Version 1.0
12 September 2018

OPEN BANKING

Open Banking Customer Experience Guidelines

Get Started ›

Contents

1.0 Introduction

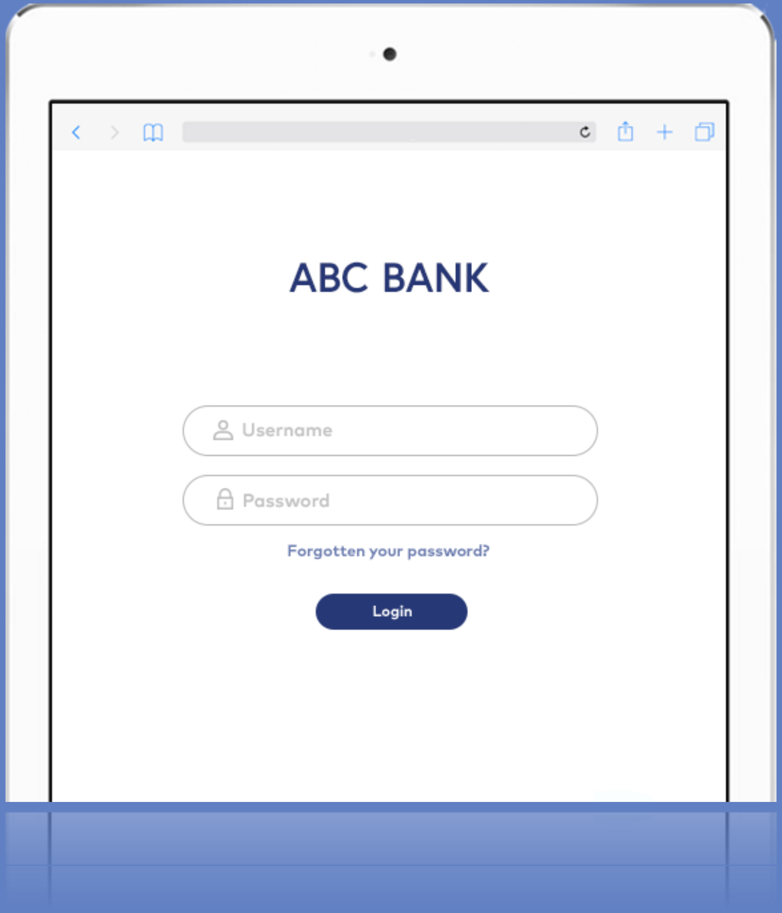
The Customer Experience Guidelines ("CEG") have been designed to facilitate widespread use of Open Banking-enabled products and services in a simple and secure manner. They bring together regulatory requirements and customer insight to create the Open Banking Standard for both TPPs and ASPSPs.

Customers will only use Open Banking products and services if their experience matches or betters their expectations, and information is presented in an intuitive manner that allows them to make informed decisions. It is therefore important that the interplay between the TPP and the ASPSP is as seamless as is possible while providing customer control in a secure environment. In particular it is essential that customers are clearly informed about the consent they are providing and the service they are receiving.

These Guidelines address the "Customer Journey", that is, the process that the customer follows from within a TPP's online app or browser, through to authentication within the ASPSP domain, and completion in the TPP domain.

The intended audience for these Guidelines is Open Banking Participants (ASPSPs, AISPs, PISPs and CBPIIs) and competent authorities with regulatory oversight of any Participant that adopts the Open Banking Standard. They should also be of use for Participants who build their own dedicated interface or adopt any other market initiative standard.

The contents of the CEG and CEG Checklist do not constitute legal advice. While the CEG and CEG Checklist have been drafted with regard to relevant regulatory provisions and best practice, they are not a complete list of the regulatory or legal obligations that apply to Participants. Although intended to be consistent with regulations and laws in the event of any conflict with such regulations and laws, those regulations and laws will take priority. Participants are responsible for their own compliance with all regulations and laws that apply to them, including without limitation, PSRs, PSD2, GDPR, consumer protection laws and anti-money laundering regulations.



1.1 The Customer Experience Guidelines form part of the Open Banking Standard Implementation Requirements

The European Banking Authority's (EBA) Draft Guidelines on the contingency mechanism exemption conditions state in Guideline 6 "where an ASPSP is implementing a market initiative standard, it should provide to its competent authority information as to which standard it is implementing and whether, and if so how, it has deviated from any standard implementation requirements of the initiative". The OBIE is therefore developing a range of Standard Implementation Requirements.

The Customer Experience Guidelines and Checklist form part of the Standard Implementation Requirements, and set out the customer experience required to deliver a successful Open Banking ecosystem, alongside technical, performance, non-functional requirements and dispute resolution practices.

The CEG Checklist has been developed for ASPSPs and TPPs to assess compliance to this aspect of the OBIE Standard Implementation Requirements.

The CEG and CEG Checklist are consistent with:

- The Revised Payment Services Directive (PSD2) (Transposed in the UK by the Payment Services Regulations 2017 (PSRs))
- The Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (RTS))
- The UK CMA Retail Banking Market Investigation Order which applies to the nine largest UK retail banks only (known as the CMA9)).

In developing its Standard Implementation Requirements, OBIE has undertaken extensive engagement with different market participants, and analysis to ensure that its standards have been designed in line with relevant regulatory and market requirements.

On this basis, where an ASPSP seeking an exemption notifies the relevant National Competent Authority (NCA) (e.g. the FCA in the UK) that its dedicated interface follows the OBIE Standard Implementation Requirements, we expect this will provide a level of assurance that the ASPSP meets the requirement of RTS Article 30(5). Conversely, when an ASPSP has deviated from the Standard Implementation Requirements, we expect that the NCA may require additional information to enable it to consider more closely whether the ASPSP's implementation is compliant with the relevant regulatory requirements. This may include the NCA requesting additional details on how and why there has been a deviation.

For this purpose, we would expect an ASPSP to complete and submit the CEG Checklist, providing supporting evidence as appropriate, to OBIE. This can then be provided to the NCA in support of its application for an exemption.

Customer Experience Checklist

The CEG Checklist takes the form of key questions that have been designated as either "required" or "recommended".

The CEG Checklist sets out which specific requirements are relevant to the Open Banking Standard Implementation Requirements, PSD2, the RTS and the CMA Order. Where relevant, it provides a regulatory reference (as per the CMA Order, PSD2/PSRs and the RTS on SCA and CSC). These are marked as either mandatory, optional or conditional in line with the definitions used across the Open Banking Standards.

For TPPs, certifying against the CEG Checklist is considered as a signal of best practice to the marketplace.

OBIE will consider the CEG Checklist for quality assurance and compliance purposes alongside other sources of information.

1.2 About these guidelines

These guidelines cover authentication and the core use cases that support market propositions

Customer insight and regulation-driven principles underpin the core customer journeys described in four sections:

- **Authentication Methods:** The primary forms of Authentication, in generic form, that may be used through a variety of services and interactions.
- **Account Information Services (AIS):** Service propositions that are enabled or initiated by customers (PSUs) consenting to share their payment account data with Account Information Service Providers.
- **Payment Initiation Services (PIS):** Service propositions enabled by customers (PSUs) consenting to Payment Initiation Service Providers (PISPs) initiating payments from their payment accounts.
- **Card Based Payment Instrument Issuers (CBPIIs):** Service propositions enabled by customers (PSUs) giving their consent to a CBPII to submit Confirmation of Funds (CoF) requests to an ASPSP.

ASPSPs should be familiar with their own role and that of other participants across all these proposition types.

TPPs (AISPs, PISPs and CBPIIs) will naturally focus on the proposition types that are relevant to their business model, but they should still be aware of the roles of all participants in order to ensure they understand the lines of demarcation and differences between each type.

The customer journey is described for each of the core use cases

Each unique journey has been broken out and described over a number of pages. They can be then be referenced in a number of ways according to individual priority e.g. whether the reader is, for example, a Regulatory Expert, Product Owner, Technical Lead or CX Designer. The page types are:

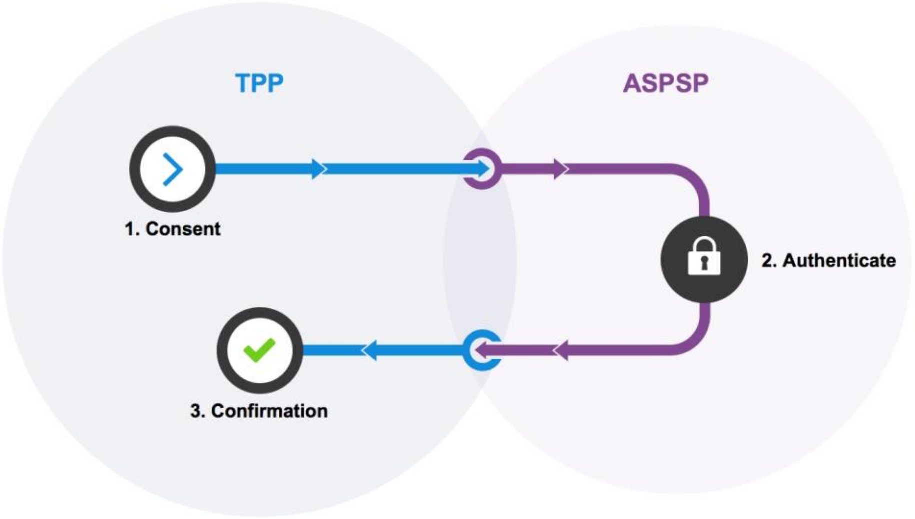
- **Journey description:** A high-level description of the specific account information, payment initiation or confirmation of funds customer journey.
- **A journey map:** This is a macro view of the customer journey, broken down by optimal steps and customer interaction points e.g. from payment initiation through authentication to completion.
- **A ‘wireframe’ journey:** This is represented by annotated ‘screens’ to identify key messages, actions, interactions and information hierarchy, as well as process dependencies.
- **Journey annotations:** This is the annotation detail referenced in the wireframes. These consist of both CEG Checklist items informing or requiring specific messaging or interactions etc. or CX considerations, where research has raised specific customer priorities or concerns that should be addressed through the eventual solution.

1.3 The Open Banking Customer Journey

For the purposes of the Customer Experience Guidelines as explained on the previous page, for each core use case customer journey, interaction and hand off have been broken into a set of clear, highly simplified white-label 'wireframes'. These are intended to be platform agnostic, to place focus on only the key elements within (e.g. messages, fields, checkboxes) and the specific number of steps that the customer must navigate. In all cases they are constructed around the primary Open Banking Customer Journey, which is illustrated to the right.

At the core of all Open Banking customer journeys is the mechanism by which the PSU gives consent to a TPP (AISP or PISP or CBPII) to access account information held at their ASPSP or to initiate payments from their ASPSP account.

In general, simplified terms, the consent request is initiated in the TPP domain (step 1 right). The PSU is then directed to the domain of its ASPSP for authentication (step 2 right). Then, once authentication is complete, the ASPSP will be able to respond to the TPP's account information or payment initiation request and redirect the PSU back to the TPP for confirmation and completion of the journey (step 3 right).



1.4 Design and experience principles

The OBIE has employed a number of design and experience principles to create the CEG. This section lays out the principles of informed decision making, providing customers with well designed experiences (using the principles of control, speed, transparency, security and trust) as well as how to protect vulnerable customers.

Open Banking products and services must place the customer in control

ASPSPs and TPPs should design customer journeys equivalent to or better than the journeys described in these guidelines in order to deliver the best possible experience and outcome.

Open Banking products and services must therefore enable:

- **Informed decision making**: Customer journeys must be intuitive and information must be easily assimilated in order to ensure informed customer decision making.
- **Simple and easy navigation**: There must be no unnecessary steps, delay or friction in the customer journey.
- **Parity of Experience:** The experience available to a PSU when authenticating a journey via a TPP should involve no more steps, delay or friction in the customer journey than the equivalent experience they have when interacting directly with their ASPSP.
- **Familiarity and trust:** The customer must only need to use the login credentials provided by the ASPSP.

1.4.1 Customer in control

The Open Banking Implementation Entity (OBIE) has undertaken considerable customer research over 18 months in order to understand how to enable customers to make informed decisions while enjoying a simple and easy navigation and a secure customer journey. A key principle throughout has been to ensure clarity of information, presented and described in a manner that ensures that Open Banking customer journeys are easy to understand, thereby enabling customers to make informed decisions. The results of this research have been shared with stakeholders as the foundations for Open Banking have been established.

The OBIE recognises that consumers and SMEs are not yet familiar with Open Banking enabled propositions. They have therefore had to interpret the concepts to be investigated based on their experience and the explanations provided in the research groups or panels. This form of ex-ante research has some limitations as there is often a difference between what customers say they will do and what they then actually do. Observed behaviours and attitudes from respondents have at times been contrary. For example, respondents will express a concern that they want to be secure and protected, but in practice they value convenience and will react with frustration to complex journeys often skimming the most important information. The consequence of this is that customers may not review the information sufficiently and may make decisions that they might later wish to reconsider. It has become clear that it is extremely important to minimise unnecessary information and process, and then to package only the most important information in an easily understandable, intuitive way so that the customer can actually assimilate the information and therefore make better informed decisions.

OBIE research has therefore identified information and steps which assist the customer as well as unnecessary steps, delays, inputs or additional information that may lead to customer frustration and subsequent drop out, or a failure to review important relevant information. In future research it is expected that further refinements based on ex-post data will be possible.

We examine the nature of both useful and unhelpful elements of the customer journey below.

Useful elements in the customer journey

Many customers are prone to skim through the information presented to them when setting up online products because the information is not well presented. In their desire to achieve the promised benefit, insufficient notice is taken of the implications of their actions, or the terms and conditions. It is commonplace to discover, once they have completed the customer journey, that they cannot spontaneously describe what they have just agreed to. The research has shown that a better understanding can be achieved by carefully designing the customer journey, and reveals that the solution is about effective, intuitive presentation of information, and is not about introducing steps to slow the customer down or repeating information. The following methods have been found to be the most effective:

- Effective messages and navigation appropriate to the redirection screens when the customer is redirected from the TPP to the ASPSP, and then again when the customer is redirected back from the ASPSP to the TPP. For a customer that has granted consent to the TPP the redirection screen creates a clear sense of separation as they enter the ASPSP's domain where they authenticate, before clearly being passed back to the TPP. This provides a familiar and trusted experience to the customer and signposts the customer's journey from one domain to the other.

1.4.1 Customer in control

- Providing useful information presented in an intuitive and easily consumable way. The principle here is to ensure that the information that the customer is presented with is kept to a minimum. If it is unavoidably necessary for the TPP to convey more complex information, it is more likely to be read and understood when presented as a series of smaller amounts of information across more than one screen. This is a much more effective method than the use of a single text-heavy screen.
- Providing supplementary information at specific points in the customer journey is useful, helping the customer to understand the process as well as ensuring comprehension of a product or offer and its implications. If executed well, it will enhance the customer journey and does not lead to increased propensity to drop off.

Unhelpful elements in the customer journey

The research has shown that superfluous information, poor or confusing choice of words, repetition, large amounts of text, too many steps or avoidable delays in the customer journey can lead to frustration, an even greater tendency to skim, and ultimately increase customer drop off. The following unhelpful elements were identified in the research and must be avoided:

- A customer authentication journey that takes too long and requires the use of separate devices such as one time password generators, especially if applied multiple times in the customer journey.
- Where there are fewer screens but a significant amount of text on the screen. This is particularly evident when this requires customers to scroll up and down the screen to progress the customer journey.
- Providing superfluous information that does not add to the customer's understanding or trust, especially when presented in a separate step or screen.
- Delays such as slow loading times, as well as web pages or apps that have not been effectively debugged, and unexpected crashing of web pages or apps.
- Inappropriate use of language, particularly language which may create a level of concern, uncertainty and doubt when going through the customer journey.
- The use of language that is too long, complex or legalistic to be easily understood when going through the customer journey.
- Asking for the same information twice, and asking for information for which there is no obvious purpose, e.g. replaying the consent to the customer that was granted to the TPP, or asking for a PIN when it is not needed.
- Forcing the customer to open a new browser window during the customer journey, and having to toggle between screens in order to progress.
- Introducing the requirement for a customer to input information that they don't readily have to hand, such as unique customer reference numbers
- Requesting input of information that could reasonably be expected to be pre-populated once the customer has authenticated.
- Failing to differentiate between new users and experienced regular users who may want to shorten the customer journey without exposing themselves to risk.

1.4.2 Customer experience principles

The Open Banking customer experience must ensure informed decision making while remaining understandable, intuitive and effective. The customer experience must be shaped and positioned into content and functionality that clearly communicates and facilitates purpose, intent and relevance.

This is especially true in a transactional context where customers need to know and understand at all times:

- Where they are in a specific process (and what they should expect from that process)
- Where they have come from
- What options, actions or steps they have in front of them (if any)
- The (implicit) consequences of taking those actions or next steps
- An unambiguous signal, feedback and/or response, once that action is taken

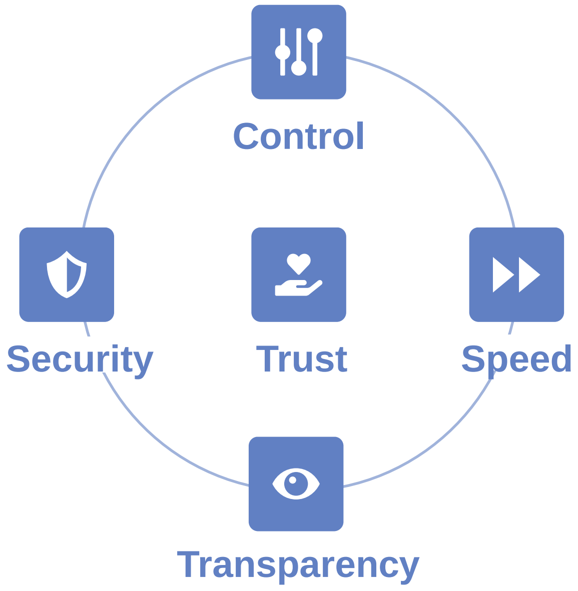
It is essential to move beyond the pure mechanics of the transactional process and into a meaningful, supportive and trusted experience that directly addresses the customer's needs, goals *and* concerns. This can be achieved in the way a transaction is structured, but also how it is expressed, designed for and organised around a range of fluctuating human needs.

A series of guiding 'experience principles' are outlined here that can be, through careful design, baked into a process or transaction, and dialled up and down where certain interactions become more critical.

These guiding experience principles are deeply customer-centred, shaped by research and insight that reflects and meets specific customer needs. They are used to drive and focus design and User Experience (UX) decisions i.e. what kind of widget, interaction, font, colour, technology, UX and User Interface (UI) best serves the aspirations and requirements of the business but also meets the needs of the customer in simple, effective ways.

Extensive customer research undertaken by OBIE has demonstrated certain recurring themes that customers deeply care about or are worried by. To promote engagement, understanding and ensure adoption these must be addressed, to varying degrees, within each of the Open Banking customer journeys described in these guidelines.

To support and achieve the goal of creating trust, these themes have been aggregated and synthesised into a number of driving experience principles for Open Banking. These principles underpin the range of core journeys and key customer interactions described throughout these guidelines.



1.4.2 Customer experience principles

Control

The introduction of any kind of new transaction, product or service - especially online - can create an opportunity for deeper engagement. However, it can also create barriers through poor implementation. From a consumer perspective, this is often about a perceived sense of control.

If customers feel they understand what is going on in a process, are able to make informed decisions and choices on their own terms - including recourse to change their mind - it provides a sense of ownership and control over what is happening. In a transactional context, where money and data are potentially at stake, getting this right is essential.

