for cheque clearing is as follows:

Step 1:

The payee submits the cheque for collection to their TPSP.

Step 2:

Where the physical cheque is presented, the cheque is scanned by the Cheque and Credit (C&C) TPSP to capture its image and code line data and process them as follows:

- The image captured/received is validated to verify if it confirms to Image Clearing Service (ICS) specified format.
- The payer sort code and account number are validated against the CASS to check for switched accounts and where required the new account details are extracted.
- Details of where to send the cheque for clearing are obtained from the eISCD.
- A file similar to the current ICS request to pay message along with the cheque image is created and sent to the payers PSP.
- Transactions details are forwarded to the payee's PSP to enable them to consolidate payments received for all the cheques associated with that transaction and apply a single credit to the payee's account.

Step 3:

The payer's PSP will receive the message and process the message as follows:

- Upon receipt of the message, the payer's TPSP validates the code line and image and compares the courtesy amount to the legal amount, checks the date, checks the payee name and checks if the cheque is stopped etc.
- For switched accounts, the Cheque and Credit Clearing (C&CC) database are checked to ensure that the cheque is not a stopped or previously paid cheque.
- Where required, the cheque is presented to the payer via their TPSP for approval e.g. a high-value cheque, suspected fraud etc. If the payer does not have an online presence, they are contacted for approval.
- Code line details of validated cheques along with the beneficiary details will be presented to the payer's PSP.

For cleared cheques

- The PSP will retrieve the routing details for the payee's PSP from the eISCD and on the due day.

- Cleared funds are pushed to clearing and settlement service as an unattended transaction early (e.g. 01:00) on the collection date.
- A settlement obligation is created between the sending and receiving PSP.

For rejected cheques

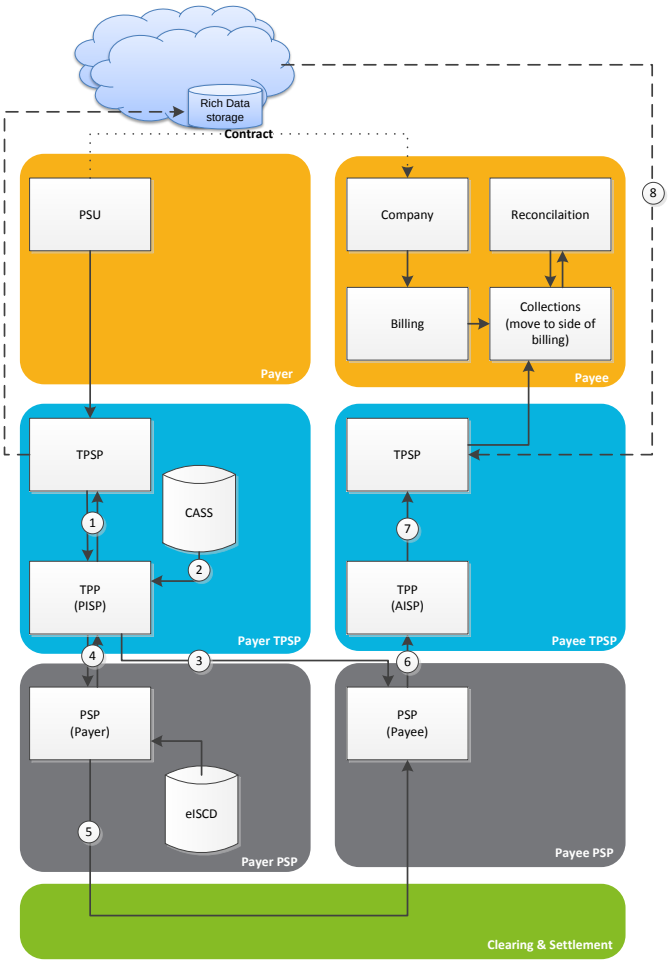
- A rejection file will be created for items that were not posted due to insufficient funds, that are not in accordance with the authorisation or for closed accounts – deceased, switched etc. and then forwarded to the payee's TPSP.

The payer's PSP will return the status of each cheque received to the payee's TPSP.

Step 4:

On receipt of the payment, the payee's PSP will reconcile the payments received against the transaction received from the payee's PSP and the aggregated credit for the transaction applied to the payee's account.

8.3.9 Paper Credit Clearing



Key:

Figure 8.9 Potential Credit Clearing Interfaces

Interfaces

Credit Clearing			
Name	**Description**	**Type**	**Source**
1. Payment Initiation - PISP	Payment initiation request to PISP (with extended data)	API	New
2. CASS lookup file	CASS lookup to determine switched accounts	File	New
3. Payee name	Payee name verification	API	New

4. Payment Initiation - PSP	Payment initiation request to PSP	API	Open Banking
5. Payment Initiation	Unattended (bulk) payment initiation	File	New
6. Account Information PSP	To get account transaction details from PSP	API	Open Banking
7. Account Information AISP	To get account transaction details from AISP	API	New
8. Enhanced Data Extract	To extract enhanced data from cloud storage	API	New

Table 8.9 Paper Credit Clearing – Payment Flows

Solution Overview

A potential solution for credit clearing is as follows:

Step 1:

The payer initiates a payment along with the supporting paper credit through his TPSP.

Step 2:

The payer's TPSP receives the credit and processes it as follows:

- Where the physical credit is presented, the Bank Giro Credit (BGC) is scanned to capture its image in the ICS specified format.
- The image is validated to confirm it is to the ICS specified format.
- The code line details and the payee name are captured from the credit image.
- Stores the supporting credit image where the payee can access it e.g. in cloud with a token.
- Sends the payment details to the PISP.

Step 3:

The PISP receives the payment request and processes the payment request as follows:

- Checks the CASS database to determine if the account has switched and, if necessary, get the switched account details.
- Where applicable, the payee's name is verified to ensure that the payment is made to the intended party.
- Passes the transaction to the payer's PSP.

Step 4:

The PSP will retrieve the routing details for the payee's PSP from the eISCD and on the due day:

- Cleared funds are pushed to clearing and settlement service as unattended transactions early in the day (e.g. 01:00). A settlement obligation is created between the sending and receiving PSP.
- A rejection file will be created for items that were not posted due to insufficient funds, that are not in accordance with the authorisation or for closed accounts – deceased, switched etc. and then forwarded to the payee's TPSP.

Step 5:

The payee's AISP will extract the transaction details and pass it to the payees TPSP.

Step 6:

Where required, the payee's TPSP will extract the image of the credit from the cloud storage and use it to enhance the payment data received with an 18 character reference field form the BGC code line or additional data from the body of the BGC.

Step 7:

The payee's collection system will receive the payment details and enhanced data. The enhanced data will be used for automated reconciliation of the accounts and/or update the correct accounts in the PSU system.