For Open Banking, control comes from providing the the right tools and clarity of information at the right time (e.g. knowing the account balance at the point of payment, or knowing that they can view and revoke consents given when they feel it is appropriate to do so).

TPPs and ASPSPs need to consider how they provide this sense of ownership and specific optionality throughout - enabling customers to feel this is a process they are both choosing and in charge of.

Speed

Speed must be appropriate to the customer and the journey they are undertaking. Convenient, speedy and intuitive design is a question of execution and interaction.

In transactional context, anything that seems more time consuming or onerous than customers are used to is going to represent a barrier to adoption. We have to manage and optimise each interaction, as well as hand-off between systems for speed, clarity and efficiency, but without sacrificing the principles of security and control.

In addition, we have to be mindful that speed of transaction or interaction is not necessarily about the ‘fastest possible’ experience. As we have indicated, we must support informed decision making through comprehension and clarity (especially in the context of AIS), allowing customers to, above all, move at a pace that suits them.

TPPs and ASPSPs need to ensure that Open Banking customer journeys remain flexible enough to support different customer contexts, expectations and situations and – critically - avoid any unnecessary friction in the completion of any journey.

Transparency

Transparency of choice, action, and importantly the consequences of actions or sharing of data is crucial to promoting the benefits of Open Banking, creating engagement and supporting adoption.

In new transactional scenarios where customers are being encouraged to share personal information this is critical. It is not only about communicating the benefits of a new service, but being explicitly clear on what is required from the customer, why it is required, and for what purposes. Customers need to be able to make an informed decision and, in turn, understand the consequences of that decision.

Sharing information is seen as unavoidable, and a trade-off for convenience and benefits. And while this is a great opportunity for TPPs and ASPSPs, the value exchange for the consumer needs to be explicitly clear.

At the same time, we do not want to overburden the customer or weigh down the business opportunity with excessive explanations. Transparency is about providing progressive levels of information, in plain language, that inform and support customer decisions.

Security

In the context of Security the key concerns for customers are fraud, which everyone understands, and data privacy, which is less well defined in the minds of consumers, since not everyone has the same idea about what ‘my data’ actually means (e.g. is it my name and address? Passwords? Names of my kids? Transactional history?) Nor is it well understood what businesses even do with their data once they get their hands on it. Such concerns can be even deeper amongst SMEs.

Explicit clarity and reassurance will be required in relation to data definition, usage, security and above all, protection.

In addition to personal data, transactional (data) security is the critical factor to ensure adoption of PISP services. As a minimum, TPPs and ASPSPs must ensure this is no less than consumers expect today.

As a new service, all security messaging should be clear and reassuring in tone, but not alarmist.

Trust

Customers are aware of the risks of sharing personal information and as expected some types of customer, particularly older demographics, may initially express cautiousness and nervousness.

It is therefore critical to establish and reinforce trustworthiness - trust in the service provider, trust in the transactional process and trust in the role and relationship with their ASPSPs, especially in a payment context where traditional, deeply established alternatives remain available.

The principles of control, speed, transparency and security combine to create a trusted environment for the customer.

TPPs and ASPSPs need to consider, engender and promote values of trust through every part of their Open Banking customer journeys, to foster understanding, acceptance and adoption of new innovative products and services.

1.4.3 Protection for vulnerable customers

Customers deemed as vulnerable, or in vulnerable circumstances, may be significantly less able to effectively manage or represent their own interests than the average customer, and more likely to suffer detriment. This may take the form of unusual spending, taking on unnecessary financial commitments or inadvertently triggering an unwanted event . Any customer can become vulnerable at any time in their life, for example through serious illness or personal problems such as divorce, bereavement or loss of income. Consent and data privacy issues are particularly relevant and important for people with mental health issues. Work done by the Money and Mental Health Policy Institute in the UK has shown the need to emphasise informed decision making, with appropriate steps and information in online experiences in order to help those with mental health problems to make informed decisions, understand the potential consequence of their decisions, or even deter a particular course of action.

ASPSPs have a particular responsibility to identify and protect vulnerable customers, needing to pay attention to possible indicators of vulnerability at a holistic level and have policies in place to deal with customers where those indicators suggest they may be at greater risk of harm. For those customers identified as vulnerable, the policies applied should be implemented at customer level, not at the transaction level or not specifically to Open Banking, just as is the case for vulnerable customers using other products provided by the ASPSP.

ASPSPs should take the following steps for vulnerable customers using products that make use of Open Banking:

- Provide support for vulnerable customers incorporating information from the Open Banking channel. ASPSPs should consider this issue holistically, treating Open Banking as they would any other customer channel. The ASPSP, having insight into customer behaviour, is well placed to provide the appropriate support, recognising that no single Open Banking customer journey should trigger vulnerability flags to the ASPSP.
- Provide useful and informative access dashboards within the ASPSPs domain that give vulnerable customers the control they need over their financial affairs and personal data. Vulnerable customers should be able to see full details of all the consents granted to TPPs, the data shared, the expiry date and to have the ability to revoke their consent.
- It is suggested that provision should be made in the ASPSP’s access dashboard enabling customers to switch on a summary information step as an opted-in choice. This represents a final chance for the customer to pause and review within the ASPSP’s domain so that this step is shown to them in all Open Banking customer journeys.

2.0 Authentication methods

One of the primary objectives of the Customer Experience Guidelines is to provide simplification and consistency across all Open Banking implementations. As such, we have defined a core set of authentication methods that can and should be used, subject to the scope and flexibility of any payment initiation and/or account information services provided by TPPs.

2.1 Overview

The EBA notes that "there would appear to currently be three main ways or methods of carrying out the authentication procedure of the PSU through a dedicated interface, and APIs in particular, namely redirection, embedded approaches and decoupled approaches (or a combination thereof). In the cases of redirection and decoupled approaches, PSU's authentication data are exchanged directly between PSUs and ASPSPs, as opposed to embedded approaches, in which PSU's authentication data are exchanged between TPPs and ASPSPs through the interface."

PSD2 requires strong customer authentication to be performed in certain circumstances. The RTS requires that this application of strong customer authorisation is based on the use of elements, which are categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is). These elements require adequate security features, which include ensuring that they are applied independently, so the breach of any element does not compromise the reliability off the other.

The Open Banking 2.0 standards specified redirection authentication flows only and the current ASPSP implementations of redirection are predominantly browser-based, whereby the PSU is redirected from the TPP app or website to the ASPSP's website in order to authenticate. It is essential that when redirection is implemented it also allows for the PSU to use their ASPSP mobile app to authenticate, if the PSU uses this method of authentication when accessing their ASPSP's channel directly.

Redirection has a specific TPP channel and device dependency and therefore cannot support channel agnostic use cases that involve telephony, POS, and IoT devices, or where physical PSU interaction is either not possible or not required within the TPP channel. These use cases can be supported using a decoupled approach to authentication.

In view of the above, the Open Banking 3.0 standards will support both redirection and decoupled authentication to allow a PSU to use the same authentication mechanisms while using an AISP or PISP as they use when accessing the ASPSP directly.

The three general principles that apply relating to authentication are:

1. **ASPSPs authenticate:** PSU needs to go through a strong customer authentication (SCA) at their ASPSP in order for a TPP request (i.e. access to information or payment initiation) to be actioned by the ASPSP.
2. **PSUs should have their normal authentication methods available:** A PSU should be able to use the elements they prefer to authenticate with their ASPSP if supported when interacting directly with their ASPSP.
3. **Parity of experience:** The experience available to a PSU when authenticating a journey via a TPP should involve no more steps, delay or friction in the customer journey than the equivalent experience they have with their ASPSP when interacting directly.

2.2 Redirection based authentication

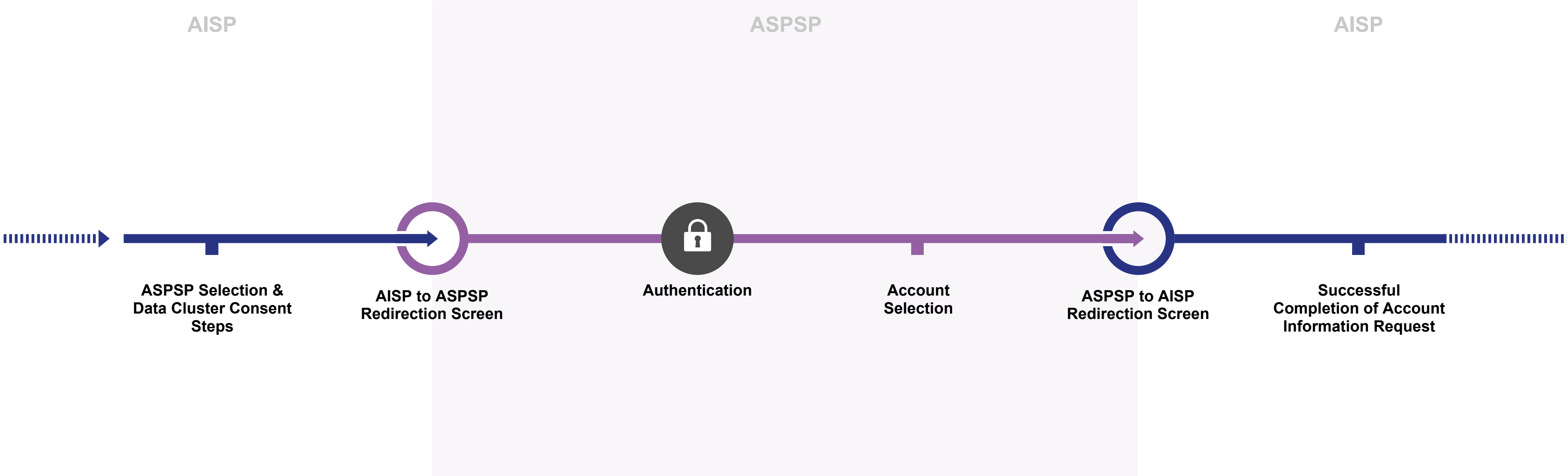
Redirection based authentication has a range of possible experiences for a PSU based on whether the PSU has an ASPSP app or not, and the device on which the PSU is consuming the TPP (AISP/PISP/CBPII) service.

We have used one example of AISP and PISP journey to demonstrate how redirection flows must work. These apply to variations in AIS/PIS/CBPII journeys related to the order of application of SCA and are covered in section 3, 4 and 5.

Featured journeys

2.2.1 Browser based redirection - AIS

User Journey | Wireframes | Requirements and Considerations


AISP
ASPSP
AISP
ASPSP Selection & Data Cluster Consent Steps
AISP to ASPSP Redirection Screen
Authentication
Account Selection
ASPSP to AISP Redirection Screen
Successful Completion of Account Information Request

PSU Authentication with the ASPSP using browser based redirection from an AISP for an AIS request.

Enables a PSU to authenticate with their ASPSP while using an AISP for AIS service, using the same web based authentication method which the PSU uses when accessing the ASPSP web channel directly.

This model works when the PSU is consuming the AISP service on a device that does not have the ASPSP app, or the PSU does not have the ASPSP mobile app.

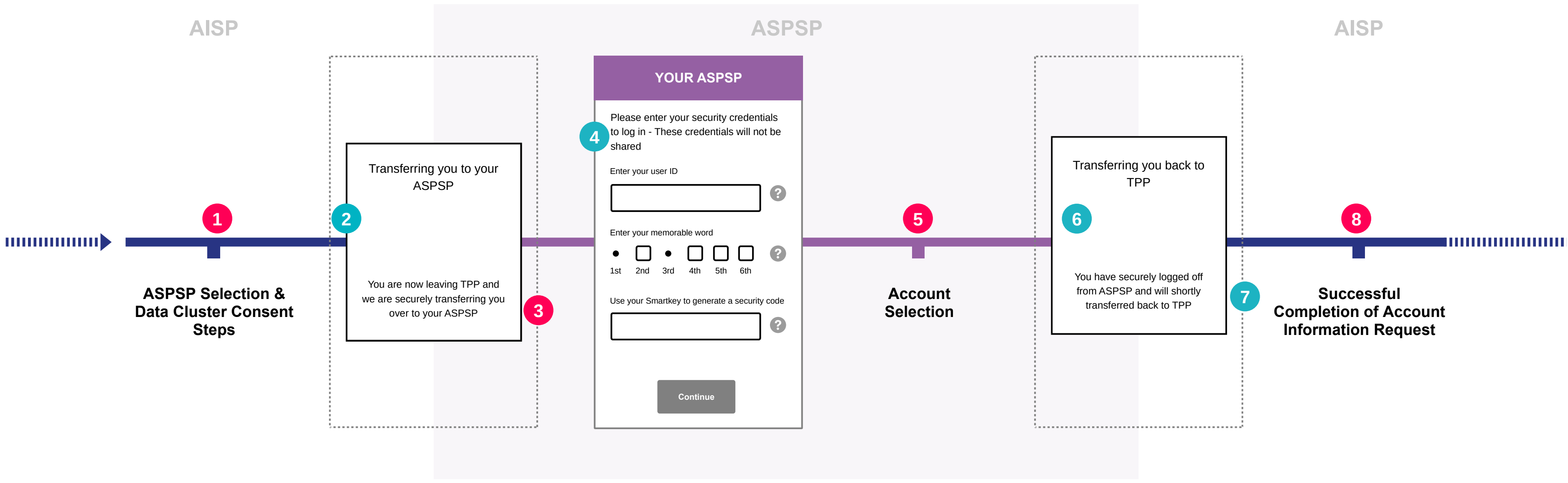
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

2.2.1 Browser based redirection - AIS

User Journey | **Wireframes** | Requirements and Considerations



ASPSP Selection & Data Cluster Consent Steps

Transferring you to your ASPSP

You are now leaving TPP and we are securely transferring you over to your ASPSP

YOUR ASPSP

Please enter your security credentials to log in - These credentials will not be shared

Enter your user ID

Enter your memorable word

● 1st □ 2nd ● 3rd □ 4th □ 5th □ 6th

Use your Smartkey to generate a security code

Continue

Account Selection

Transferring you back to TPP

You have securely logged off from ASPSP and will shortly transferred back to TPP

Successful Completion of Account Information Request

2.2.1 Browser based redirection - AIS

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	AISP **must** initially ask the PSU to identify the ASPSP so that the consent request can be constructed in line with the ASPSP's data clusters.	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	AISP	Required
3	The redirection **must** take the PSU to the ASPSP web page (desktop/mobile) for authentication purposes only without introducing any additional screens. The web based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the web based ASPSP channel (desktop/mobile).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
5	PSU **must** be able to confirm the account(s) which they would like the AISP to have access to without having to go through any further unnecessary screens.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
8	AISP **should** confirm the successful completion of account information data request.	• n/a	18	AISP	Recommended

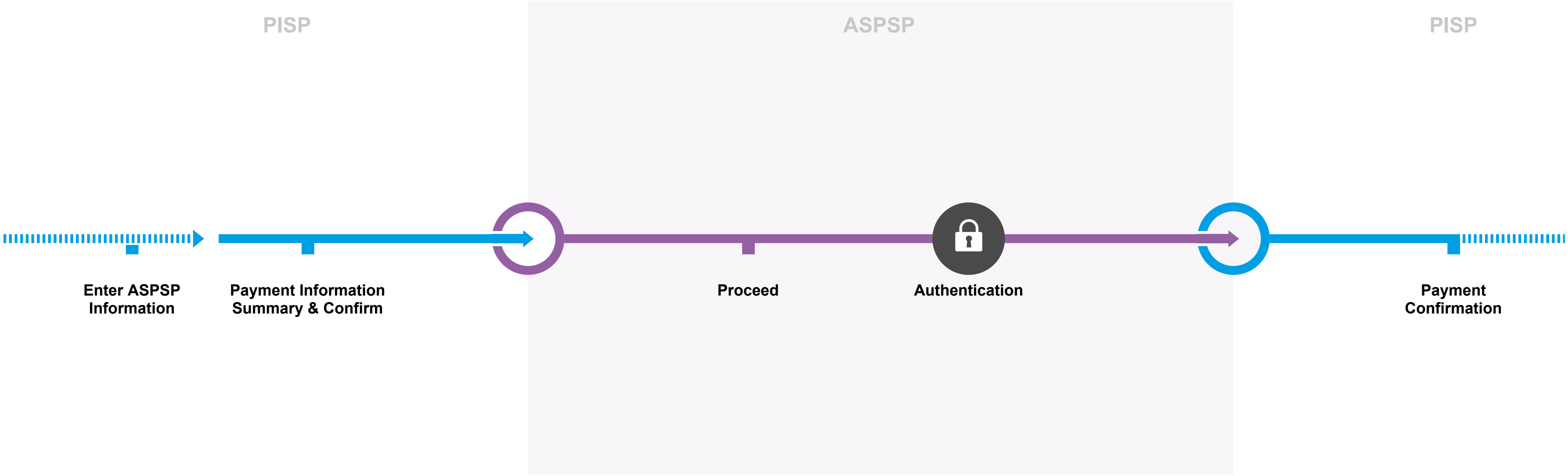
	CX Considerations
2	AISP **should** make the PSU aware that they will be taken to their ASPSP for authentication.
4	ASPSP **should** make the PSU aware that the PSU login details will not be visible to the AISP.
6	ASPSP **should** have intermediary screen which indicates the status of the request and informing the PSU that they will be automatically taken back to the AISP.
7	ASPSP **should** inform the PSU on the intermediary screen that their session with the ASPSP is closed.

To demonstrate web based redirection part of the journey we have used AISP initial setup (Sec 3.1.1) as one example.

The redirection flow applies to other AIS journeys covered in detail under **Section 3.**

2.2.1 Browser based redirection - PIS

User Journey | Wireframes | Requirements and Considerations



PSU Authentication with the ASPSP using browser based redirection for a PIS request.

Enables a PSU to authenticate with their ASPSP while using a TPP for PIS service, using the same web based authentication method which they use when accessing the ASPSP web channel directly.

This model works when the PSU is consuming the PIS service on a device that does not have the ASPSP app, or the PSU does not have the ASPSP mobile app.

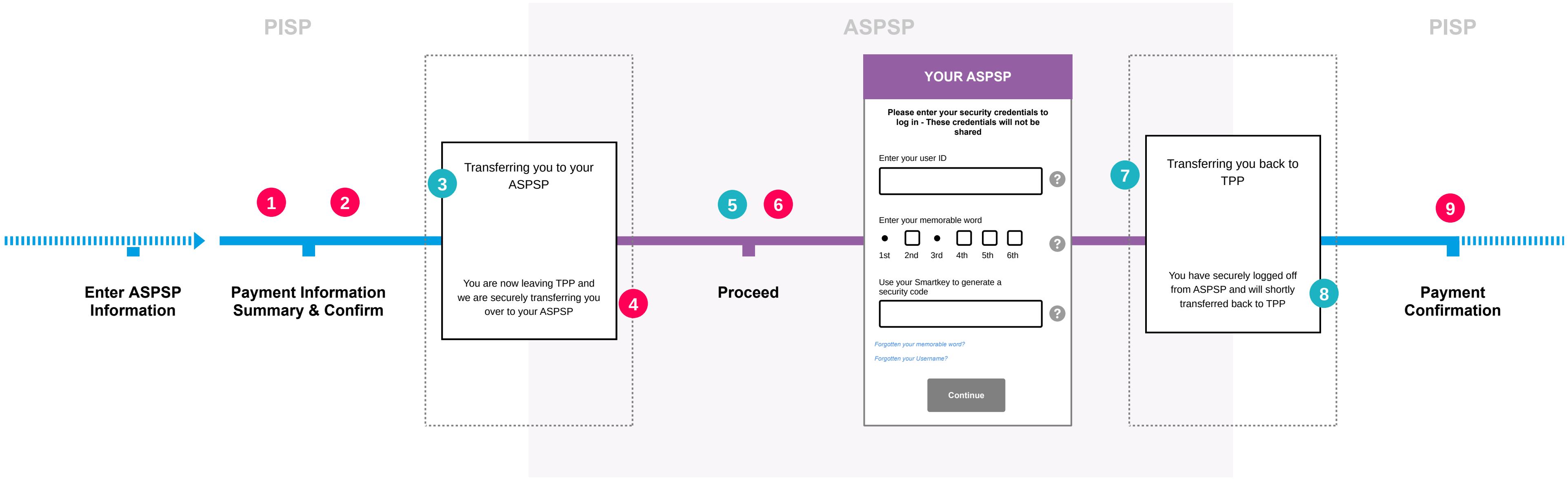
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

2.2.1 Browser based redirection - PIS

User Journey | Wireframes | Requirements and Considerations



Transferring you to your ASPSP

You are now leaving TPP and we are securely transferring you over to your ASPSP

YOUR ASPSP

Please enter your security credentials to log in - These credentials will not be shared

Enter your user ID

Enter your memorable word

● 1st □ 2nd ● 3rd □ 4th □ 5th □ 6th

Use your Smartkey to generate a security code

Forgotten your memorable word?

Forgotten your Username?

Continue

Transferring you back to TPP

You have securely logged off from ASPSP and will shortly transferred back to TPP

What the research says

Research amongst consumers has shown that 29% of participants actively prefer a browser based PIS journey for a single domestic payment, whilst 32% prefer an app based journey. Those preferring a browser based journey refer to security and ease to explain their choice. Those preferring the app based alternative select it because they deem it easier than the web based experience, with fewer mentioning security.

> See more

2.2.1 Browser based redirection - PIS

User Journey | Wireframes | Requirements and Considerations

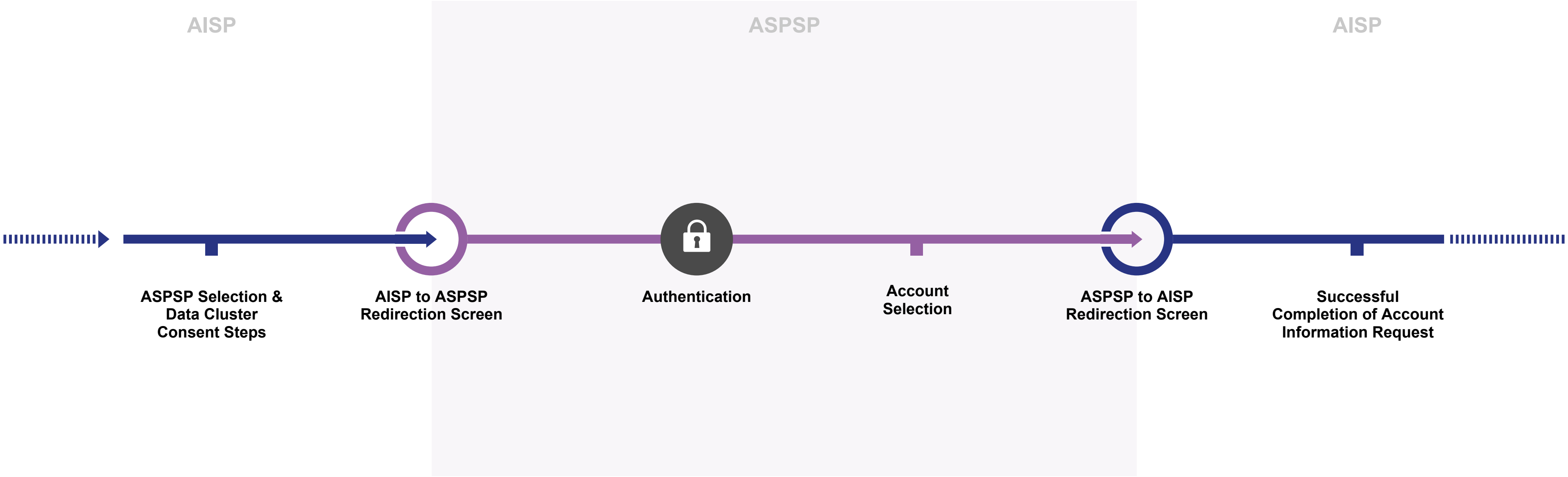
	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**PSU payment Account Selection** PISPs **must** provide PSUs at least one of the following options: • enter their Payer's payment Account Identification details • select their Account Identification details (this assumes they have been saved previously)	• n/a	24	PISP	Required
2	The PISP **must** communicate information clearly to the PSU when obtaining consent in order to initiate the payment order.	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
4	The redirection **must** take the PSU to a ASPSP web page (desktop/mobile) for authentication purposes only without introducing any additional screens.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
6	The ASPSP web based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the web based ASPSP channel (desktop/mobile).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
9	PSU **must** be redirected straight back to the PISP website/app on the same device where PISP displays confirmation of successful initiation.	• PSR Reg. 44(1)	26	PISP	Required

	CX Considerations
3	ASPSP **should** make the PSU aware through an intermediary screen that they are being taken to their ASPSP for authentication to complete the payment.
5	ASPSP **should** display the amount and payee of the payment as part of the authentication journey.
7	ASPSP **should** have intermediary screen which indicates the status of the request and informs the PSU that they will be automatically taken back to the PISP.
8	ASPSP **should** inform the PSU on the intermediary screen that their session with the ASPSP is closed.

To demonstrate web based redirection we have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order from the PISP. This redirection flow applies to other variations of PIS journeys covered in detail under **Section 4.**

2.2.2 App based redirection - AIS

User Journey | Wireframes | Requirements and Considerations


AISP
ASPSP
AISP
ASPSP Selection & Data Cluster Consent Steps
AISP to ASPSP Redirection Screen
Authentication
Account Selection
ASPSP to AISP Redirection Screen
Successful Completion of Account Information Request

PSU authentication with the ASPSP using the ASPSP mobile app installed on the same device on which the PSU is consuming the AISP service.

Enables the PSU to authenticate with the ASPSP while using an AISP for AIS service using the same ASPSP app based authentication method which they use when accessing the ASPSP mobile channel directly.

AISP service could be web based or app based. The redirection must directly invoke the ASPSP app to enable the PSU to authenticate and must not require the PSU to provide any PSU identifier or other credentials to the AISP.

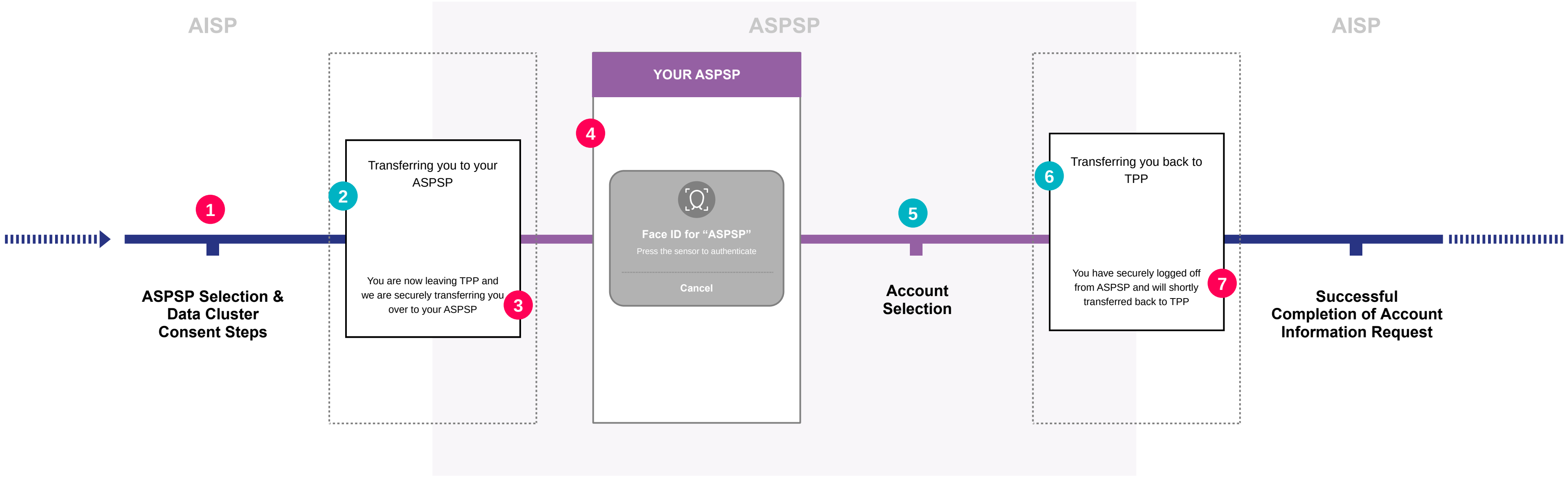
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

2.2.2 App based redirection - AIS

User Journey | **Wireframes** | Requirements and Considerations


AISP
ASPSP
AISP
1
ASPSP Selection & Data Cluster Consent Steps
2
Transferring you to your ASPSP
You are now leaving TPP and we are securely transferring you over to your ASPSP
3
YOUR ASPSP
4
Face ID for “ASPSP”
Press the sensor to authenticate
Cancel
5
Account Selection
6
Transferring you back to TPP
You have securely logged off from ASPSP and will shortly transferred back to TPP
7
Successful Completion of Account Information Request

2.2.2 App based redirection - AIS

User Journey | Wireframes | Requirements and Considerations

CEG Checklist Requirements		Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	AISP **must** initially ask PSU to identify ASPSP so that the consent request can be constructed in line with the ASPSP's data cluster capabilities.	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	AISP	Required
3	If the PSU has an ASPSP app installed on the same device the redirection **must** invoke the ASPSP app for authentication purposes only without introducing any additional screens. The ASPSP app based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app(biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
4	After authentication the PSU **must** be **deep linked within the app** to confirm the account(s) which they would like the AISP to have access to without having to go through any further mandatory screens. **For details on deep linking see** Appendix 7.3.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
7	The AISP **should** confirm the successful completion of the account information request.	• n/a	18	AISP	Recommended

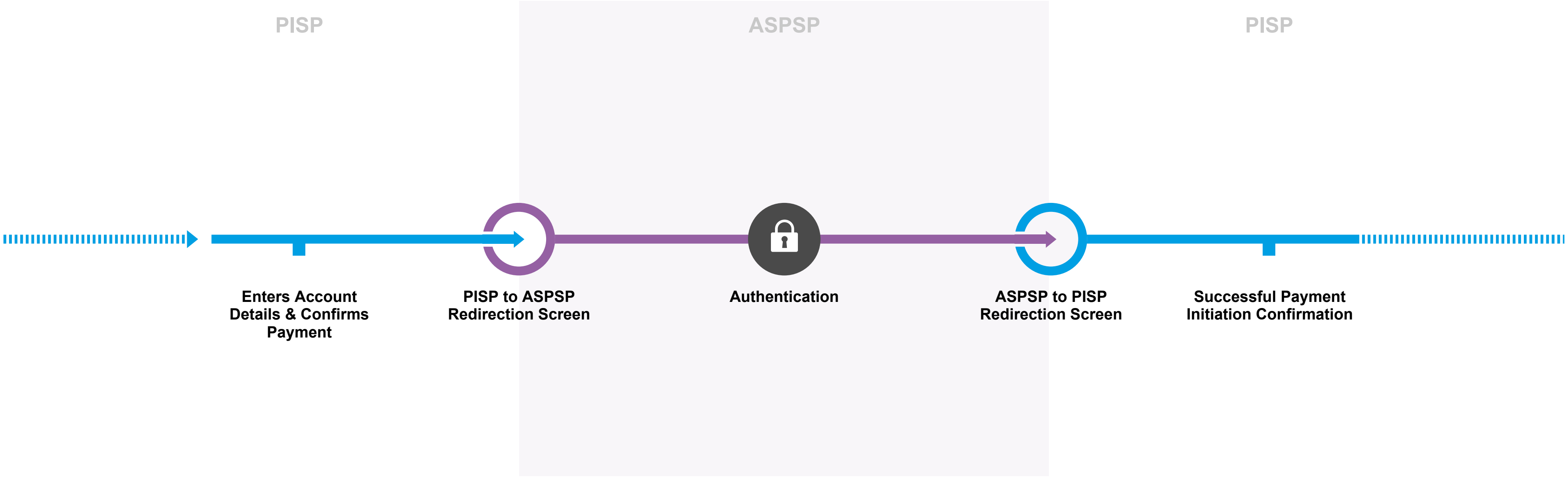
CX Considerations	
2	AISP **should** make the PSU aware that they will be taken to their ASPSP for authentication.
5	ASPSP **should** have intermediary screen which indicates the status of the request and informing the PSU that they will be automatically taken back to the AISP.
6	ASPSP **should** inform the PSU on the intermediary screen that their session with the ASPSP is closed.

To demonstrate an app based redirection part of the journey we have used AISP initial setup (Sec 3.1.1) as one example.

The app based redirection flow applies to other AIS journeys covered in detail under **Section 3.**

2.2.2 App based redirection - PIS

User Journey | Wireframes | Requirements and Considerations


PISP
ASPSP
PISP
Enters Account Details & Confirms Payment
PISP to ASPSP Redirection Screen
Authentication
ASPSP to PISP Redirection Screen
Successful Payment Initiation Confirmation

PSU authentication, with the ASPSP using the ASPSP mobile app installed on the same device on which the PSU is consuming the PISP service.

Enables the PSU to authenticate with the ASPSP while using a PISP for PIS, service using the same ASPSP app based authentication method that they use when accessing the ASPSP mobile channel directly.

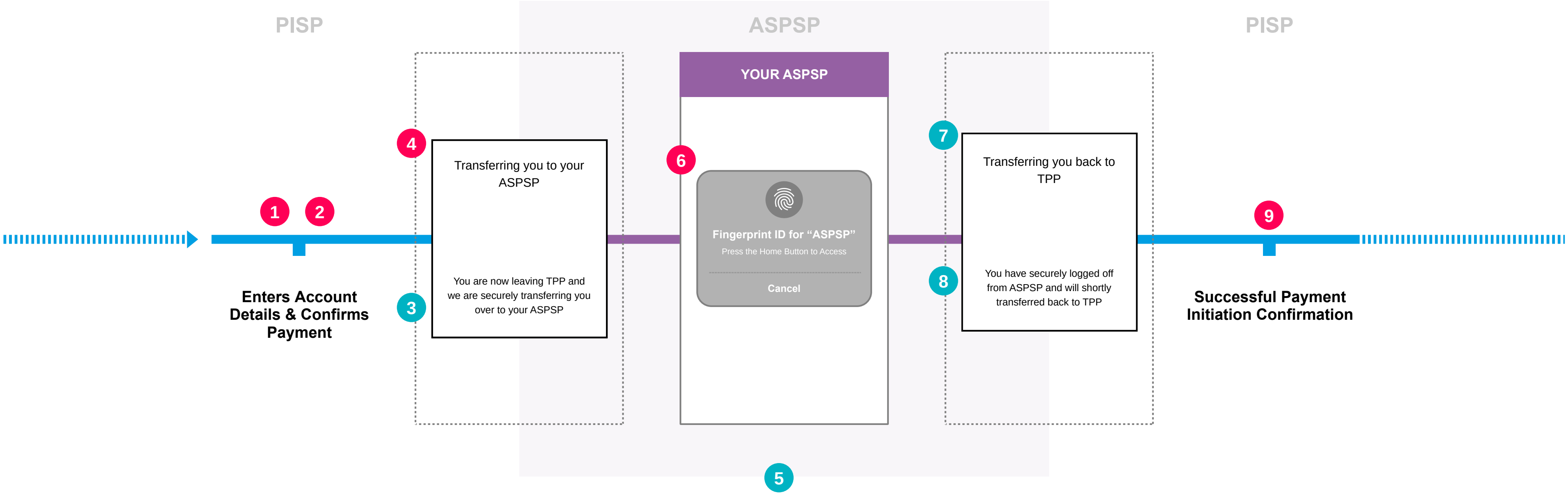
The PISP service could be web based or app based. The redirection must directly invoke the ASPSP app to enable the PSU to authenticate, and must not require the PSU to provide any PSU identifier or other credentials to the PISP.

Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

2.2.2 App based redirection - PIS


PISP
ASPSP
PISP
1
2
Enters Account Details & Confirms Payment
4
3
Transferring you to your ASPSP
You are now leaving TPP and we are securely transferring you over to your ASPSP
YOUR ASPSP
6
Fingerprint ID for "ASPSP"
Press the Home Button to Access
Cancel
5
7
8
Transferring you back to TPP
You have securely logged off from ASPSP and will shortly transferred back to TPP
9
Successful Payment Initiation Confirmation

What the research says

Consumer research has shown that people feel authentication via Fingerprint ID adds a reassuring sense of security to the journey.

> See more

2.2.2 App based redirection - PIS

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	PISP **must** allow the PSU to either enter the account details or select the account with their ASPSP.	• n/a	24	PISP	Required
2	The PISP **must** communicate information clearly to the PSU when obtaining consent in order to initiate the payment order.	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
4	If the PSU has an ASPSP app installed on the same device the redirection **must** invoke the ASPSP app for authentication purposes only without introducing any additional screens.	• EBA Draft Guideline 5.1(b) • EBA Opinion paragraph 50 • Trustee P3/P4 letter Action P3 A6	5a	ASPSP	Required
6	The ASPSP app based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app (biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
9	PSU **must** be redirected straight back to the PISP website/app on the same device where PISP displays confirmation of successful initiation.	• PSR Reg. 44(1)	26	PISP	Required

	CX Considerations
3	PISP **should** provide messaging to inform PSU that they will be taken to their ASPSP to complete the payment.
5	ASPSP **should** display the amount and payee of the payment as part of the authentication journey.
7	ASPSP **should** have intermediary screen which indicates the status of the request and informs the PSU that they will be automatically taken back to the PISP.
8	ASPSP **should** inform the PSU on the intermediary screen that their session with the ASPSP is closed.

To demonstrate an app based redirection part of the journey we have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order from the PISP.
This redirection flow applies to other variations of PIS journeys covered in detail under Section 4.

2.2.3 App-to-browser redirection – AIS

It is possible that a PSU using a mobile device does not have their ASPSP mobile app installed, or their ASPSP does not provide an app at all. In these instances, the TPP app will need to launch the native mobile browser in order to present the PSU with their ASPSP's web channel to authenticate.

It is imperative in these circumstances that the browser channel has been optimised for mobile browser and device type.

2.2.4 Browser-to-app redirection

Conversely, a TPP may be browser only, but this should not preclude a PSU from having their ASPSP app invoked if the PSU is using a mobile browser, and has the ASPSP app installed on their device. In this situation the TPP browser should invoke the app for authentication, and following authentication the PSU needs to be redirected back to the TPP browser.

If a PSU is using a desktop to access the TPP, then under the redirection model the journey will have to be completed on the ASPSP browser channel. Only with Decoupled authentication can the PSU use their app to authenticate in this situation.

2.2.5 Effective use of redirection screens

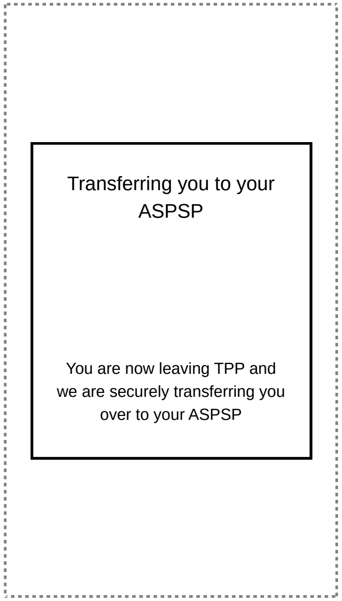
Within a typical redirection journey, a customer is presented with two redirection screens by the ASPSP:

- Redirection from the TPP domain to ASPSP domain, after the PSU has provided consent to the TPP for the account information or payment initiation service.
- Redirection from the ASPSP domain to TPP domain, after the ASPSP has authenticated the PSU.