8.3.10 Refund Requests

Key:

Figure 8.10 Refunds – Payment Flows

Interfaces

Refund Requests			
Name	**Description**	**Type**	**Source**
1. Refund Request	Refund request (with extended data)	API	**New**
2. CASS lookup	CASS lookup to determine switched accounts	API	**New**
3. Refund Request	Refund request to a TPSP	API	**New**
4. Enhanced Data Extract	To extract enhanced data from cloud storage	API	**New**
5. Response to Refund Request	Response to refund request	API	**New**

Table 8.10 Potential Refund Request Interfaces

Solution Overview

A potential solution for refund requests is as follows:

The use case is based on a payer disputing a payment made and then requesting a refund through their TPSP. The refund request could be for any payment type e.g. RtP, SIP, Direct Debits, Cheques etc.

Request to Pay Refund:

For an RtP refund the payer's RtP TPSP:

- Extracts the payment details from the payer's PSP via the AISP.
- Stores the enhanced data where the payee's PSP/TPSP can access it.
- Creates the refund request message and sends it to the payee's RtP TPSP.

The payee's RtP TPSP:

- Retrieves the enhanced data from cloud storage.
- Where required, liaises with either the payee or payee's PSP.
- Where the refund request is accepted, they initiate a payment through the PISP.
- Sends the outcome of the refund request to the payer's RtP TPSP.

Cheque Refund

For cheque refund, the TPSP receives the refund request and passes it to the payer's PSP:

The payer's PSP validates the request and:

- Stores the cheque image and any supporting information as enhanced data where the payee's PSP/TPSP can access it.
- Creates the refund request message and sends it to the payee's C&CC TPSP.

The payee's C&CC TPSP:

- Retrieves the enhanced data from cloud storage.
- Where required, laisses either with payee or payee's PSP.
- Where the refund request is accepted they initiate a payment through the PISP.
- The outcome of the refund request is sent back to the payer's PSP.

Direct Debit Refund

For a Direct Debit refund, the TPSP receives the refund request and stores the enhanced data where the payer's PSP, payee's PSP/utility company can access it and passes it to the payer's PSP.

The payer's PSP validates the request, creates the refund request and sends it to the utility company or the payee's PSP as required.

The utility company/payee's PSP:

- Retrieves the enhanced data from cloud storage.
- Where the refund request is accepted initiates a payment through the PISP.
- Sends the outcome of the refund request to the payer's PSP.

Customer Initiated payment refund request

For customer initiated payment refund requests, the TPSP receives the refund request and stores the enhanced data where the payer's PSP can access it and passes it to the payee's/payer's PSP.

The payer's PSP validates the request, creates the refund request and sends it to the payee's PSP.

The payee's PSP:

- Retrieves the enhanced data from cloud storage.
- Where the refund request is accepted, initiates a payment through the PISP.
- Sends the outcome of the refund request to the payer's PSP.

8.3.11 APIs and Messages

Consolidated APIs

API's	RtP	SIP	DD Man	DD Col	DC	SO	Cheque	BGC	RR
1. Proxy Register API	✓								
2. CASS lookup API	✓	✓				✓		✓	
3. RtP Message	✓								
4. RtP Response	✓								
5. Enhanced Data Extract	✓	✓			✓			✓	✓
6. Payment Initiation - PISP/PSP/Debit Account	✓	✓			✓			✓	
7. Account Information to AISP/TPSP	✓	✓			✓			✓	
8. Payee Name		✓			✓	✓		✓	
9. DD mandate to PISP/PSP			✓						
10. Standing Order details						✓			
11. Transaction Detail							✓		
12. C&CC DB lookup							✓		
13. Payee Authorisation							✓		
14. Refund Request (RR)									✓
15. Response to RR									✓

Table 8.11 Consolidated APIs

Consolidated Files

API's	RtP	SIP	DD Man	DD Col	DC	SO	Cheque	BGC	RR
1. Attended (single) payment initiation	✓	✓							✓
2. Unattended (bulk) payment initiation				✓	✓	✓	✓	✓	
3. Collection file (DD & Cheque)				✓			✓		

API's	RtP	SIP	DD Man	DD Col	DC	SO	Cheque	BGC	RR
4. Response file (DD & Cheque)				✓			✓		
5. CASS Validation file				✓	✓		✓		
6. CASS Response file				✓	✓		✓		

Table 8.12 Consolidated Files

Reference Data

Reference Data Required	
Name	**Potential Source**
CASS	Provided by TPSP/NPSO
Proxy Register	Provided by TPSP/NPSO
TPSP Directory	Directory Services
eISCD	Directory Services
C&CC switched account data	Provided by TPSP/NPSO

Table 8.13 Reference Data

8.4 Appendix 4: Detailed Analysis for Clearing and Settlement Approach

8.4.1 Option 1: Central Settlement Clearing (Recommended)

Model Overview

Following a comprehensive assessment, this option is the recommended clearing and settlement model for NPA. The centralised clearing and settlement model is based on central participant messaging with clearing and settlement via the central node. The node validates that the sending participant is operating within its NSC, clears the payment and adjusts the senders and receivers net positions. Participants routing is via the central participant messaging.

Option 1 provides:

- Controlled settlement processing - no settlement risk.
- Simplified governance, operating and reconciliation.
- A well-understood approach with existing schemes and best practice globally including the recent US (TCH) and EU (SCT Inst) models.
- Simplified interfacing and messaging.
- Simplified PSP to PSP relationship management – a new PSP only needs to establish a relationship with the central clearing and settlement Infrastructure.
- Easier to add or remove PSPs.

High-Level Clearing and Settlement Flow

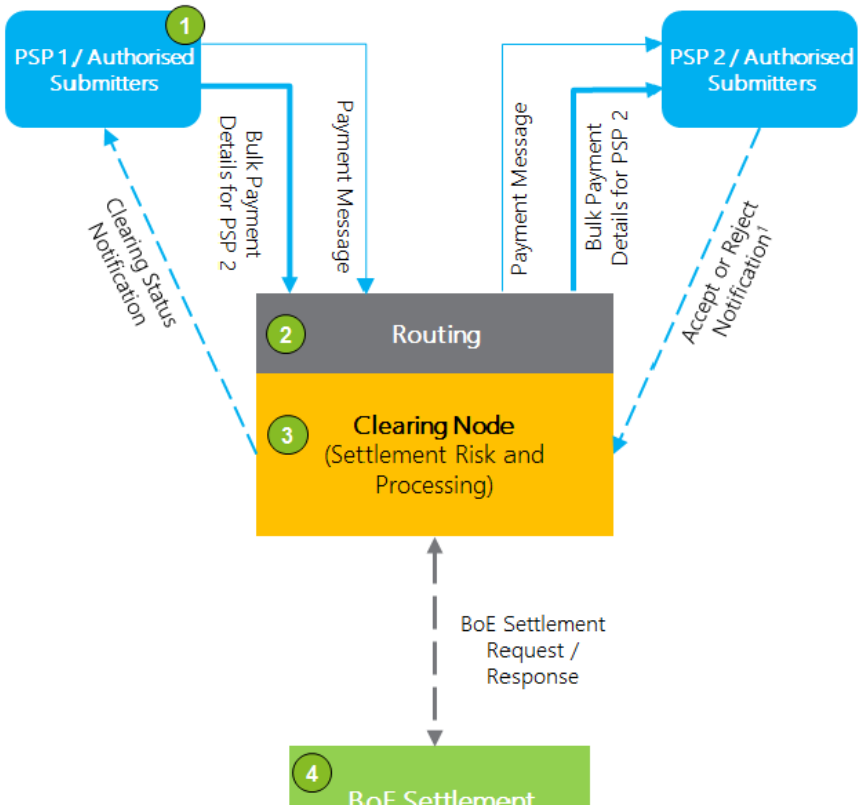


Figure 8.11 Option 1: Clearing and Settlement

All payment messages routed via central participant messaging.

1. PSPs, send payments to a central clearing node.
2. Routing:
    a. Receipt of payment message(s)
    b. Routing of messages
3. Clearing Node:
    a. Maintenance and checking of a participating PSP's settlement risk position
    b. Notifications
    c. Initiates settlement according to configured cycles
4. BoE settlement completion.

Responsibilities within Centralised Clearing and Settlement

The recommended clearing and settlement model uses the concept of a logical central infrastructure for both clearing and settlement. Below is a representation of the primary roles of centralised settlement and clearing.

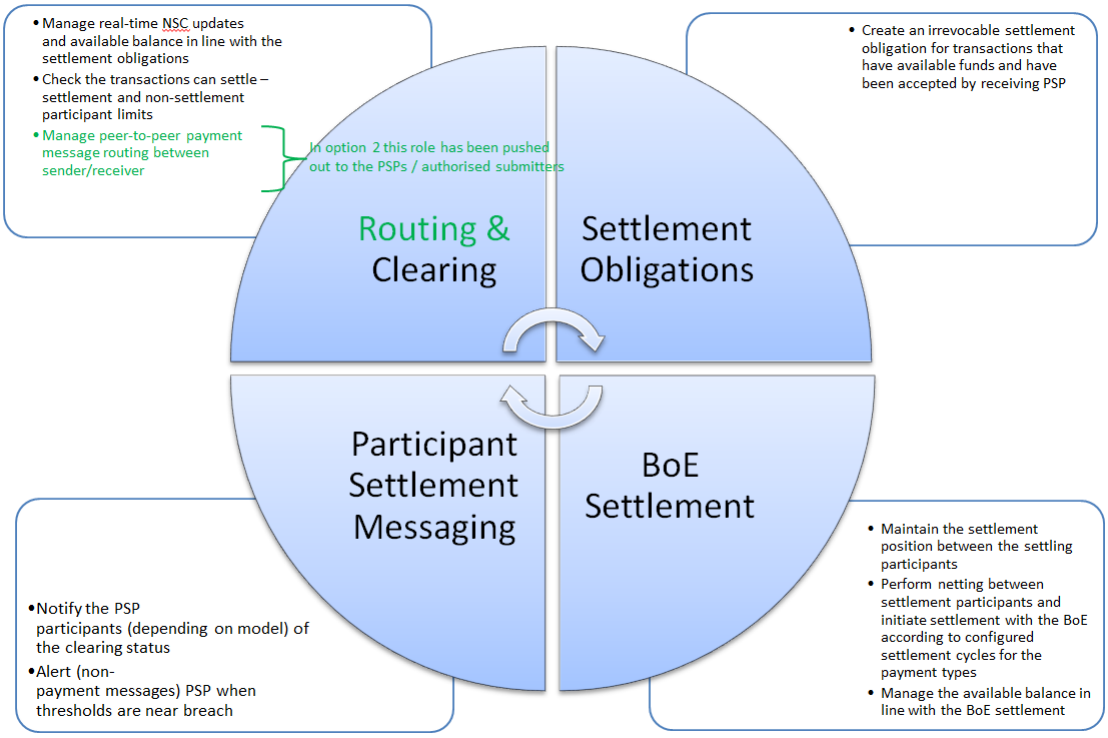


Figure 8.12 Centralised Clearing and Settlement Responsibilities

8.4.2 Option 2: Hub and Spoke Settlement and Peer-to-Peer Clearing

Model Overview

The distributed model (peer-to-peer participant messaging with centralised risk and settlement management) requires the participants to exchange payment messages with each other, with the sender accountable for ensuring settlement via a common settlement risk and settlement processing service (clearing node). The clearing node validates that the sending participant is operating within its NSC and adjusts the settlement positions for the cleared transactions.

Option 2 provides:

- Controlled settlement processing - no settlement risk.
- Provides a different model of governance and control via NPSO rules and standards.

High-Level Clearing and Settlement Flow

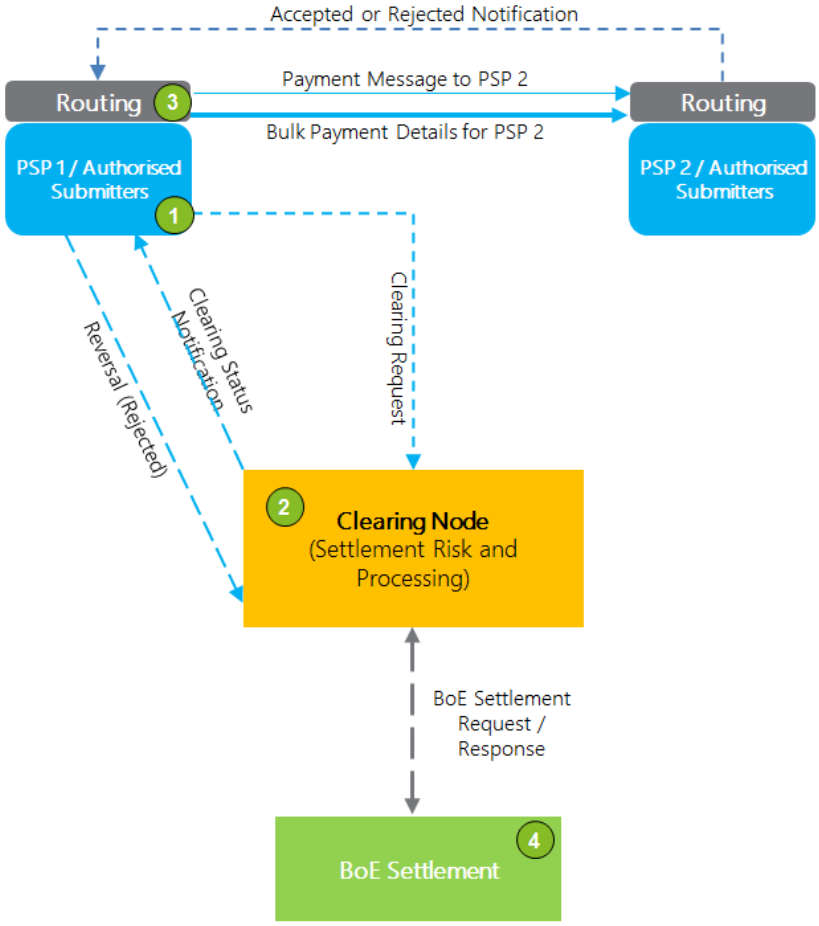


Figure 8.13 Option 2: Clearing and Settlement

1. The sender sends a clearing request to the clearing node
   The clearing node:
   a. Checks the risk position.
   b. Creates a settlement obligation.
   c. Sends a clearing status (with token) notification to the sender.
   d. Initiates settlement completion with the Bank of England according to configured cycles
2. The sender sends cleared payments to the receiver (with a token).
3. BoE settlement completion.