The research has suggested that the redirection screens are a useful part of the process, providing customer trust. The following reasons are noted:

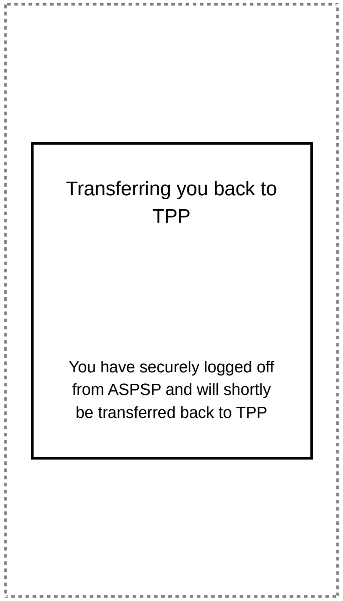
- They help customers navigate their online journey and inform them of what is going to happen next.
- They help create a clear sense of separation between the TPP's domain and the ASPSP's domain.

The research has suggested the messaging on the redirection screens serves to reassure the customer that they are in control, and helps engender trust. For example, customers will be more willing to trust the process if they feel there is a partner (TPP or ASPSP) on their side that is known and reputable (use language such as 'we', 'our'). In this sense, use of words that indicate that the customer is in control and taking the lead are key, as these are indications that the TPP or the ASPSP is working with or for the customer.



Transferring you to your ASPSP

You are now leaving TPP and we are securely transferring you over to your ASPSP



Transferring you back to TPP

You have securely logged off from ASPSP and will shortly be transferred back to TPP

2.3 Decoupled authentication

A major addition to the Open Banking standards known as "Decoupled" authentication, where typically the PSU uses a separate, secondary device to authenticate with the ASPSP. This model allows for a number of innovative solutions and has the added benefit of allowing a PSU to use their mobile phone to authenticate, taking advantage of biometrics for SCA, where they are engaging with a PISP through a separate terminal such as a point of sale (POS) device.

We have used examples for a PIS journey, but the same principles apply for a AIS and CBPII journeys.

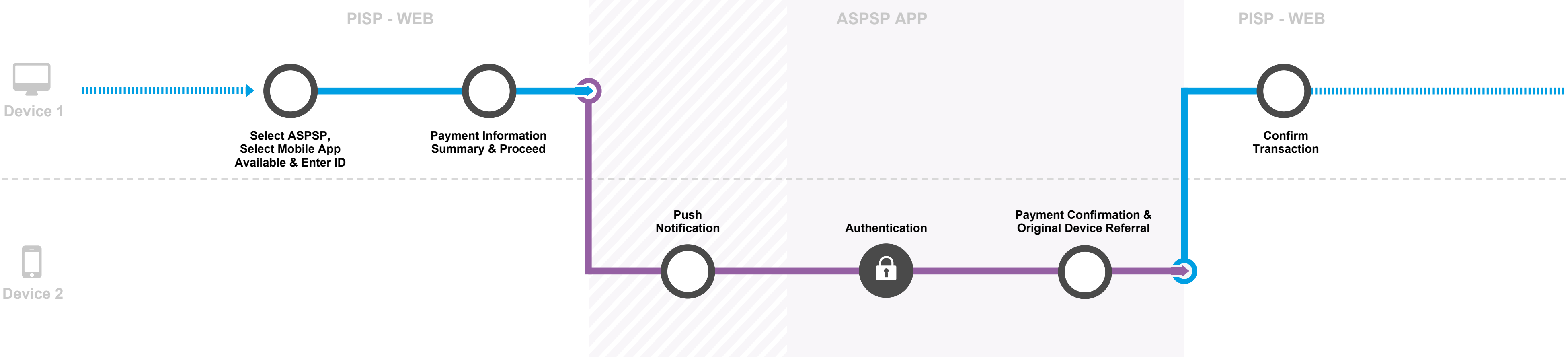
Under the Decoupled standard, the following customer experiences are available:

Featured journeys

2.3.1 Model A: Static PSU identifier

PSU provides a static identifier to the TPP (AISP/PISP/CBPII) which is passed to ASPSP to identify the PSU

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations


PISP - WEB
ASPSP APP
PISP - WEB
Device 1
Device 2
Select ASPSP, Select Mobile App Available & Enter ID
Payment Information Summary & Proceed
Confirm Transaction
Push Notification
Authentication
Payment Confirmation & Original Device Referral

A decoupled authentication flow where the PSU provides a static identifier to the TPP (AISP/PISP/CBPII) which is used by the ASPSP to notify the PSU, such that the PSU can authenticate using the ASPSP app on a separate device.

This enables the PSU to use the same app based authentication method with their ASPSP they use when accessing the ASPSP mobile app directly.

This model is best suited to TPP apps with good user input options (e.g. website on PC/laptop), but also where POS terminals can scan debit card numbers and automatically resolve the ASPSP if these are used as a customer identifiers.

The exact type of identifier supported by the ASPSP must be published by the ASPSP.

Relevant Customer Insight and supporting regulation

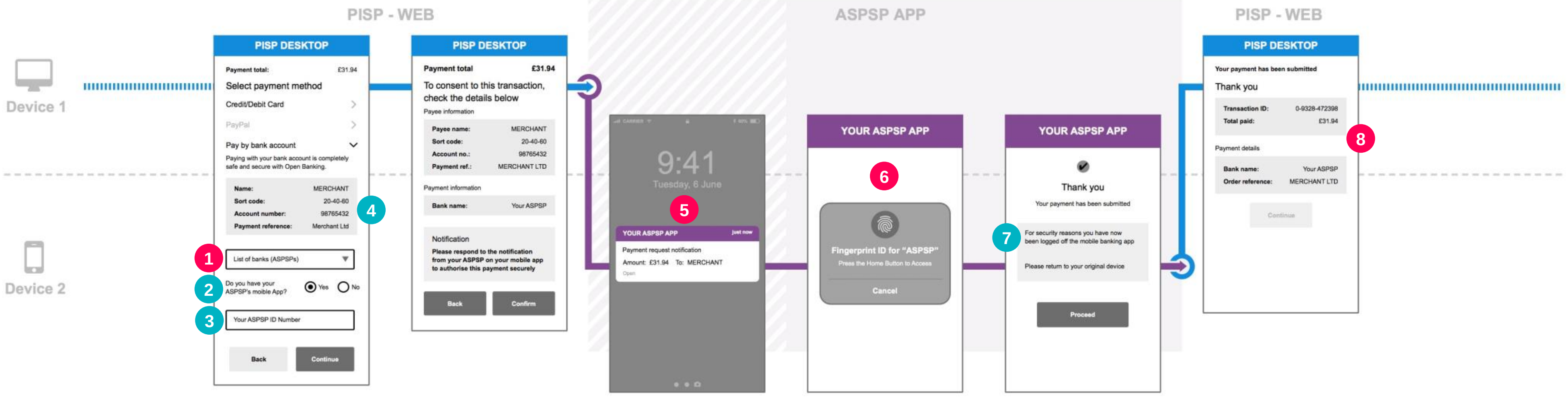
> View CX Customer Research

> View CEG Checklist

2.3.1 Model A: Static PSU identifier

PSU provides a static identifier to the TPP (AISP/PISP/CBPII) which is passed to ASPSP to identify the PSU

User Journey | **Wireframes** | CEG Checklist Requirements | CX Considerations



PISP DESKTOP

Payment total:	£31.94

Select payment method

Credit/Debit Card >

PayPal >

Pay by bank account ∨

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

List of banks (ASPSPs) ▼

Do you have your ASPSP's moible App? ● Yes ○ No

Your ASPSP ID Number

Back | Continue

PISP DESKTOP

Payment total	£31.94

To consent to this transaction, check the details below

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP

Notification

Please respond to the notification from your ASPSP on your mobile app to authorise this payment securely

Back | Confirm

CARRIER

9:41

Tuesday, 6 June

YOUR ASPSP APP just now

Payment request notification

Amount: £31.94 To: MERCHANT

Open

YOUR ASPSP APP

Fingerprint ID for "ASPSP"

Press the Home Button to Access

Cancel

YOUR ASPSP APP

✔

Thank you

Your payment has been submitted

For security reasons you have now been logged off the mobile banking app

Please return to your original device

Proceed

PISP DESKTOP

Your payment has been submitted

Thank you

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Order reference:	MERCHANT LTD

Continue

What the research says

Research shows that consumers are familiar with decoupled authentication when making a payment or setting up a new payment. This means that, if PIS journey designs follow similar patterns, consumers will be comfortable with them. Many welcome the additional level of security decoupled authentication provides.

> See more

2.3.1 Model A: Static PSU identifier

PSU provides a static identifier to the TPP (AISP/PISP/CBPII) which is passed to ASPSP to identify the PSU

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**PSU payment Account Selection** PISPs **must** provide PSUs at least one of the following options: • enter their Payer's payment Account Identification details • select their Account Identification details (this assumes they have been saved previously)	• n/a	24	PISP	Required
5	After the PSU enters the specified identifier, if the PSU has an ASPSP app then the ASPSP **must** notify the PSU through the ASPSP app for authentication purposes without introducing any additional screens. The notification **must** clearly mention the payment request with the amount and the payee.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
6	The ASPSP app based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app (biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
8	The PISP **must** confirm successful confirmation of payment initiation	• PSR.Reg 44(1)	26	PISP	Required

To demonstrate a Model A based decoupled journey we have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order from the TPP.
This flow applies to other variations of PIS journeys covered in detail under Section 4, AISP journeys covered under Section 3 and CBPII journeys covered under Section 5.

2.3.1 Model A: Static PSU identifier

PSU provides a static identifier to the TPP (AISP/PISP/CBPII) which is passed to ASPSP to identify the PSU

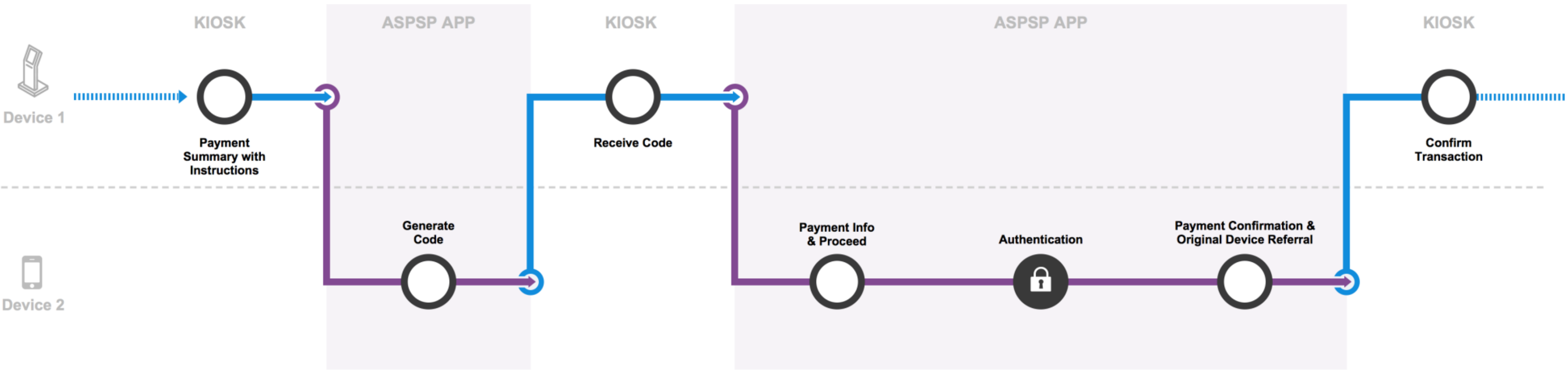
User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

CX Considerations	
2	The PISP **should** present the PSU the authentication options supported by the ASPSP which in turn can be supported by the TPP device/channel (for e.g. A TPP kiosk that can only support authentication by ASPSP mobile app).
3	If the PISP and the ASPSP supports Model A then the TPP **should** request from the PSU the identifier which is supported by their ASPSP.
4	The PISP **should** make the PSU aware about how this identifier will be used.
7	If the PSU is logged off from the ASPSP app, the ASPSP must make the PSU aware that they have been logged off and notify them to check back on the originating TPP app.

2.3.2 Model B: ASPSP generated identifier

PSU provides an ASPSP generated unique identifier to the TPP (AISP/PISP/CBPII) which is then passed back to ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations



A decoupled authentication flow where the PSU provides a dynamic identifier generated with their ASPSP to the TPP(AISP/PISP/CBPII), which is then used by the ASPSP to identify the PSU through the ASPSP app to authenticate and action the TPP request.

This model is best suited to a TPP app that can "capture" the code from the ASPSP app (e.g. by scanning a QR code).

Alternatively, the PSU can be prompted to type in an identifier in the TPP App. This may be a long series of characters and may result in a sub-optimal customer experience.

Relevant Customer Insight and supporting regulation

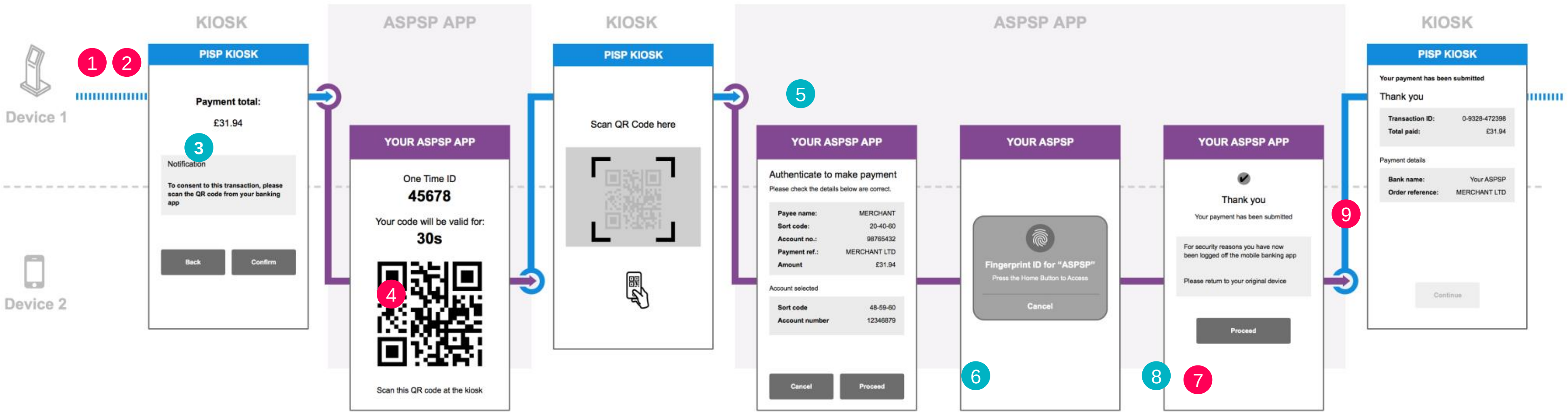
> View CX Customer Research

> View CEG Checklist

2.3.2 Model B: ASPSP generated identifier

PSU provides an ASPSP generated unique identifier to the TPP (AISP/PISP/CBPII) which is then passed back to ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations



PISP KIOSK

Payment total:

£31.94

Notification

To consent to this transaction, please scan the QR code from your banking app

Back | Confirm

YOUR ASPSP APP

One Time ID

45678

Your code will be valid for:

30s

Scan this QR code at the kiosk

PISP KIOSK

Scan QR Code here

YOUR ASPSP APP

Authenticate to make payment

Please check the details below are correct.

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD
Amount	£31.94

Account selected

Sort code	48-59-60
Account number	12346879

Cancel | Proceed

YOUR ASPSP

Fingerprint ID for "ASPSP"

Press the Home Button to Access

Cancel

YOUR ASPSP APP

✔

Thank you

Your payment has been submitted

For security reasons you have now been logged off the mobile banking app

Please return to your original device

Proceed

PISP KIOSK

Your payment has been submitted

Thank you

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Order reference:	MERCHANT LTD

Continue

We have illustrated an example where the dynamic identifier is a QR code and is scannable by the TPP. The code generated by the ASPSP is however not limited to QR code.

The general guidance is that the code generation with the ASPSP should not introduce friction in the journey.

What the research says

Research shows that consumers are familiar with decoupled authentication when making a payment or setting up a new payment. This means that, if PIS journey designs follow similar patterns, consumers will be comfortable with them. Many welcome the additional level of security decoupled authentication provides.

> See more

2.3.2 Model B: ASPSP generated identifier

PSU provides an ASPSP generated unique identifier to the TPP (AISP/PISP/CBPII) which is then passed back to ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1,2	Not shown in the diagram but as in 1 & 2 in Model A.	• RTS Art. 36(4)	22	PISP	Required
4	PSU uses the ASPSP app to generate the unique identifier.	• EBA Opinion paragraph 50 • Trustee P3/P4 letter Action P4 A2	6	ASPSP	Recommended
7	ASPSPs **must** apply SCA which should have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app (biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
9	The PISP **must** confirm successful confirmation of payment initiation.	• PSR.Reg 44(1)	26	PISP	Required

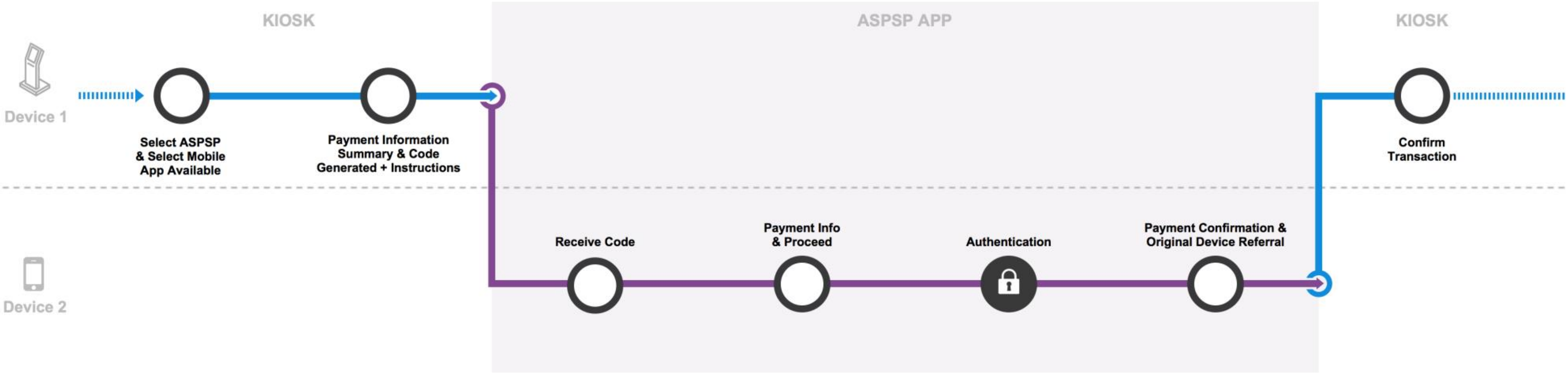
	CX Considerations
3	If the PISP and the ASPSP support Model B then the PISP **should** provide the PSU information on how the identifier can be generated with their ASPSP and make the PSU aware about how this identifier will be used.
5	The PSU **should** be able to easily provide the identifier to the PISP application (e.g. scan the code into the Kiosk in this instance).
6	After the PSU provides the ASPSP app generated identifier to the PISP then the ASPSP **must** display the payment request within the same session of the ASPSP app and clearly mention the amount and the payee.
8	The ASPSP **must** make the PSU aware that they have been logged off from the ASPSP app and notify them to check back on the originating PISP app.