Responsibilities within Centralised Settlement

The settlement model uses the concept of a logical central infrastructure for settlement risk and settlement processing, whereas the clearing and routing use peer-to-peer messaging. The primary roles of the centralised settlement are shown below:

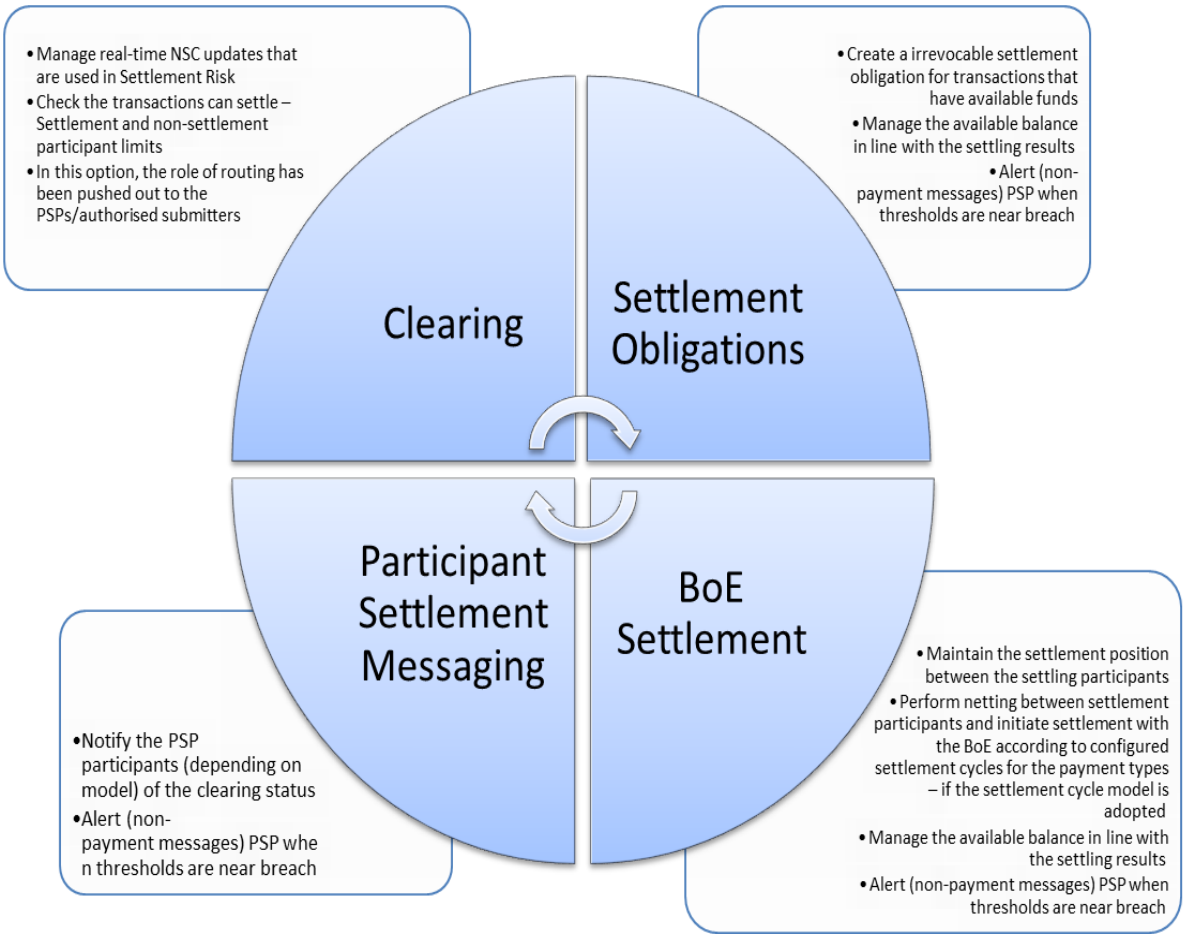


Figure 8.14 Centralised Settlement Responsibilities

Discarded High-Level Clearing and Settlement Flow

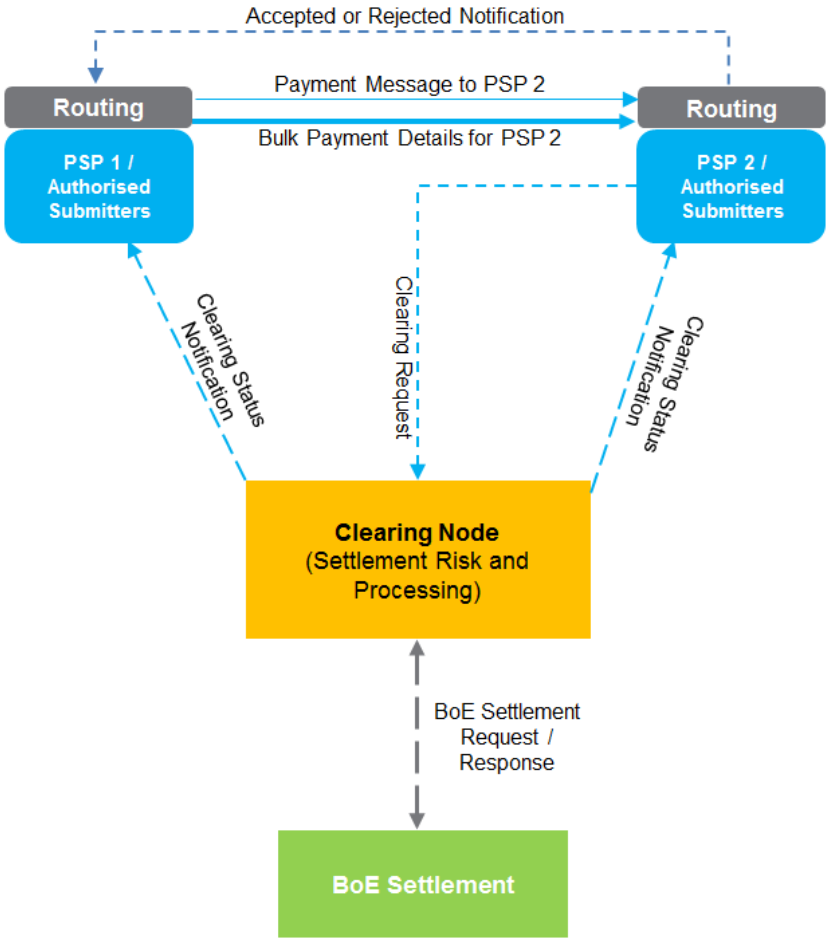


Figure 8.15 Discarded Flow 1 – Receiver Initiates Clearing and Settlement

The implementation of peer-to-peer routing (option 2) requires a specific message flow implementation to enforce the requirement of only receiving cleared and settled funds. The following subsection provides a view of the peer-to-peer flows that were discarded as they do meet this requirement.

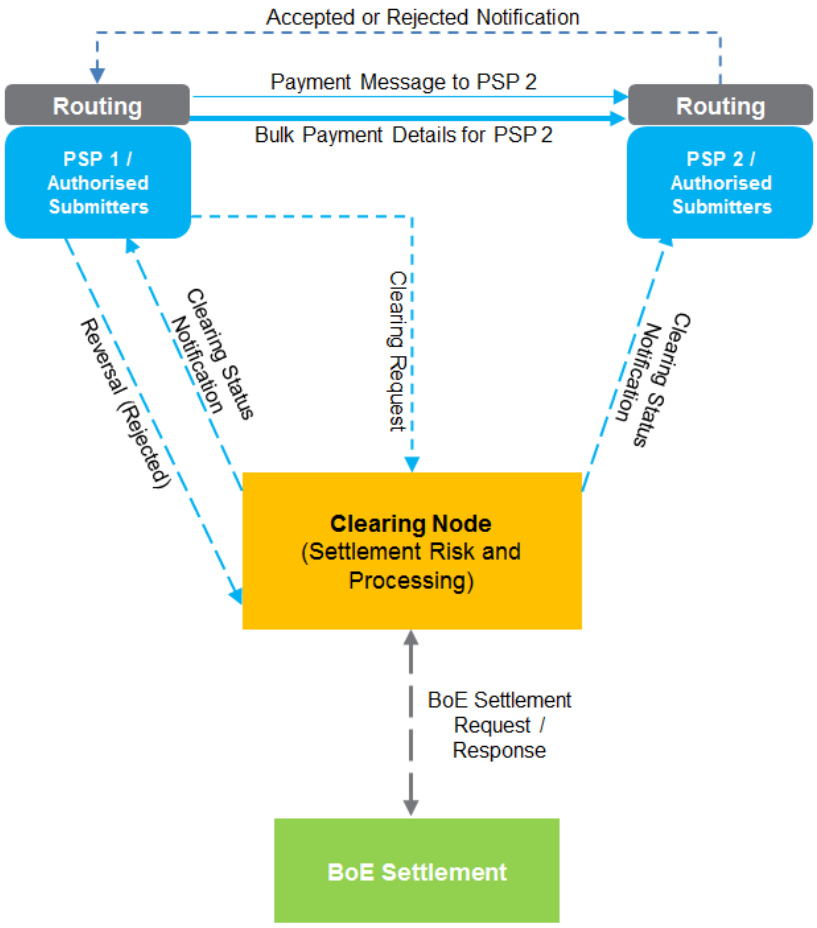


Figure 8.16 Discarded Flow 2 Sender initiates clearing and settlement

8.4.3 Option 3: Bilateral Messaging and Settlement (Discarded)

Model overview

Option 3 is based on a fully distributed model with bilateral messaging (no central control or risk management). Participants elect to send and receive payments where the immediate value is passed on to the beneficiary. The bilateral messaging and settlement model assumes that settlement will follow, and participants will have to trust each other to settle at a later date.

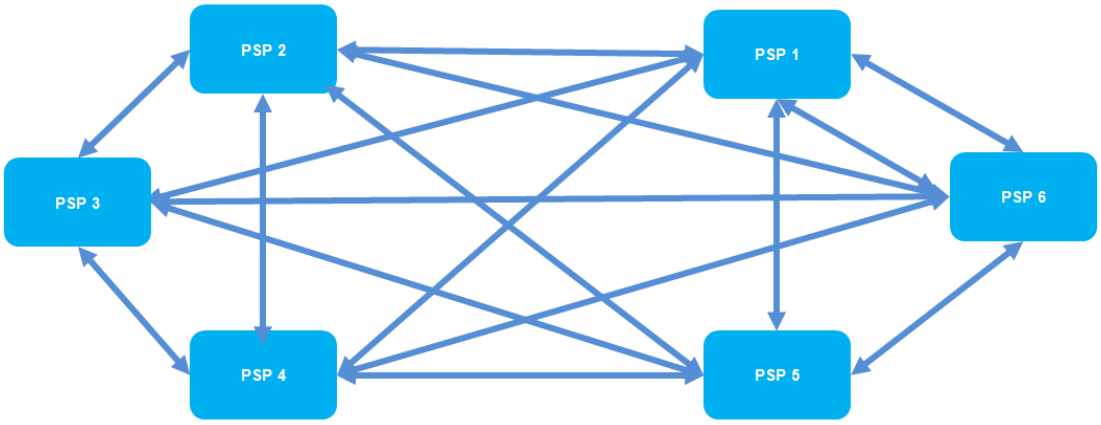


Figure 8.17 Distributed Model with Bilateral Messaging

Reasons for discarding

- Introduces unlimited settlement risk
- Requirement to settle in Central Bank money is not met
- Difficult to govern and enforce settlement

8.4.4 Option 4: Bilateral Messaging with Nostro/Vostro (Discarded)

Model overview

Option 4 involves a fully distributed model with bilateral messaging with Nostro/ Vostro accounting. Option 4 is similar to Option 3, although participants maintain accounts with each other to reduce settlement risk. In this model the senders account with the receiver is debited at the point of sending the transaction with periodic payments made between participants to settle their respective accounts.

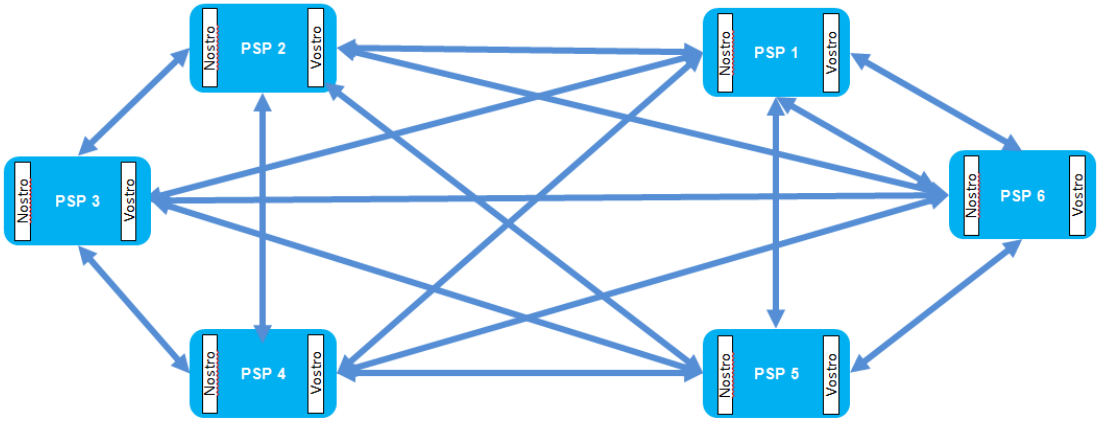


Figure 8.18 Distributed Model with Bilateral Messaging with Nostro/Vostro Accounting

Reasons for discarding

- Introduces limited control over settlement risk
- Inefficient - too many accounts to actively manage
- Each account would need liquidity management/funding
- Complex to reconcile
- No netting – increased reserve collateral required by each participant
- Requirement to settle in Central Bank money is not met

- Need for loss sharing agreements between participants – increased exposure of ring-fenced and non-ring fenced may not be acceptable to PSPs or regulators
- Possibility of ring-fencing and non-ring fencing requirements being breached
- No protection of reserve funds held at each participant

8.4.5 Option 5: Bilateral Messaging and Central Bank Settlement (Discarded)

Model overview

The following model uses distributed bilateral participant messaging with central settlement risk and settlement management by Bank of England. Participants will exchange messages with each other with a copy to the Bank of England. The Bank of England will be responsible for settlement risk management and validating that the sender has sufficient funds.