To demonstrate a Model B based decoupled journey we have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order from the PISP.
This flow applies to other variations of PIS journeys covered in detail under Section 4, AISP journeys covered under Section 3 and CBPII journeys covered under Section 5.

2.3.3 Model C: TPP generated identifier

PSU provides a TPP (AISP/PISP/CBPII) generated unique identifier to the ASPSP to identify the request from the TPP

User Journey | Wireframes | Requirements and Considerations


KIOSK
ASPSP APP
KIOSK
Device 1
Device 2
Select ASPSP & Select Mobile App Available
Payment Information Summary & Code Generated + Instructions
Confirm Transaction
Receive Code
Payment Info & Proceed
Authentication
Payment Confirmation & Original Device Referral

A decoupled authentication flow where the PSU provides a dynamic identifier generated with their ASPSP to the TPP (AISP/PISP/CBPII), which is then used by the ASPSP to identify the PSU through the ASPSP app to authenticate and action the TPP request.

This model is best suited to a TPP app that can "capture" the code from the ASPSP app (e.g. by scanning a QR code). Alternatively, the PSU can be prompted to type in an identifier in the TPP App. This may be a long series of characters and may result in a sub-optimal customer experience.

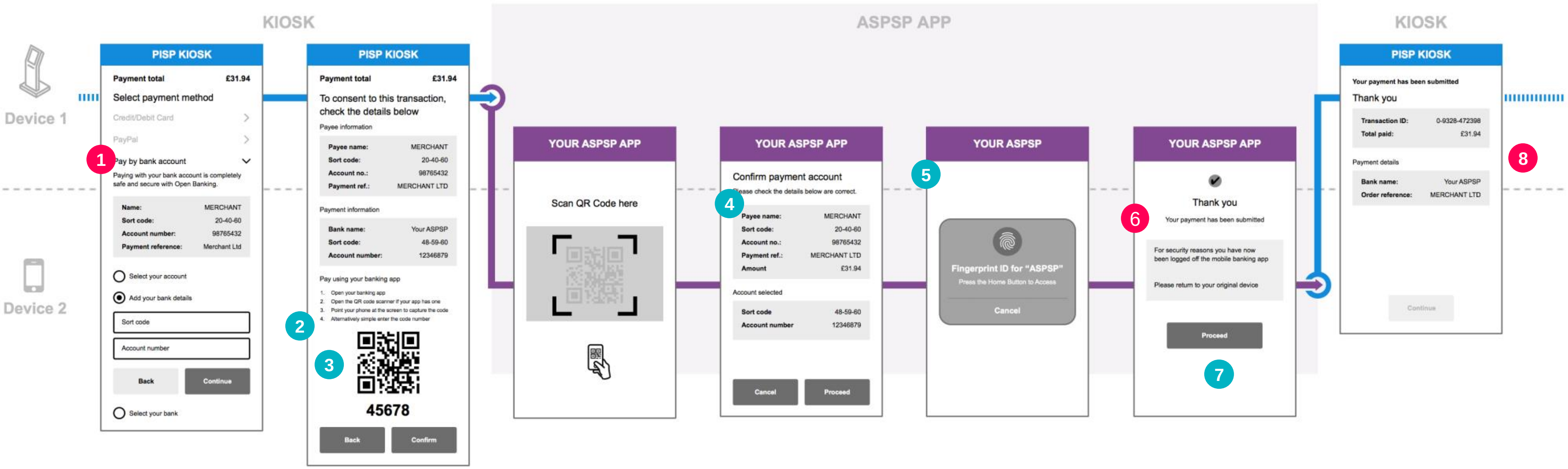
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

2.3.3 Model C: TPP generated identifier

PSU provides a TPP (AISP/PISP/CBPII) generated unique identifier to the ASPSP to identify the request from the TPP



PISP KIOSK

Payment total £31.94

Select payment method

Credit/Debit Card

PayPal

Pay by bank account

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your account

● Add your bank details

Sort code

Account number

Back | Continue

○ Select your bank

PISP KIOSK

Payment total £31.94

To consent to this transaction, check the details below

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879

Pay using your banking app

1. Open your banking app
2. Open the QR code scanner if your app has one
3. Point your phone at the screen to capture the code
4. Alternatively simple enter the code number

45678

Back | Confirm

YOUR ASPSP APP

Scan QR Code here

YOUR ASPSP APP

Confirm payment account

Please check the details below are correct.

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD
Amount	£31.94

Account selected

Sort code	48-59-60
Account number	12346879

Cancel | Proceed

YOUR ASPSP

Fingerprint ID for "ASPSP"

Press the Home Button to Access

Cancel

YOUR ASPSP APP

✔

Thank you

Your payment has been submitted

For security reasons you have now been logged off the mobile banking app

Please return to your original device

Proceed

PISP KIOSK

Your payment has been submitted

Thank you

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Order reference:	MERCHANT LTD

Continue

We have illustrated an example where the dynamic identifier is a QR code and scannable by the ASPSP app. The code generated is however not limited to QR code and the options supported are chosen by the ASPSP. The general guidance is that the use of the code within the ASPSP app should not introduce friction in the journey.

2.3.3 Model C: TPP generated identifier

PSU provides a TPP (AISP/PISP/CBPII) generated unique identifier to the ASPSP to identify the request from the TPP

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**For this step, please refer Section 4.1.1, step 1 & step 2.**				
6	The ASPSP performs a SCA. The ASPSP app based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app(biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
8	The PISP **must** confirm successful confirmation of payment initiation.	• PSR.Reg 44(1)	26	PISP	Required

	CX Considerations
2	The PISP **must** present the PSU the authentication options supported by the ASPSP which in turn can be supported by the PISP device/channel (e.g. A PISP kiosk that can only support authentication by ASPSP mobile app).
3	If the PISP and the ASPSP supports Model C then the PISP **must** display an identifier generated from the ASPSP to the PSU (e.g. QR code) and information on how the identifier should be used within the ASPSP app (e.g scan QR code with the ASPSP app).
4	The PSU **should** be able to easily use the identifier presented by the PISP application (e.g. scan the code from the Kiosk in this instance) without much friction (e.g of manually entering an alphanumeric code).
5	After the PSU scans the identifier from the PISP within the ASPSP app then the ASPSP **must** display the payment request and clearly mention the amount and the payee and payment account.
7	The ASPSP **must** make the PSU aware that they have been logged off from the ASPSP app and notify them to check back on the originating PISP app.

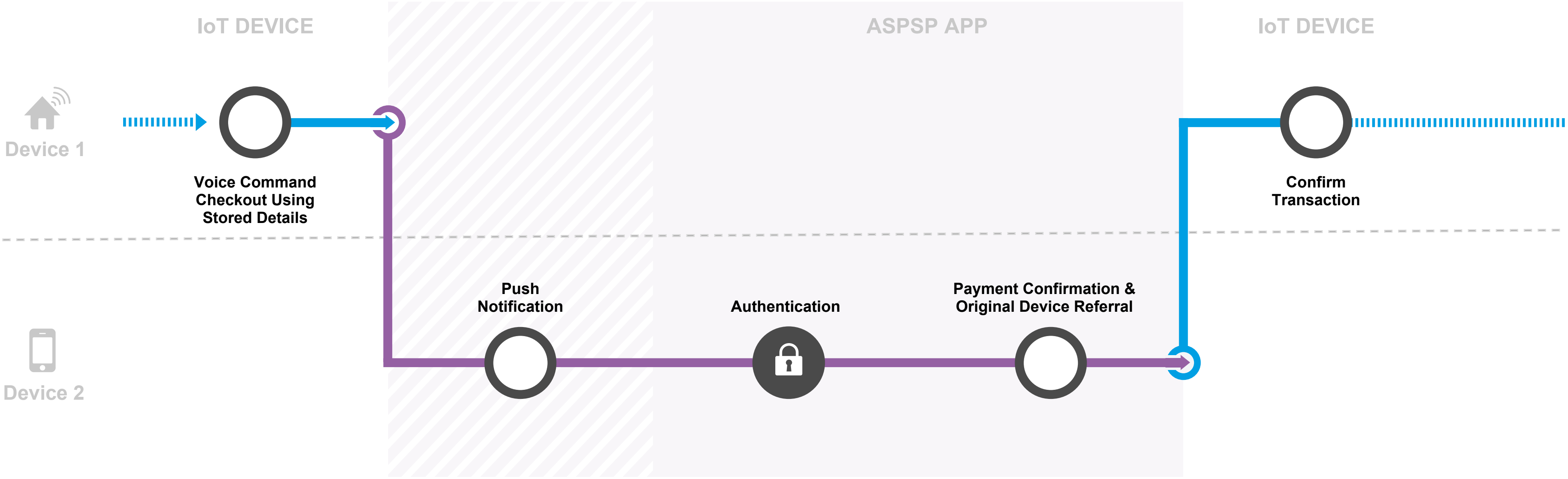
To demonstrate Model C based decoupled we have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order via the code generated by the PISP.

This flow applies to other variations of PIS journeys covered in detail under Section 4, AISP journeys covered under Section 3 and CBPII journeys covered under Section 5.

2.3.4 Model D: PSU with a TPP account

TPP (AISP/PISP/CBPII) passes the PSU's stored unique identifier to the ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations



A decoupled authentication flow where the TPP (AISP/PISP/CBPII) provides the ASPSP a stored PSU identifier, generated by the ASPSP from a previous PSU transaction. This is used by the ASPSP to notify the PSU such that the PSU can authenticate using the ASPSP app on a separate device**.**

This model is ideally suited where the services offered by the TPP involves POS, telephony, or where PSU interaction with the TPP is not possible through a graphical interface (IoT devices), or even when the PSU may not be present within the TPP channel.

Relevant Customer Insight and supporting regulation

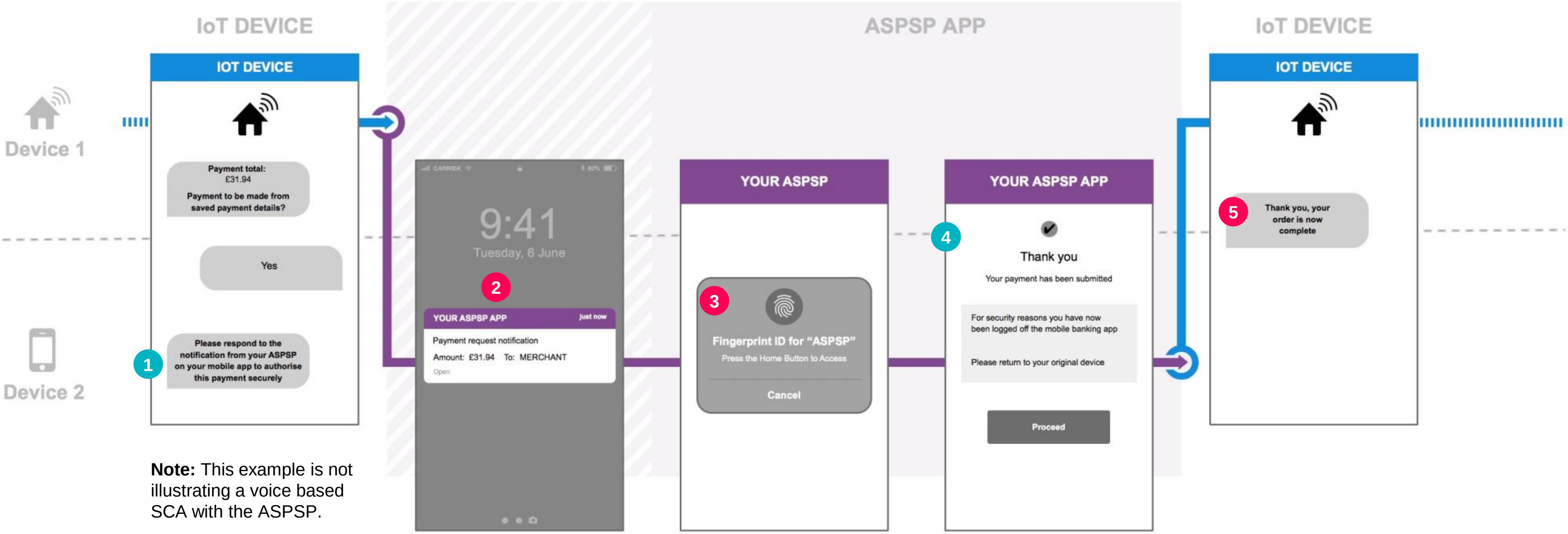
> View CX Customer Research

> View CEG Checklist

2.3.4 Model D: PSU with a TPP account

TPP (AISP/PISP/CBPII) passes the PSU's stored unique identifier to the ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations



1. Payment total: £31.94
Payment to be made from saved payment details?

Yes

Please respond to the notification from your ASPSP on your mobile app to authorise this payment securely

2. YOUR ASPSP APP — just now
Payment request notification
Amount: £31.94 To: MERCHANT
Open

3. Fingerprint ID for "ASPSP"
Press the Home Button to Access
Cancel

4. Thank you
Your payment has been submitted
For security reasons you have now been logged off the mobile banking app
Please return to your original device
Proceed

5. Thank you, your order is now complete

Note: This example is not illustrating a voice based SCA with the ASPSP.

2.3.4 Model D: PSU with a TPP account

TPP (AISP/PISP/CBPII) passes the PSU's stored unique identifier to the ASPSP to identify the PSU

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
2	The ASPSP **must** notify the PSU through the ASPSP app for authentication purposes only without introducing any additional screens. The notification **must** clearly mention the payment request with the amount and the payee.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
3	The ASPSP app based authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP mobile app (biometric, passcode, credentials).	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
5	The PISP **must** confirm successful confirmation of payment initiation	• PSR.Reg 44(1)	26	PISP	Required

	CX Considerations
1	PISP IoT device through voice enabled commands asks if they would like to checkout for the requested payment using their stored ASPSP account. After the PSU confirms, the PISP uses the stored PSU identity with the ASPSP to request for payment.
4	The ASPSP **must** make the PSU aware that they have been logged off from the ASPSP app and notify them to check back on the originating PISP app.

We have used one variation of PIS journey (Sec 4.1.1) as an example, where the ASPSP receives all the details of the payment order via the TPP device.

The voice commands are an example of how the PSU interacts with the TPP.

This flow applies to other variations of PIS journeys covered in detail under Section 4, AISP journeys covered under Section 3 and CBPII journeys covered under Section 5.

3.0 Account Information Services (AIS)

One of the primary ambitions of these guidelines is to provide simplification and consistency throughout each stage of the Open Banking implementation. As such, we have defined a core set of AIS journeys to illustrate the roles played by each of the Participants in the Open Banking ecosystem.

3.1. AIS Core Journeys

The Open Banking Read/Write API specifications support Account Information Services (AIS). They enable an Account Information Service Provider (AISP) to access account information from online payment accounts held at Account Service Payment Service Providers (ASPSPs), in order to provide account information services to a Payment Service User (PSU), provided they have obtained the PSU's explicit consent.

This section describes the core journeys that support the set-up and management of AIS. The key components are:

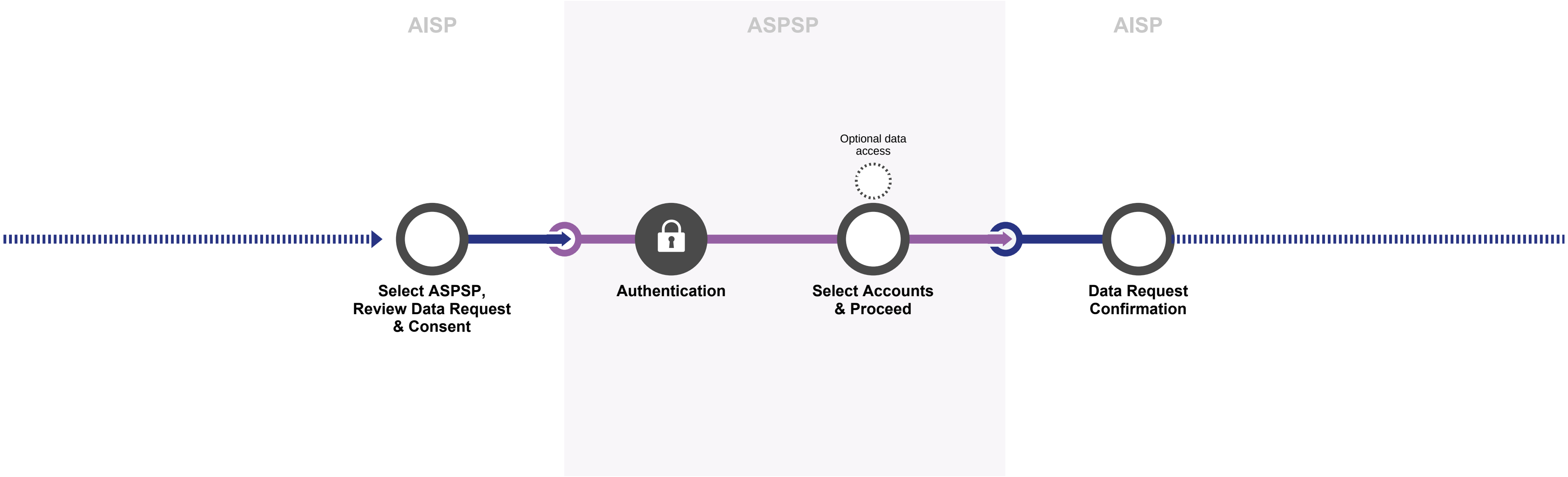
- Account Information Consent - PSU giving consent to an AISP to request account information from their ASPSP
- Refreshing AISP Access - PSU authenticating at their ASPSP to refresh on-going access they previously given consented to
- Consent Dashboard and Revocation - AISP facility to enable a PSU to view and revoke consents given to that AISP
- Access Dashboard and Revocation - ASPSP facility to enable a PSU to view all AISPs that have access to their account(s) and the ability to revoke that access
- Generic guidance around the effective use of re-direction screens (when the PSU is transferred to and from the ASPSP domain) is included in section 2.2.5

(Note: This section does not include guidance around scenarios when more than one TPP is involved in the delivery of a service - sometimes referred to as "Onward Provisioning". This subject will be addressed as part of the on-going OBIE evaluations of eIDAS and Consent/Access Dashboards.)

Featured journeys

3.1.1 Account Information Consent

User Journey | Wireframes | Requirements and Considerations


AISP
ASPSP
AISP
Optional data access
Select ASPSP, Review Data Request & Consent
Authentication
Select Accounts & Proceed
Data Request Confirmation

In this journey the AISP presents to the PSU a description of the data that it requires in order to support its service proposition. PSU selects the ASPSP(s) where their payment account(s) is held. The PSU is then directed to the domain of its ASPSP for authentication and to select the account(s) they want to give access to. Once the PSU has been authenticated, their ASPSP will able to respond to the AISP's request by providing the account information that has been requested.

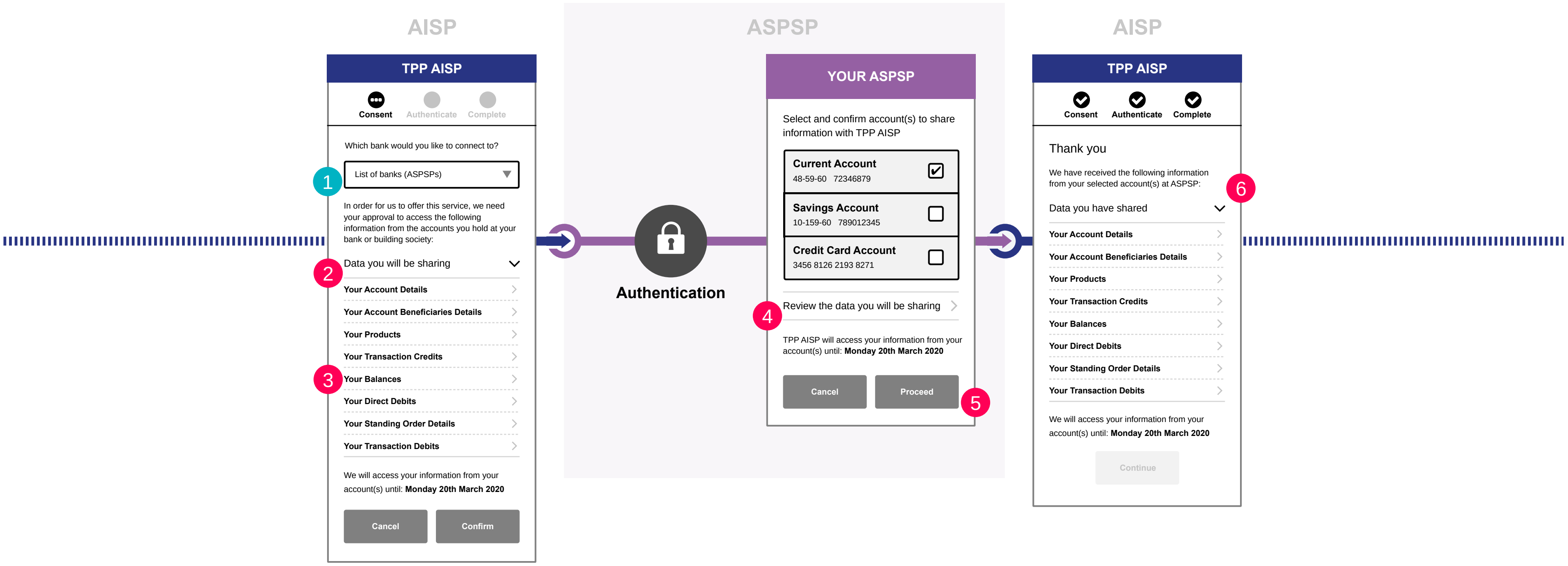
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

3.1.1 Account Information Consent

User Journey | Wireframes | Requirements and Considerations



AISP

TPP AISP

Consent · Authenticate · Complete

Which bank would you like to connect to?

1 List of banks (ASPSPs) ▼

In order for us to offer this service, we need your approval to access the following information from the accounts you hold at your bank or building society:

2 Data you will be sharing

- Your Account Details
- Your Account Beneficiaries Details
- Your Products
- Your Transaction Credits
- 3 Your Balances
- Your Direct Debits
- Your Standing Order Details
- Your Transaction Debits

We will access your information from your account(s) until: **Monday 20th March 2020**

Cancel | Confirm

Authentication

ASPSP

YOUR ASPSP

Select and confirm account(s) to share information with TPP AISP

Current Account 48-59-60 72346879	☑
Savings Account 10-159-60 789012345	□
Credit Card Account 3456 8126 2193 8271	□

4 Review the data you will be sharing

TPP AISP will access your information from your account(s) until: **Monday 20th March 2020**

Cancel | Proceed 5

AISP

TPP AISP

Consent · Authenticate · Complete

Thank you

We have received the following information from your selected account(s) at ASPSP:

6 Data you have shared

- Your Account Details
- Your Account Beneficiaries Details
- Your Products
- Your Transaction Credits
- Your Balances
- Your Direct Debits
- Your Standing Order Details
- Your Transaction Debits

We will access your information from your account(s) until: **Monday 20th March 2020**

Continue

3.1.1 Account Information Consent

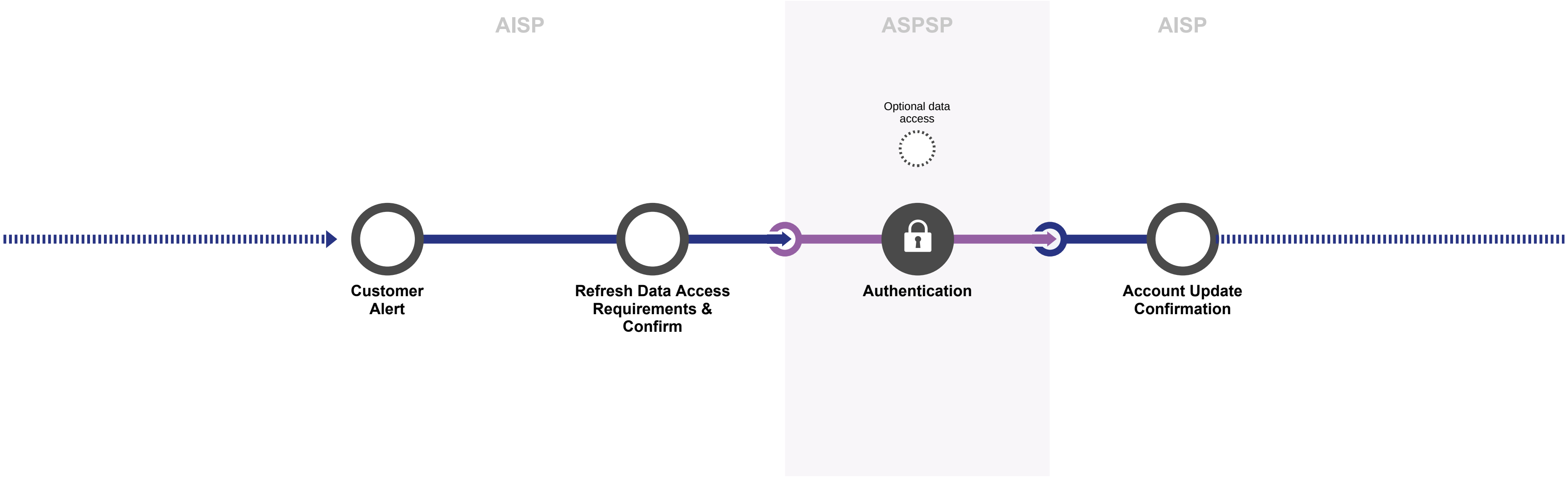
User Journey | Wireframes | **Requirements and Considerations**

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
2	The AISP **must** provide the PSU sufficient information to enable the PSU to make an informed decision, for example, detail the purpose for which the data will be used (including whether any other parties will have access to the information), the period over which it has been requested and when the consent for the account information will expire (consent could be on-going or one-off).	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8 12	TPP AISP	Required
3	The AISP **must** provide the PSU with a description of the data being requested using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below). The AISP **must** present the data at a Data Cluster level and allow the PSU to expand the level of detail to show each Data Permission. Once PSU has consented, the PSU will be directed to their ASPSP. Please refer section 2.2.5 for relevant messaging.	n/a	13b	AISP	Required
4	If the ASPSP provides an option for the PSU to view the data they have consented to share with the AISP as supplementary information, this **must** be done using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below) . Display of such information **must not** be provided to the PSU as a default.	CMA Order 10.2	13a	ASPSP	Required
5	The ASPSP **must** not seek confirmation of the consent that has already been provided by the PSU to the AISP. Once the PSU has selected the account(s), refer to section 2.1.5 for redirection messaging.	• EBA Opinion paragraph 13 • EBA Draft Guideline 5.2(c) • RTS Art. 32(3) • FCA Approach Document paragraph 17.48	2	ASPSP	Required
6	The AISP **should** confirm the successful completion of the account information request to the PSU.	n/a	18	AISP	Recommended

	CX Considerations
1	AISP **should** ask PSU to identify their ASPSP before requesting consent so that the consent request can be constructed in line with the ASPSP's data capabilities (which the ASPSP must make available to all TPPs). ASPSP Implementation guides, which are located on the Open Banking Developer Zone will have information about the ASPSP's data capabilities.

3.1.2. Refreshing AISP access

User Journey | Wireframes | Requirements and Considerations | Additional Information


AISP
ASPSP
AISP
Optional data access
Customer Alert
Refresh Data Access Requirements & Confirm
Authentication
Account Update Confirmation

The PSRs require strong customer authentication to be performed each time the PSU accesses its online payment account either directly or using the services of an AISP. The frequency of authentication can be reduced if an ASPSP applies the exemption relevant to account information access (RTS, Article 10), however this will still require the PSU to be authenticated at least every 90 days. This section describes the customer journey when a PSU needs to refresh AISP access, so the AISP can continue to provide the service previously consented to by authenticating again at their ASPSP. All other elements of the consent (data permissions required, purpose for which the data will be used, transaction history period and consent expiration date) remain unchanged.

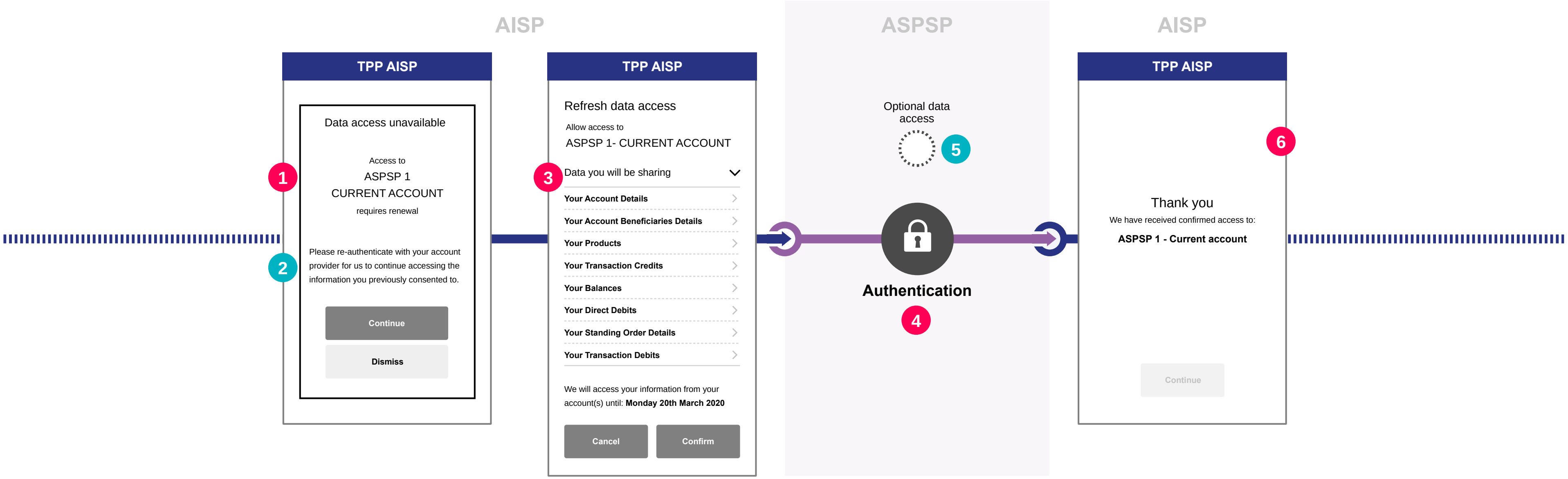
(It should be noted that the API specification allows the AISP to inform the ASPSP that the request is a refresh rather than a new request).

Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

3.1.2. Refreshing AISP access



TPP AISP

Data access unavailable

Access to
ASPSP 1
CURRENT ACCOUNT
requires renewal

Please re-authenticate with your account provider for us to continue accessing the information you previously consented to.

Continue

Dismiss

TPP AISP

Refresh data access

Allow access to
ASPSP 1- CURRENT ACCOUNT

Data you will be sharing

- **Your Account Details**
- **Your Account Beneficiaries Details**
- **Your Products**
- **Your Transaction Credits**
- **Your Balances**
- **Your Direct Debits**
- **Your Standing Order Details**
- **Your Transaction Debits**

We will access your information from your account(s) until: **Monday 20th March 2020**

Cancel | Confirm

Optional data access

Authentication

TPP AISP

Thank you

We have received confirmed access to:

ASPSP 1 - Current account

Continue

3.1.2. Refreshing AISP access

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	AISP **should** alert the PSU when authentication needs to be performed to refresh AISP access.	• P2 and P15 of Agreed Arrangements	16	AISP	Recommended
3	The AISP **must** present a high level summary of the data that is being requested and make it clear that this data and the purpose for which it will be used are the same as when originally requested. This should be done using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below).	n/a	13b	AISP	Required
4	The ASPSP **must not** replay the data requested (as a default) or seek re-confirmation of consent.	• EBA Opinion paragraph 13 • EBA Draft Guideline 5.2(c) and paragraph 34(c) • RTS Art. 32(3) • FCA Approach Document paragraph 17.48	2	ASPSP	Required
6	The AISP **should** confirm the successful completion of the account information request to the PSU.	n/a	18	AISP	Recommended

	CX Considerations
2	The AISP **should** make it clear that the PSU is being asked to authenticate to extend the AISP access to their account data and that no other element of the consent (e.g. the data permissions required, the purpose for which it will be used etc.) will change
5	As part of the authentication journey the ASPSP **could** have a call to action , for example, to an expandable section that the PSU can click on for information purposes only. If the ASPSP provides this option for the PSU as supplementary information, it will enable the PSU to view the data they have chosen to share with the AISP. This should be done using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below).

3.1.2. Refreshing AISP access

90 day access period

With the PSU's consent, the AISP can access account data covering any period of time going back, provided that the information is available to the PSU online and the AISP does not request more data then they need to support their service proposition. SCA must be performed prior to the AISP's first access, and subsequently re-performed at least every 90 days (where the ASPSP is applying the Art. 10 exemption), or otherwise where required by the ASPSP.

For example, let's say the PSU (on 14 January 2018) consents to AISP1 accessing the last three years' of account information (i.e. from 15 January 2015 -14 January 2019) from ASPSP2 with the consent validity lasting until 31 December 2018. ASPSP2 offers AISP1 three years of account information in the first access request after SCA has been performed. If ASPSP2 is applying the Art. 10 exemption, AISP1 can then continue to access either or both of the account balance and/or the last 90 days' payment transactions without SCA having to be performed again until 14 April 2018. However, SCA will have to be performed:

- At any time AISP1 requests more than either or both of the account balance and/or 90 days of payment transactions;
- AISP1 requests account information after 14 April 2018; or
- At any time the ASPSP requests the PSU to do so

In this example, the PSU will need to provide a new consent for the AISP to access the account information after 31 December 2018.

Amending Consent

In situations where a PSU wants to amend the access they have given to an AISP (e.g. they want to allow the AISP access to additional data elements), the AISP will have to take the PSU through a new consent process (as in section 3.1.1) as the API specifications do not support the ability to edit specific elements of a consent. It is in the domain of the AISP to clearly explain this process to the PSU and develop customer journeys for each scenario where this might apply.

Accounts associated with AISP long lived consent

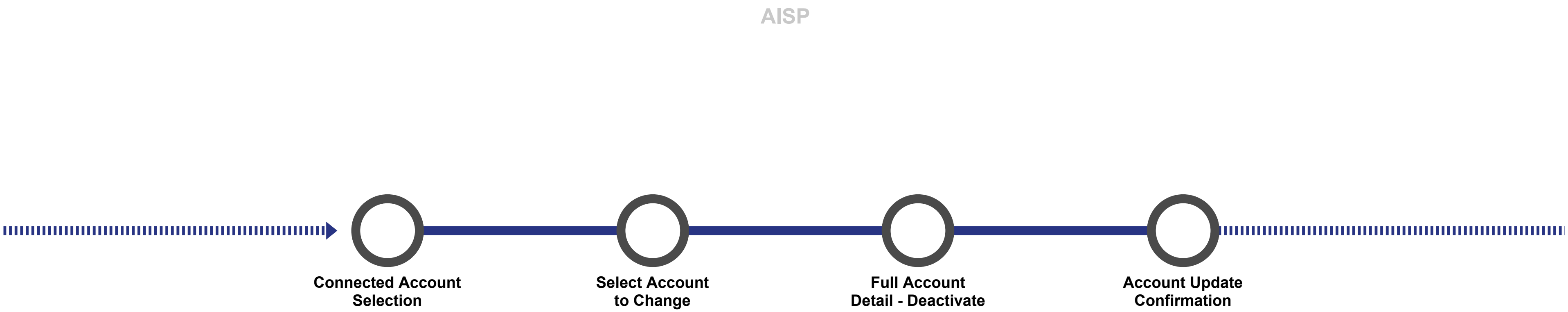
From a technical perspective, the consent given by the PSU with respect to account information is bound to the data clusters requested by the AISP and the period over which access has been requested (including any expiry date).
The actual selection of the designated payment account(s) then happens in the ASPSP space.
The designated payment account(s) could subsequently change for the following reasons:

- The ASPSP offers a dashboard functionality which allows a PSU to manage the designated payment accounts to which an AISP has access.
- A designated payment account is no longer available as it has been closed or temporarily suspended etc.

In these circumstances, the consent given to the AISP is still valid (provided it is "long-lived"), and the AISP should check the most updated list of designated payment accounts during subsequent requests for data access.

3.1.3. Consent Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations


AISP
Connected Account Selection
Select Account to Change
Full Account Detail - Deactivate
Account Update Confirmation

AISPs **must** provide PSUs with a facility to view and revoke on-going consents that they have given to that AISP. They may have consented to share data from several ASPSPs with a single AISP. This section describes how these consents should be displayed and how the customer journey to revoke them should be constructed.

Relevant Customer Insight and supporting regulation

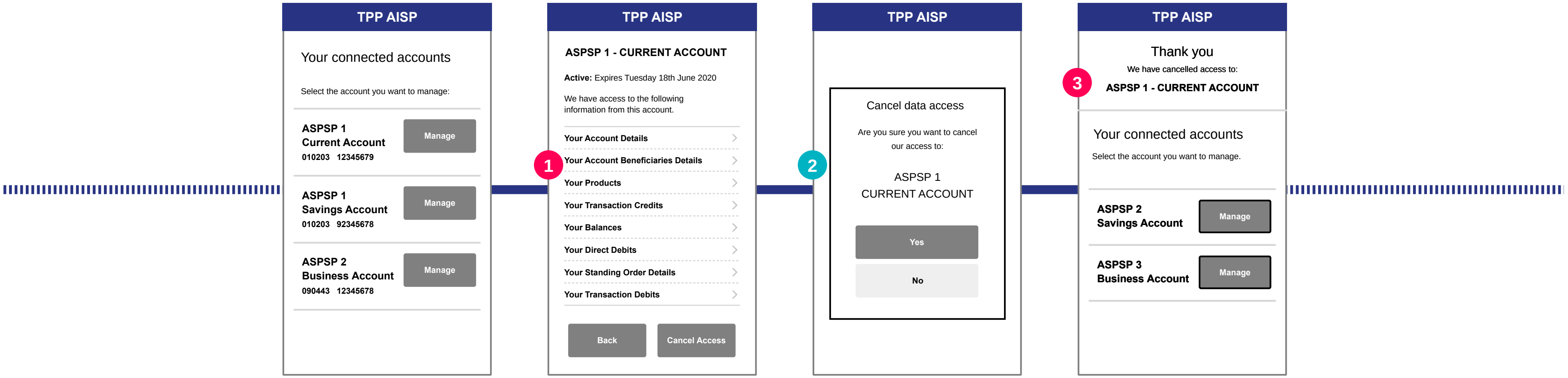
> View CX Customer Research

> View CEG Checklist

3.1.3. Consent Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations

AISP



TPP AISP

Your connected accounts

Select the account you want to manage:

ASPSP 1
Current Account
010203 12345679
Manage

ASPSP 1
Savings Account
010203 92345678
Manage

ASPSP 2
Business Account
090443 12345678
Manage

TPP AISP

ASPSP 1 - CURRENT ACCOUNT

Active: Expires Tuesday 18th June 2020

We have access to the following information from this account.