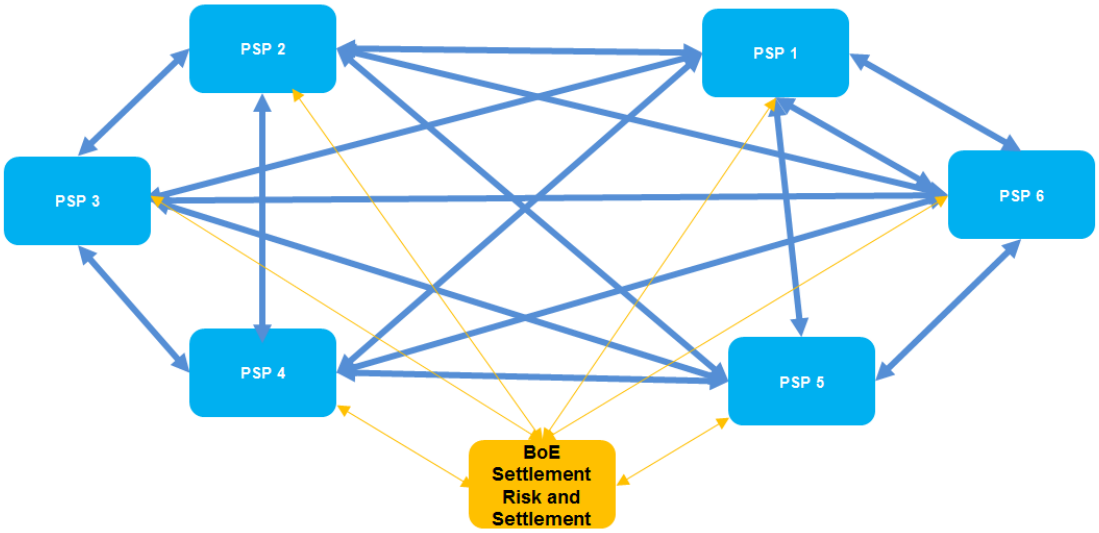


Figure 8.19 Bilateral Participant Messaging with Central Settlement Risk

Reasons for discarding

- Requires each payment to be settled in real time
- The BoE will have to operate a fully resilient 24x7 system - downtime in service will cause payment failures
- No opportunities for netting
- Increased message traffic between the BoE and participants

8.4.6 Option 1 vs. Option 2 Assessment

Option 1 and option 2 were assessed and evaluated against a set of defined criteria. The table below provides the outcome of the discussions and shows how the recommendation was informed.

Criteria	Option 1: Central Routing	Option 2: Peer-to-Peer routing
Financial Stability: Only receive cleared and settled funds	• Central routing will send cleared funds to the receiver • Simple Process • The routing informs the	• Sending PSPs will route payment messages to the receiving PSP once the sending PSP has received positive notification that

Criteria	Option 1: Central Routing	Option 2: Peer-to-Peer routing
	settlement- a central routing function provides consistent and accurate settlement information in real-time. Allows consistent cap management • Removes systemic risk of participant failures by insulating them from each other • Provides a 'buffer' between Participants - protect a Participant from receiving more payments than they can handle through a central throttling mechanism (particularly useful for handling debulked file volumes), avoiding overload and managing priorities.	the payment has been cleared. Assurance will be provided to receiving PSP through a token to the sender on notification of clearing. • Complex process: the use of the token, and additional (to Option 1) messaging does not draw out that this requires a much higher processing overhead, due to increased complexity for each PSP compared to Option 1 • Provides no protection from a PSP receiving a large volume in a very short time frame, which can lead to timeouts and a degraded end-user experience – in extremis such a situation resembles a DDOS attack.
Thin Infrastructure: Allowing provider to compete in the market simultaneously	• More complexity at the centre moves complexity away from PSPs/authorised submitters – both options are just shifting complexity between the centre and PSPs • Thin requirements for each Participant - designed to be as thin as necessary at the centre • Reduced overall cost and risk to industry • Less complex implementation than option	• Less complexity at the centre moves complexity out to PSPs/authorised submitters – both options are just shifting complexity between the centre and PSPs • Increased overall cost and risk to industry • More complex implementation than option 1.
Scalability: Accommodate future growth in a cost-effective manner – encouraging suppliers to compete	• Clearing requires a single vendor to scale, which leaves the buyer exposed to the cost and delivery charges without the opportunity to seek competitive pricing. A single provider would control the entire market – mitigated by regular competitive procurement and contractual negotiations around scalability; should a vendor seek to exploit their position, then they risk being excluded from future tendering	• For clearing each PSP can scale to its required volumes, which introduces flexibility and makes the model commercially competitive • There is a strong dependency on all participants scaling and the Master Node will still need to scale – along with the additional token and message handling introduced in this model • In both Options, PSPs would need to be scalable, but Option 2 gives less protection if they misjudge this

Criteria	Option 1: Central Routing	Option 2: Peer-to-Peer routing
Financial Crime: Support sharing of payment details with the Financial Crime Utility	• Simpler interface through a single point to share payment information for financial crime purposes • Simplified regulatory reporting • Operationally move efficient (single point of contact for support).	• Requires each PSP to interface with Financial Crime directly • Supervision and control is more complex than option 1 • Assurance will be provided that data is shared with the financial crime utility correctly (through testing, accreditation/certification).
Transition: The option must support a low risk and smooth transition from the existing payments services to the NPA	• The transition options are still being investigated. Currently, there is limited information to suggest one clearing and settlement option has advantages over the other.	• The transition options are still being investigated. Currently, there is limited information to suggest one clearing and settlement option has advantages over the other.
Redirection (CASS): Support the clearing of payments affected by account switching	• Centrally managed through the CASS database - a single redirection database in the centre, such that all transactions are processed against the same version of the truth • Less processing for each PSP to do prior to submission. • Central redirection also caters for the approximately 30,000 direct submitters (SME, Corporate and Government users) that use the PSP-agnostic software.	• Centrally managed through the CASS database - a single redirection database in the centre, such that all transactions are processed Controls will ensure that participants can only access data applicable to payments that they are processing. • More complex than option 1 to address the large number of direct submitters without either requiring them to each call out to the registry/database before submitting payments (process and tech change) or changing the direct submission model to a 'through PSP' model that makes changing PSP a bigger task (and therefore reduces the effects of competition) • CASS redirection data caching restrictions apply – restriction on holding copies of data locally will make implementation more complex • Adds an additional call by PSPs to a redirection database/registry before submitting payments - more processes for a payment to pass through in its journey, introducing more potential failure point.
Trust and Control: Reduces risk of errors and enforces control	• Centralised implementations have less risk of error as a single capability (validation, duplication checks and rejection management etc.) is servicing all PSPs	• Multiple supplier implementations have a higher risk of errors - mitigated with simplified published specification, rules and assurance through testing and