- **Your Account Details**
- **Your Account Beneficiaries Details**
- **Your Products**
- **Your Transaction Credits**
- **Your Balances**
- **Your Direct Debits**
- **Your Standing Order Details**
- **Your Transaction Debits**

Back | Cancel Access

TPP AISP

Cancel data access

Are you sure you want to cancel our access to:

ASPSP 1
CURRENT ACCOUNT

Yes

No

TPP AISP

Thank you

We have cancelled access to:

ASPSP 1 - CURRENT ACCOUNT

Your connected accounts

Select the account you want to manage.

ASPSP 2
Savings Account
Manage

ASPSP 3
Business Account
Manage

What the research says

In addition, consumer research has shown that respondents prefer confirmation of a revocation in writing via email in addition to text on the website.

> See more

3.1.3. Consent Dashboard & Revocation

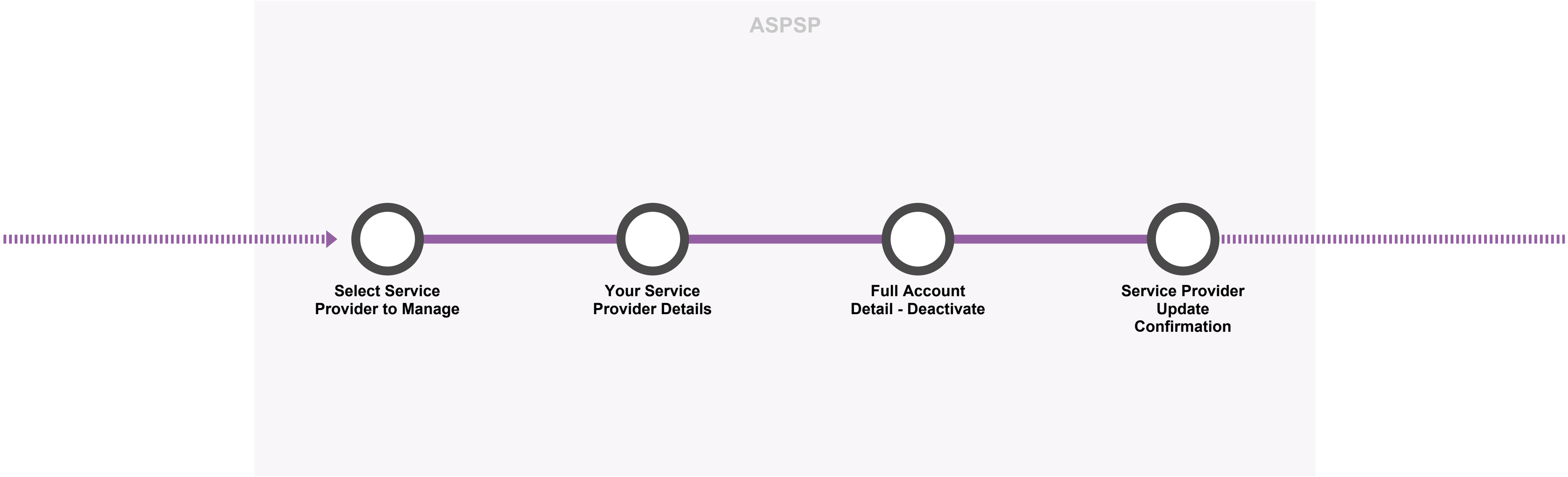
User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	The AISP **must** describe the data being shared through each consent using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below). The AISP should present the data at a Data Cluster level and allow the PSU to expand the level of detail to show each Data Permission The Consent Dashboard should also describe: • The purpose of the data request (including whether any other parties will have access to the information) • The period for which the transaction data has been requested • When the TPP's access to the data will expire • The date the consent was granted	n/a	13b	AISP	Required
3	The AISP **must** inform the ASPSP that the PSU has withdrawn consent by making a call to DELETE the account-access-consent resource (as described in Release 3 of the API specifications). This will ensure that no further account information is shared. The ASPSP must support the Delete process as described in the Release 3 API specifications. (This is not visible to the PSU but will ensure no further account information is provided by the ASPSP to the AISP).	P2 and P15 of Agreed Arrangements	9	TPP	Required

	CX Considerations
2	The AISP should make the exact consequences of cancelling the consent clear to the PSU - i.e. they will no longer be able to provide the specific service to the PSU

3.1.4 Access Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations


ASPSP
Select Service Provider to Manage
Your Service Provider Details
Full Account Detail - Deactivate
Service Provider Update Confirmation

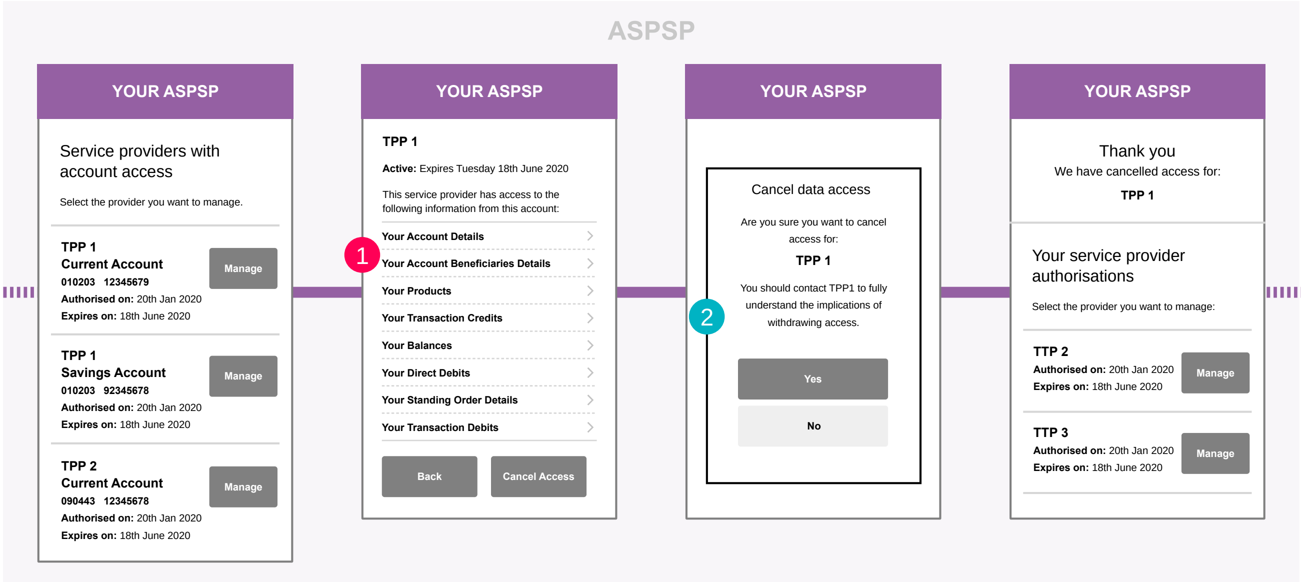
ASPSPs must provide PSUs with a facility to view and revoke on-going access that they have given to any AISP for each account held at that ASPSP. This section describes how AISP access should be displayed and how the customer journey to revoke them should be constructed.

Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

3.1.4 Access Dashboard & Revocation



ASPSP

YOUR ASPSP

Service providers with account access

Select the provider you want to manage.

TPP 1
Current Account
010203 12345679
Authorised on: 20th Jan 2020
Expires on: 18th June 2020
Manage

TPP 1
Savings Account
010203 92345678
Authorised on: 20th Jan 2020
Expires on: 18th June 2020
Manage

TPP 2
Current Account
090443 12345678
Authorised on: 20th Jan 2020
Expires on: 18th June 2020
Manage

YOUR ASPSP

TPP 1

Active: Expires Tuesday 18th June 2020

This service provider has access to the following information from this account:

- **Your Account Details**
- **Your Account Beneficiaries Details**
- **Your Products**
- **Your Transaction Credits**
- **Your Balances**
- **Your Direct Debits**
- **Your Standing Order Details**
- **Your Transaction Debits**

Back | Cancel Access

1

YOUR ASPSP

Cancel data access

Are you sure you want to cancel access for:

TPP 1

You should contact TPP1 to fully understand the implications of withdrawing access.

Yes

No

2

YOUR ASPSP

Thank you

We have cancelled access for:

TPP 1

Your service provider authorisations

Select the provider you want to manage:

TTP 2
Authorised on: 20th Jan 2020
Expires on: 18th June 2020
Manage

TTP 3
Authorised on: 20th Jan 2020
Expires on: 18th June 2020
Manage

What the research says

Consumer research has shown that people feel most confident that a revocation has been actioned, when it is has taken place with an ASPSP. Their perception is that they are 'stopping' the information at 'source' rather than instructing a TPP not to 'take' the information.

> See more

3.1.4 Access Dashboard & Revocation

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	The ASPSP **must** describe the data being accessed using the structure and language recommended by OBIE following customer research (see Data Cluster Structure & Language below). The ASPSP should present the data at a Data Cluster level and allow the PSU to expand the level of detail to show each Data Permission The Access Dashboard should also describe: • The status of the authorisation e.g. Active/Inactive • When the AISP's access to the account(s) will expire • The date the authorisation was granted The access dashboard **must** allow a PSU to view or cancel the access they have given consent to. These 2 functions should be given equal prominence when offered to the PSU.	CMA Order 10.2	13a 10	ASPSP	Required

	CX Considerations
2	The ASPSP **should** advise the PSU that they should contact the associated AISP to inform them of the cancellation of access and/or understand the consequences of doing so

3.2 Permissions and Data Clusters for AIS journeys

3.2.1 Permissions

In the Open Banking API design, data elements are logically grouped together into "permissions". It is at this level that AISPs request data access. If they request access to a specific permission they will have access to all the data elements in the permission. This provides a pragmatic approach, allowing AISPs to be selective but at the same time creating a consent process that is at an acceptable level of granularity for the PSU. Details of the data elements within each permission are included in the API technical specifications.

3.2.2 Data Clusters

OBIE customer research found that grouping permissions together and adding another layer of description aided the PSU's understanding of the data they were being asked to consent to share. This approach also allows a consistency of language across ASIPs and ASPSPs to provide additional comfort to the PSU that they are sharing the data they intended to. If consistent language is used across all Participants this will drive PSU familiarity and adoption. These groups of permissions are known as Data Clusters. Data Clusters are not reflected in the API specifications, they are purely a presentational layer on top of permissions to aid PSU understanding.

It should be noted that the P15 Evaluation (Efficacy of Consent Dashboards) currently underway will consider the structure of data clusters and the language used to support them. These guidelines will be amended in line with the output of that evaluation exercise.

3.2 Permissions and Data Clusters for AIS journeys

3.2.3 Data Cluster Structure & Language

The following table describes how permissions should be grouped into Data Clusters and the language that **must** be used to describe the data at each of these levels (Checklist item 13a and 13b). Both AISPs and ASPSPs **must** describe the data being shared at a Data Cluster level and allow the PSU to "drill-down" to see the detail at Permission level using the permission language set-out in the table below.

Where both Basic and Detail permissions are available from the same API end point, the Detail permission contains all data elements of the Basic permission plus the additional elements described in the table

Data Cluster Language	API End Points	Permissions	Permissions Language	Information available
Your Account Details	Accounts	Accounts Basic	*Any other name by which you refer to this account*	Currency of the account, Nickname of account (E.g. 'Jakes Household account')
		Accounts Detail	*Your account name, number and sort-code*	Account Name, Sort Code, Account Number, IBAN, Roll Number (used for Building Society) (plus all data provided in Accounts Basic)
	Balances	Balances	*Your account balance*	Amount, Currency, Credit/Debit, Type of Balance, Date/Time, Credit Line
	All where PAN is available	PAN	*Your card number*	PAN masked or unmasked depending on how ASPSP displays online currently
Your Regular Payments	Beneficiaries	Beneficiaries Basic	*Payee agreements you have set up*	List of Beneficiaries
		Beneficiaries Detail	*Details of Payee agreements you have set up*	Details of Beneficiaries account information (Name, Sort Code, Account) (plus all data provided in Beneficiaries Basic)
	Standing Orders	Standing Order Basic	*Your Standing Orders*	SO Info, Frequency, Creditor Reference Info, First/Next/Final Payment info
		Standing Order Detail	*Details of your Standing Orders*	Details of Creditor Account Information (Name, Sort Code, Account) (plus all data provided in Standing Order Basic)
	Direct Debits	Direct Debits	*Your Direct Debits*	Mandate info, Status, Name, Previous payment information
	Scheduled Payments	Scheduled Payments Basic	*Recurring and future dated payments*	Scheduled dates, amount, reference. Does not include information about the beneficiary
		Scheduled Payments Detail	*Details of recurring and future dated payments*	Scheduled dates, amount, reference. Includes information about the beneficiary
Your Account Transactions	Transactions	Transactions Basic Credits	*Your incoming transactions*	Transaction Information on payments made into the customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Does not include information about the entity that made the payment
		Transactions Basic Debits	*Your outgoing transactions*	Same as above, but for debits
		Transactions Detail Credits	*Details of your incoming transactions*	Transaction Information on payments made into the customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Includes information about the entity that made the payment
		Transactions Detailed Debits	*Details of your outgoing transactions*	Same as above but for debits

3.2 Permissions and Data Clusters for AIS journeys

Data Cluster Language	API End Points	Permissions	Permissions Language	Information available
Your Statements	Statements	Statements Basic	*Information contained in your statement*	All statement information excluding specific amounts related to various balance types, payments due etc.
		Statements Detail	*Details of information contained in your statement*	All statement information including specific amounts related to various balance types, payments due etc.
Your Account Features and Benefits	Products	Product	*Product details - fees, charges, interest, benefits/rewards*	Refers to customer account product details defined in the Open data API (the fees, charges, interest, benefits/rewards)
	Offers	Offers	*Offers available on your account*	Balance transfer, promotional rates, limit increases, start & end dates
Your contact details	Party	Party	*Your address, telephone numbers and email address as held by your bank/card issuer*	Address, telephone numbers and email address as held by your bank/card issuer, party type (sole/joint etc.)

3.2.4 Optional Data

If an AISP requests additional information (e.g. Party) and the ASPSP chooses to provide this information to the AISP, both parties must ensure that they consider GDPR in the processing of this request i.e. both parties must ensure that they have a legal basis for processing.

What the research says

If an AISP is asking for data access solely to a card account they should adjust the language they use to describe the ASPSP (e.g. “card provider” rather than “bank”) and use card specific data clusters and permissions

> See more

4.0 Payment Initiation Services (PIS)

One of the primary ambitions of the Customer Experience Guidelines is to provide simplification and consistency throughout each stage of the Open Banking implementation. As such, we have defined and illustrated a core set of payment initiation journeys.

4.1 PIS Core Journeys

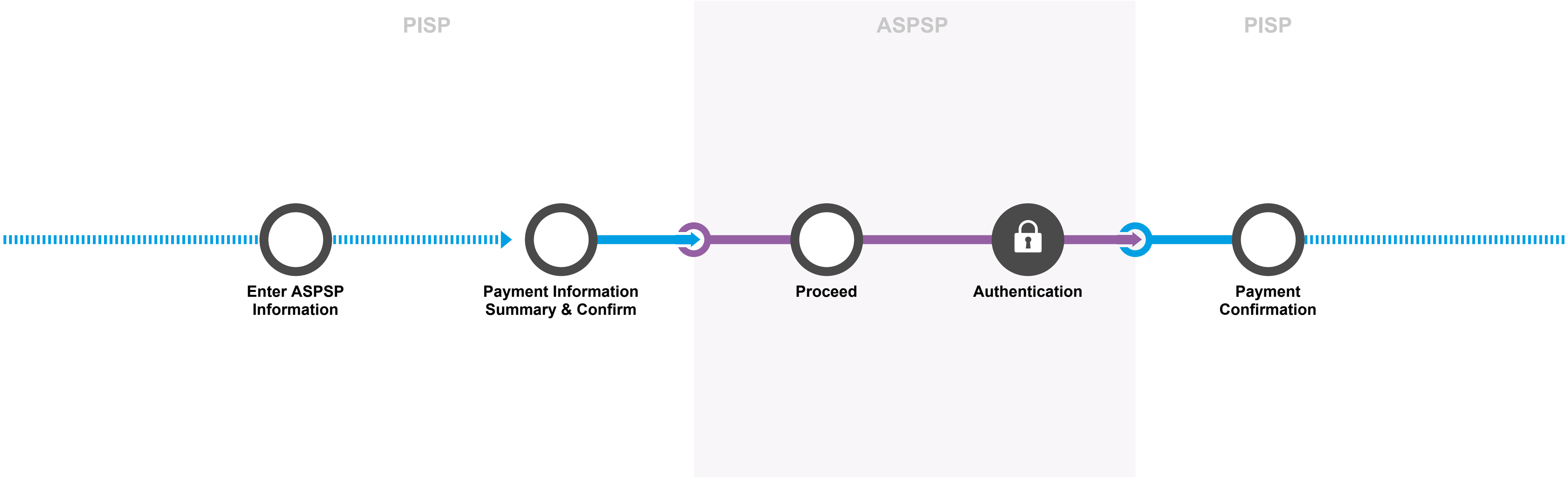
Open Banking API specifications support Payment Initiation Services (PIS) that enable a PISP to initiate a payment order, with the PSU's explicit consent, from their online payment account held at their ASPSP. The PISP is then further able to retrieve the status of a payment order. This section describes how each of the Participants (PISPs and ASPSPs) in the delivery of these services can optimise the customer experience for these services. Furthermore, it provides some clarifications to these Participants on the usage of the APIs which are not covered by the technical specifications, and some best practice guidelines for implementation of the customer journeys.

Please note that ASPSPs do not need to support the initiation of certain payment methods described in this section by a PISP, where the ASPSP does not support such transactions through their own channels (such as future dated foreign transactions and bulk payment files).

Featured journeys

4.1.1 Single Domestic Payments - a/c selection @ PISP

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations



PSUs can initiate, by providing their consent to PISPs, an instruction to their ASPSPs to make a one-off payment for a specific amount to a specific payee.

Where all information for a complete payment order (including the PSUs' account details) is passed from PISPs to ASPSPs, once PSUs have been authenticated, PSUs must be directed back to the PISP domain without any further steps taking place in the ASPSP domain.

This excludes the cases where supplementary information is required to be provided to PSUs as described in Section 4.1.2).