Criteria	Option 1: Central Routing	Option 2: Peer-to-Peer routing
	• NPSO oversight of ecosystem more achievable.	accreditation/certification • Creates a much higher mutual dependency on other PSPs than Option 1, where the clearing layer insulates • Sender less protected from receiver unavailability. NPSO has fewer tools to manage the safety and security of service • NPSO has less oversight of ecosystem, without being more intrusive into each PSP.
Competition: Promotes competition 'in the or for the market'	• Clearing supports competition for the market • Settlement Risk and Settlement Processing supports competition FOR THE market.	• Clearing supports competition in the market • Settlement Risk and Settlement Processing supports competition FOR THE market.
Cost of Adoption: A cost-effective model that encouraging suppliers to compete	• Purchase power of the entire market would leverage strong negotiation position - contracts would be negotiated to manage risks – e.g. volume growth be agreed as part of contract • There is also the cost of adoption to new entrants, with a central routing requiring less complex functionality to be developed at the PSP.	• Smaller PSPs, without a scale, would lack buying power – which would mean a material higher item cost, which reduces the potential market of PSPs and therefore gives less competition for end-users to benefit from.
Cost of Access: Costs for Clearing and Settlement	• Access for new entrants with a central routing requiring less complex functionality to be developed at the PSP.	• Multiple suppliers can compete to provide services encouraging competitive pricing • Each PSP would need to procure a 'thicker', technically and operationally more complex solution – so higher cost than the thin gateway required for Option 1.
Reconciliation	• Single, multilateral reconciliation process – with absolute clarity as to fate/response to each payment provided by a single party.	• Many relationships and routing to maintain. Scale of small participants may not support demand from large • Refer to Scalability.

Table 8.14 Option 1 vs. Option 2 assessment

8.5 Appendix 5: Glossary

4th EU Money Laundering Directive (4MLD): A directive aiming to strengthen the anti-money laundering regime across the European Union. 4MLD looks to enhance the transparency of beneficial ownership, clarify the definition of a Politically Exposed Person (PEP) and ensure greater controls when performing risk assessments.

Account Identifier: Combination of numeric, alphabetical or alphanumeric characters used to uniquely identify an account.

Account Information Service: An online service to provide consolidated information on one or more payment accounts held by the Payment Service User with another Payment Service Provider or with more than one Payment Service Provider, and includes such a service whether the information is provided.

Account Information Service Provider (AISP): A payment service provider which provides account information services.

Acknowledged/Not Acknowledged Messages: Acknowledgement that a message is accepted for onward processing/ Not Acknowledgement that a message is not accepted for onward processing.

Aggregation / Collection: A function that collects funds for a customer's account and updates their account with the aggregated value.

Aggregator: An organisation that provides one or more PSPs with technical access to one or more payment systems.

Application Programming Interface (API): A set of functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or another service.

Attended Payment: A payment where the payer who initiated the payment is physically awaiting a response i.e. either a successful or unsuccessful outcome. This will typically be a Single Immediate Payment. Existing products that are likely to fall into this category are FPS SIP payments.

Auth Store: A data store that holds the payer's authorisation code that is tied to a specific transaction.

Authorised payment: A payment where the customer has given their consent for the payment to be made.

Back Office: A centre in which the administrative work of an organisation is carried out without direct contact with the customer.

Bacs: Formerly known as Bankers' Automated Clearing Services. The organisation responsible for the clearing and settlement of UK automated payment methods, including Direct Debits and Direct Credits.

Bacs Payment Schemes Ltd (BPSL): the operator of the Bacs payment system.

Bacstel IP: A communication channel used to connect to the BPSL infrastructure. This is typically used by indirect PSPs and corporates with smaller transaction volumes.

Bank of England (BoE): The central bank of the United Kingdom, providing the role as a settlement agent for interbank funds transfers.

Bulk Payment: Provides the ability to make multiple debit payments in one transaction.

Bureau: An organisation that sends payments to Bacs on behalf of another organisation.

Central Bank Money: Allows settlement between participants in money that is held by the Bank of England.

Channel: An interface through which communication can be made.

CHAPS: Clearing House Automated Payment System. The scheme typically used for high-value payments which are settled in real time.

Cheque & Credit (C&C): Payment system providing net settlement of cheques and paper credits between financial institutions. It operates on a three-day cycle and settles net once a day in RTGS.

Cheque & Credit Clearing Ltd (C&CCL): Operator of the Cheque & Credit Clearing payment scheme.

Competition and Markets Authority (CMA): A non-ministerial department of the UK government that promotes competition for the benefit of consumers, both within and outside the UK.

Competition and Markets Authority 9 (CMA9) - The Competition and markets authority issued The Retail Banking Market Investigation Order 2017 and has mandated nine banks namely, RBS, Lloyds, Barclays, HSBC, Santander, Nationwide, Danske, Bank of Ireland and Allied Irish Bank to set up an 'implementation entity' by 16 February 2017 to "implement, maintain and make widely available" the new standards as set out in the Retail Banking market investigation: Final report.

Consent Store: A database which holds a customer's consent to allow a TPSP to initiate a payment.

Consumer: A person who buys goods or services for their own use.

Corporate: Typically, a large company that employs more than 250 employees.

Credit card transaction: A card-based payment transaction where the amount of the transaction is debited in full or in part at a pre-agreed specific calendar month date to the payer, in line with a prearranged credit facility, with or without interest.

Current Account Switch Service (CASS): Free to use service that lets consumers and small businesses switch their current account from one participating bank or building-society to another. It has been designed to be simple, reliable and stress-free and is backed by the Current Account Switch Guarantee. The CASS database also contains the Bulk Payment Redirection Service (BPRS).

Customer accounts: A customer account that can be debited or credited by the PSP.

Direct Credit: A payment scheme by which an organisation makes payments in bulk to individual bank accounts e.g. salaries.

Direct Debit (DD): A Bacs payment scheme by which an organisation collects pre-notified payments in bulk from individual payers' bank accounts e.g. utility bills.

Directory Look-Up: A function which obtains reference data from the master database (e.g. sort code, bank, overlay level EISCD reference data, CASS account transfers and customer reference data, PSP and TPSP endpoints, roles and certificates). These are necessary to make and route payments.

Discounted Cash Flow (DCF): A valuation method used to estimate the attractiveness of an investment opportunity.

End-user: Person or organisation that actually uses a product or service.

Extended Industry Sort Code Directory (EISCD): A downloadable database containing information about banks and building societies that are connected to the UK clearing systems. These include BPSL, FPSL, CHAPS Sterling and Cheque and Credit Clearing.

Faster Payments Service (FPS): The scheme used for real-time payments, including Standing Orders.

Faster Payments Scheme Limited (FPSL): Operator of the FPS payment system.

Financial Conduct Authority (FCA): A regulatory body for financial services industry in the UK. Its role includes protecting consumers, keeping the industry stable, and promoting healthy competition between financial service providers.

FinTech: Financial Technologies. Companies that provide technology to financial institutions.

Forward Dated Payment: A payment set up to be processed on a date in the future.

General Data Protection Regulations (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Parliament, the Council and the European Commission intend to strengthen and unify data protection for individuals within the European

Union (EU). It was published in the Official Journal of the EU on 4 May 2016. It will apply from 25 May 2018.

Governing body: A group of people who formulate the policy and direct the affairs of an institution in partnership with the managers, especially on a voluntary or part-time basis.

Image Clearing System (ICS): The proposed new method revolutionising how cheques are cleared in the UK. The cheques will be cleared using a digital image of the cheque rather than via the current paper-based clearing system.

Information Commissioner's Office (ICO): The UK's independent body set up to uphold information rights.

Intellectual Property (IP): Intangible property that is the result of creativity, such as patents and copyrights.

ISO 20022: An international standard for the development of financial messages.

JSON: JavaScript Object Notation. An open-standard file format used to transmit data.

Market participant: An entity that has a payments service relationship with the NPSO. It can include settlement participants, direct participants, indirect participants, service participants, third party service providers and aggregators.

Net Sender Cap (NSC): A control mechanism to limit the credit exposure each participant brings to the system.

Net Present Value (NPV): The value in the present sum of money, in contrast to some future value it will have when it has been invested at compound interest.

New Payment System Operator (NPSO): The new Payment Services Operator that will consolidate the existing Bacs, Faster Payments and Cheque & Credit schemes.

Open Banking: PSD2 sets out the regulatory regime that lays the foundations for open banking, by giving registered/authorised third party providers a 'right' to access a consumers account. As part of the implementation of this, Open Banking are designing API Standards to create a more effective system for connecting third party service providers and financial institutions.

Payee: A person who is the intended recipient of transferred funds.

Payer: A person who holds a payment account and allows instructions to be given to transfer funds from that payment account, or who gives instructions to transfer funds.

Paym: A service that enables payments to be made using a proxy, such as a mobile phone number, to make a payment to a bank account.

Payment Assurance: A function that confirms the payee's and payer's identity as well as the status of a payment.

Payment Gateway: A service that facilitates a payment transaction by transferring information between the buyer and seller.

Payment Institution: A legal person that has been granted authorisation by the FCA in accordance with Article 11 (PSD2) to provide and execute payment services.

Payment method: The way that a buyer chooses to compensate the seller of a good or service that is also acceptable to the seller.

Payment Service Provider (PSP): A Payment Service Providers can be any of the following when carrying out payment services; authorised payment institutions, small payment institutions, registered account information service providers, EEA authorised payment institutions, EEA registered account information service providers, electronic money institutions, credit institutions, the Post Office Limited, the Bank of England, the European Central Bank, and the national central banks of EEA States (other than when acting in their capacity as a monetary authority or carrying out other functions of a public nature),

government departments and local authorities (other than when carrying out public functions) and agents of Payment Service Providers and excluded providers.

Payment Service User (PSU): A person when making use of a payment service in the capacity of the payer, payee, or both.

Payment Account: An account held in the name of one or more Payment Service Users which is used for the execution of payment transactions.

Payment System Operator (PSO): A company that operates one or more schemes. All PSOs are regulated by the PSR and additionally certain PSOs are supervised by the Bank of England.

Payments Messaging: A communication channel that facilitates the exchange of non-clearing messages (e.g. reports and adjustments) between the PSP and the clearing function.

Payment Services Directive (EU Directive on Payment Services): Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC of 13 November 2007, published in the Official Journal of the EU on 5 December 2007.

Payment Services Directive 2 (PSD2): Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, published in the Official Journal of the EU on 23 December 2015.

Payments Strategy Forum (PSF): A forum made up of payment industry and end-user representatives with the aim to develop a strategy for payment systems in the United Kingdom. The PSR, the Financial Conduct Authority and the Bank of England attend the Forum as observers.

Payment Systems Regulator (PSR): The economic regulator of payment systems in the United Kingdom. The PSR aims to promote competition, innovation and interests of end-users of payment systems.

Pull payments: Payments where the person who is due to receive the money instructs their bank to collect money from the payer's bank. Can be authorised or unauthorised.

Push Payments: Payments where a customer instructs their bank to transfer money from their account to someone else's account. Can be authorised or unauthorised.

Real-Time Gross Settlement (RTGS): The accounting arrangements established for the settlement in real-time of sterling payments across settlement accounts maintained in the Bank of England's settlement system.

Reserves Collateralisation Account (RCA): An account held by each member of a Deferred Net Settlement Payment System at the Bank of England used for prefunding.

Request to Pay (RtP): A flexible payment and bill management service concept that offers payers more control over bill payments that is initiated by the payee.

Service Level Agreement (SLA): Is a contractual agreement between a service provider and end-user that defines the conditions and level of service expected from the service provider.

Service provider: A payments service provider is a technical provider of payment services or the technical infrastructure required to facilitate a payment service. This includes vendors, infrastructure providers, and Technical Payment providers.

Service user: Service users are defined under Financial Services (Banking Reform) Act 2013 as those who use, or are likely to use, services provided by payment systems and is not limited to a specific group of users. Service users will include – banks who use payment services provided by other institutions; businesses; retailers; charities; government and consumers.

Settlement: The process by which a valid claim from the payee's institution is discharged by means of a payment from the payer's institution to the payee's institution. Specifically, the steps in the settlement process are: (a) collection and integrity check of the claims to be settled, (b) ensuring the availability of

funds for settlement, (c) settling the claims between the financial institutions, and (d) logging and communication of settlement to the parties concerned.

Single Euro Payments Area (SEPA): SEPA is a payment-integration initiative of the European Union with the objective to simplify bank transfers denominated in Euro. As of 2015, SEPA consists of the 28 member states of the European Union, the four member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco and San Marino. The project's aim is to improve the efficiency of cross-border payments and turn the fragmented national markets for euro payments into a single domestic one.

Single Immediate Payment (SIP): A payment set up to be paid immediately.

Small and Medium sized Enterprises (SMEs): Any business with typically less than 250 employees.

Standing Order (SO): A payment for a fixed amount to be paid regularly to the same beneficiary.

Sort Code and Account Number addressable accounts (SCAN): Accounts bearing a sort code and account number. They are the most common retail accounts in the UK i.e. current accounts, head office collection accounts and some saving accounts.

Third Party Service Provider (TPSP): Provide services across the payments value chain to facilitate the initiation, processing, acceptance, management and/or transmission of payments, as well as provision of information (e.g. technology providers, telecommunication providers, payment gateways/platforms, point of sale terminal providers, fraud management services).

Unattended payment: A payment where the payer who initiated the payment does not require a response. Unattended payments are typically bulk payments. Existing products that are likely to fall into this category are FPS SOP and FDP, Bacs DD and DC and ICS.

Unauthorised payment: A payment made without the customer's consent – for example, a payment made due to a bank error or one made using a stolen payment card.

Vendor: A technology provider of payment services.