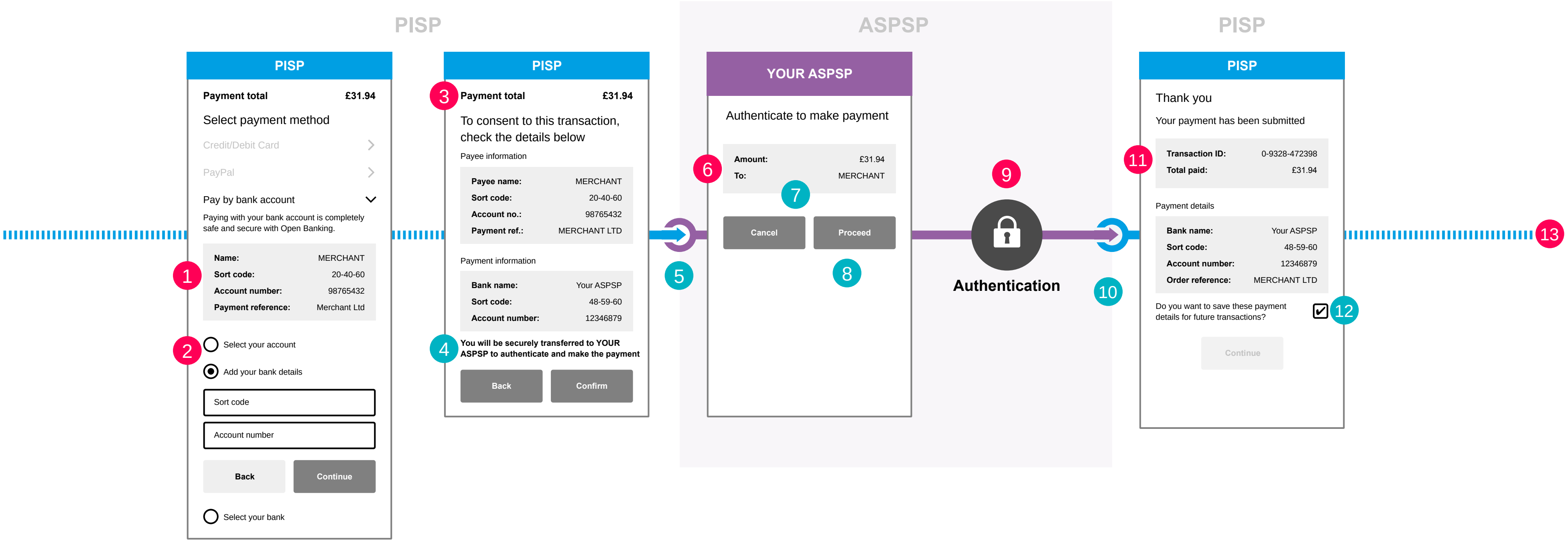
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.1 Single Domestic Payments - a/c selection @ PISP

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations



PISP

PISP

Payment total **£31.94**

Select payment method

Credit/Debit Card ›

PayPal ›

Pay by bank account ⌄

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your account

● Add your bank details

Sort code

Account number

Back | Continue

○ Select your bank

PISP

Payment total **£31.94**

To consent to this transaction, check the details below

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

ASPSP

YOUR ASPSP

Authenticate to make payment

Amount:	£31.94
To:	MERCHANT

Cancel | Proceed

Authentication

PISP

PISP

Thank you

Your payment has been submitted

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879
Order reference:	MERCHANT LTD

Do you want to save these payment details for future transactions? ☑

Continue

What the research says

Research amongst consumers has shown that 64% of participants prefer to be shown confirmation that the payment has been received at the TPP. This would provide reassurance that the process has worked.

> See more

4.1.1 Single Domestic Payments - a/c selection @ PISP

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

CEG Checklist Requirements		Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters** PISPs **must** either allow PSUs to specify the below minimum set of parameters or pre-populate them for the PSUs: • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN) • Payment Reference - This is optional but it is good practice to be populated for a payment	• RTS Art. 36(4)	22	PISP	Required
2	**PSU payment Account Selection** PISPs **must** provide PSUs at least one of the following options: • enter their Payer's payment Account Identification details • select their Account Identification details (this assumes they have been saved previously) • select their ASPSP in order to select their PSU payment Account from there later on in the journey	• n/a	24	PISP	Required
3	**PSU Consent to PISP** PISPs **must** request for the PSUs' consent to the payment in a clear and specific manner. PISPs **must** display the following information in the consent screen: • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payment Reference, **if** it has been entered by PSUs or prepopulated by PISPs in item #1 • PSU payment Account Identification **and/or** the selected ASPSP (based on item #2 options) • *Note 1: if PSU payment Account identification is selected in item #2, PISPs **should** mask the PSU payment Account details on the consent screen. Otherwise, if the PSU payment Account identification has been input by PSUs in item #2, PISPs **should not** mask these details to allow PSUs to check and verify correctness* • *Note 2: if PSU payment Account identification is provided by PSUs in item #2, PISPs **could** use this to identify and display the ASPSP without having to ask PSUs.* For Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN): • if this has been provided by PSUs in item #1, then PISPs **must** also display this in the consent screen to allow PSUs to check and verify correctness • if this has been pre-populated by PISPs (e.g. in a eCommerce payment scenario) PISPs **could** choose whether to display this information or not	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	TPP	Required
6	ASPSPs **must** display as minimum the Payment Amount and Currency and the Payee Account Name to comply with dynamic linking obligations.	• RTS Art. 5(1)(a)	28	ASPSP	Required
9	SCA Authentication (including dynamic linking) **must** be the only action required at the ASPSPs (unless supplementary information required, refer to section 4.1.2). ASPSPs **must** inform PSUs about their "point of no return" for making the payment and that their payment will be made after authentication occurs. Example wording: "Authenticate to make payment" The ASPSP authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP channel.	• Trustee P3/P4 letter Action P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
11	**PISP Confirmation** PISPs **must** display the information received from the ASPSP. This information may include: • The unique identifier assigned to the payment instruction by ASPSPs • The payment status (and status update date & time) - Confirmation of successful payment initiation If received by ASPSPs, PISPs must display any of the following information regarding initiation and execution of the payment: • The expected payment execution date & time • The expected settlement date & time (i.e. the value date of the payment) • The ASPSP charges (where applicable)	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.26 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
13	**Further Payment Status Update** PISPs **should** follow up with ASPSPs in order to check and update the PSUs with the most updated information that can be received by ASPSPs in relation to the execution of the payment.	• n/a	27	PISP	Recommended

4.1.1 Single Domestic Payments - a/c selection @ PISP

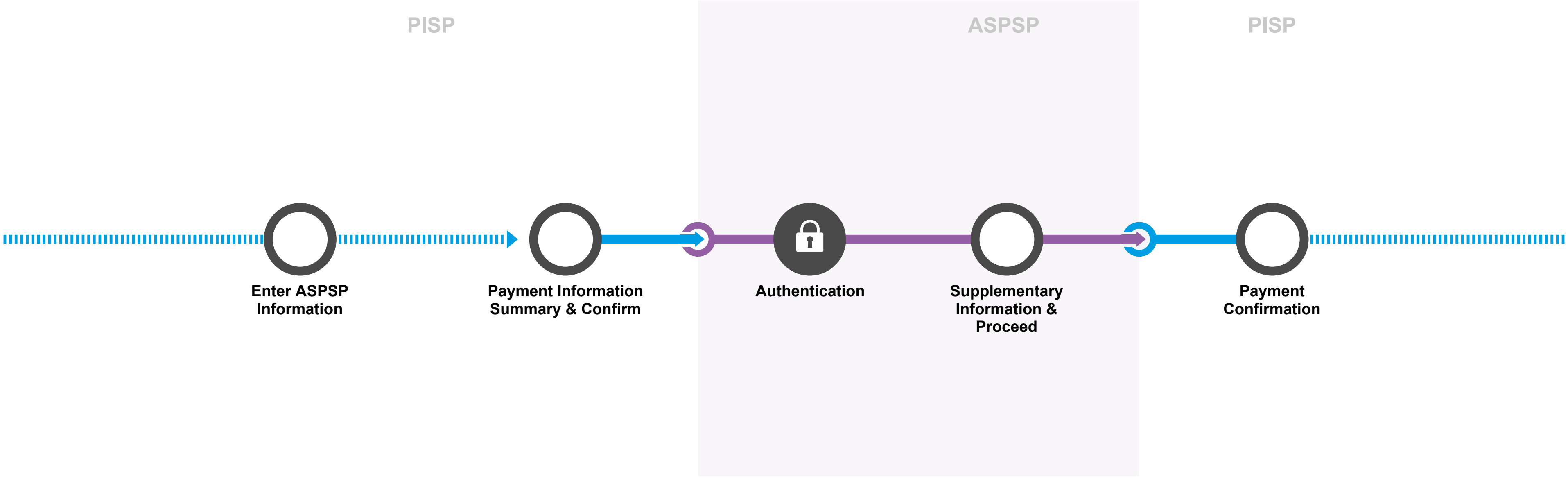
User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

CX Considerations	
4	PISPs **should** provide messaging to inform PSUs that they will be taken to their ASPSPs to complete the payment. Example wording: *"You will be securely transferred to YOUR ASPSP to authenticate and make the payment"*
5	Generic PISP to ASPSP redirection screen and message. Please refer to Section 2.2.5
7	ASPSPs **could** display the balance of PSUs payment account (not shown on user journey) (an ASPSP for instance **could** use device identification to identify the PSU and display the balance)
8	If SCA as described in item #9 cannot occur on the same screen as #6 and #7 of displaying the amount and the payee (e.g. for some biometric authentications methods), then ASPSPs **should** offer PSUs options to proceed or cancel the payment with "equal prominence"
10	Generic ASPSP to PISP redirection Screen and message. Please refer to Section 2.2.5
12	**If** PSUs provide their payment account identification details (as per item #2 options), PISPs **could** save the account details for future transactions, where this is part of the payment initiation service explicitly requested by the PSU.

Note: This core journey will result in a single domestic payment which will be processed by the ASPSPs as a Single Immediate Payment (SIP) via Faster Payments. Single domestic payments through other payment schemes can be initiated as described in section 4.1.2.1.

4.1.2 Single Domestic Payments - a/c selection @ PISP (Supplementary info)

User Journey | Wireframes | Requirements and Considerations | Additional Information


PISP
ASPSP
PISP
Enter ASPSP Information
Payment Information Summary & Confirm
Authentication
Supplementary Information & Proceed
Payment Confirmation

In some scenarios, an additional step in ASPSPs' journeys may be required to display supplementary information to PSUs. ASPSPs should determine the situations where this supplementary information is required, having regard to the principle that parity should be maintained between Open Banking journeys and ASPSPs' online channel journeys, such that if supplementary information is not provided within the ASPSPs' online channels directly to PSUs, then it must not be provided during an Open Banking PIS journey. ASPSPs should also ensure that this information does not constitute an obstacle or additional check on the consent provided by the PSU to the TPP.

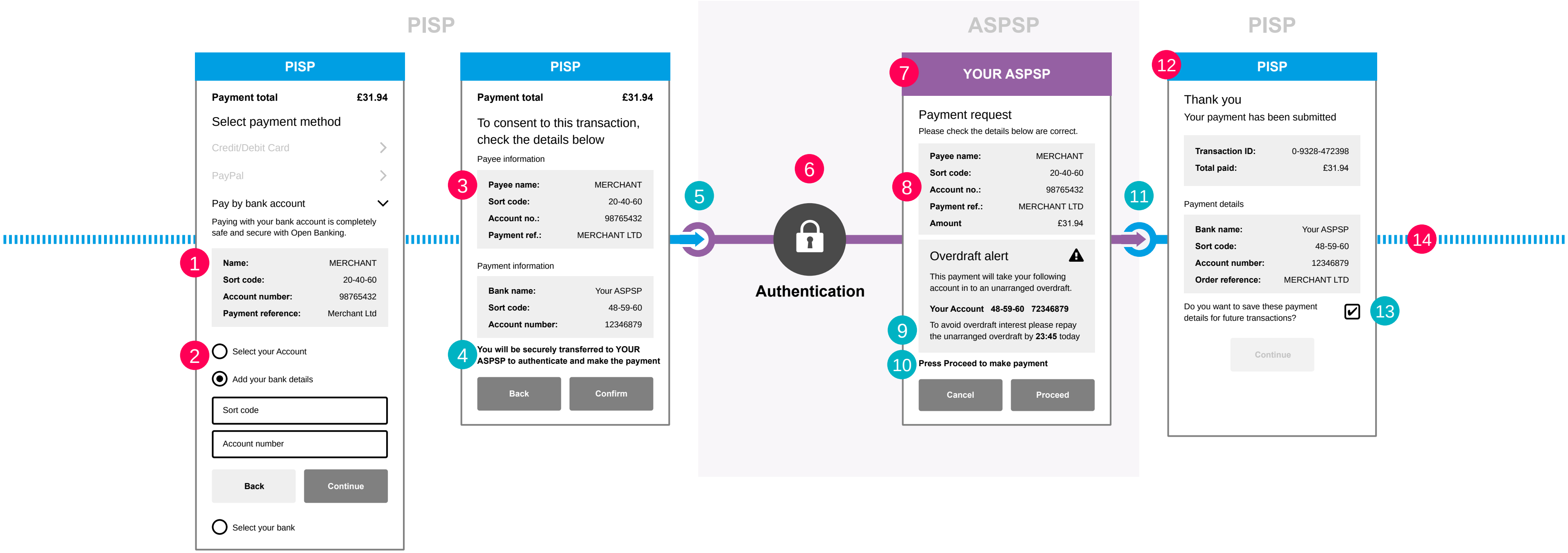
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.2 Single Domestic Payments - a/c selection @ PISP (Supplementary info)

User Journey | Wireframes | Requirements and Considerations | Additional Information



PISP

Payment total	**£31.94**

Select payment method

Credit/Debit Card >

PayPal >

Pay by bank account ⌄

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your Account

● Add your bank details

Sort code

Account number

Back | Continue

○ Select your bank

PISP

Payment total	**£31.94**

To consent to this transaction, check the details below

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Payment request

Please check the details below are correct.

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD
Amount	£31.94

Overdraft alert ⚠

This payment will take your following account in to an unarranged overdraft.

Your Account 48-59-60 72346879

To avoid overdraft interest please repay the unarranged overdraft by **23:45** today

Press Proceed to make payment

Cancel | Proceed

PISP

Thank you

Your payment has been submitted

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879
Order reference:	MERCHANT LTD

Do you want to save these payment details for future transactions? ☑

Continue

4.1.2 Single Domestic Payments - a/c selection @ PISP (Supplementary info)

User Journey | Wireframes | Requirements and Considerations | Additional Information

CEG Checklist Requirements		Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters:** As per 4.1.1, item #1	• RTS Art. 36(4)	22	PISP	Required
2	**PSU payment Account Selection:** As per 4.1.1, item #2	• n/a	24	PISP	Required
3	**PSU Consent to PISP** : As per 4.1.1, item #3	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	TPP	Required
6	ASPSPs **must** apply SCA including dynamic linking, unless an exemption applies. The ASPSP authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP channel.	• RTS Art. 33(2) • Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
7	**Supplementary Information** ASPSPs **must** be able to introduce a step as part of the authentication journey to display supplementary information associated with that payment if required.	• EBA Draft Guideline 5.2(d)	20	ASPSP	Required
10	ASPSPs **must** allow PSUs to review as a part of the authentication process any supplementary Information. The PSU can either proceed with the payment or cancel it on the same screen with items #7 & #8,using options with "equal prominence".	• EBA Draft Guideline 5.2(d)	20	ASPSP	Required
12	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.23-17.24 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
14	**Further Payment Status Update:** As per 4.1.1, item #13	• n/a	27	PISP	Recommended

CX Considerations	
4	As per 4.1.1, item #4
5	As per 4.1.1, item #5
8	ASPSPs **should** display to PSUs all the payment instruction information received from PISPs together with the supplementary information. This information may include the following: • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payment Reference, if it has been entered by PSUs or prepopulated by PISPs in item #1 • PSU payment Account Identification and/or the selected ASPSP (based on item #2 options). • Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN) ASPSPs could display the balance of PSUs payment account (see Section 4.1.3 for clarification on SCA requirements)
9	ASPSPs **should** inform PSUs about their "point of no return" for making the payment and that their payment will be made after pressing the Proceed button. Example wording: "Press Proceed to make payment"
11	As per 4.1.1, item #10
13	As per 4.1.1, item #12

4.1.2 Single Domestic Payments - a/c selection @ PISP (Supplementary info)

User Journey | Wireframes | Requirements and Considerations | Additional Information

List of Supplementary Information:

ASPSPs **must** determine the situations where Supplementary Information is required to be shown to the PSU, having regard to the principle that parity should be maintained between Open Banking journeys and ASPSP direct online channel journeys. Supplementary Information may be required:

- Where fees, charges or Forex apply(e.g single CHAPS international payments)
- Where interest rates apply
- To facilitate confirmation of payee (for UK implementations, where ASPSPs applied COP validation and found inconsistency between payee account name and payee account details)
- To display a PSU warning that the relevant payment account will become overdrawn / exceed an overdraft limit as a result of the intended payment
- If the relevant payment submission cut-off time has elapsed and the ASPSP wishes to offer an execution date/time
- Where the PSU has been identified by the ASPSPs as a vulnerable customer (who therefore receives tailored journeys and messages in ASPSP's own online platforms)
- To show value-add information based on functionality implemented by ASPSPs in competitive space which provides positive customer outcome (e.g. cashflow prediction engine)
- For high value transactions using a different payment scheme
- Where the payments may be duplicated by the customer in a short period (e.g. ASPSP may display a warning that payment appears to be duplicated).

4.1.2.1 Single Domestic Payments - BACS and CHAPS

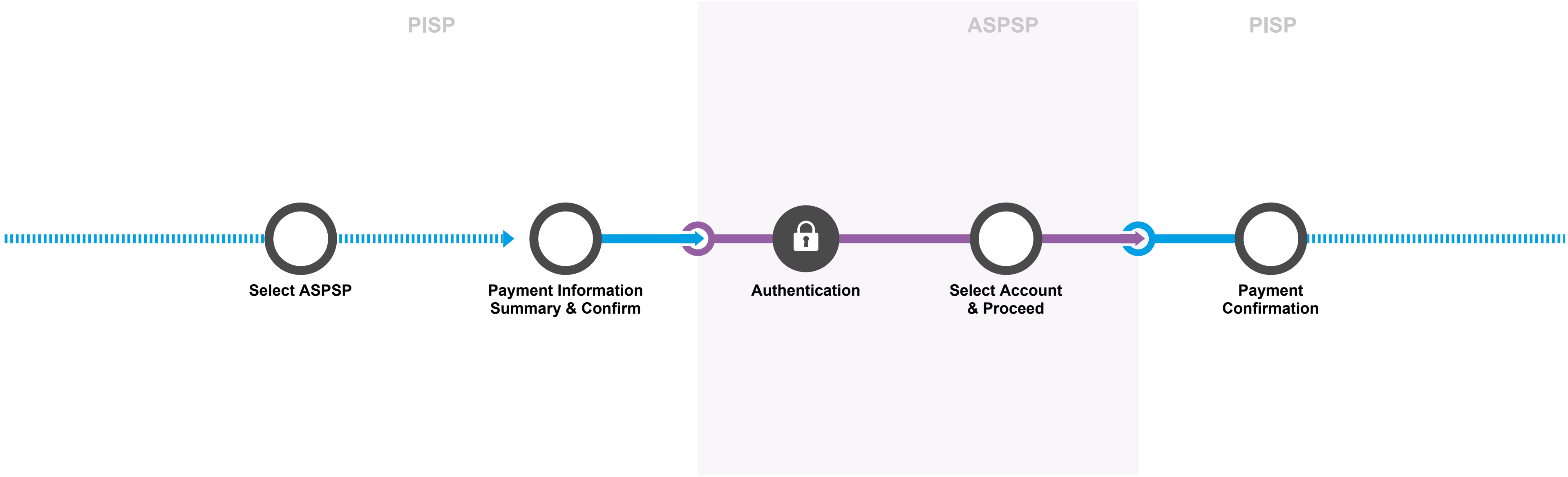
Journey 4.1.2 can be used to initiate single domestic payment through Bacs or CHAPS, with the chosen payment scheme to be captured and included in the payment order. Thus:

- **Minimum Set of Parameters:** PISPs **must** either allow PSUs to specify the Payment Scheme as part of the information they provide to the PISP or pre-populate this information for the PSUs (in use cases where applicable).
- The payment scheme (Bacs, CHAPS, or Faster Payments) will then be included in the PSUs' consent screen and will be forwarded to the ASPSP as part of the payment order.
  - Please note that Faster Payments does not need to be explicitly defined, as it is considered to be the default payment scheme to use when the optional parameter is not defined.

Note: Single Bacs or CHAPS payments may require the display of supplementary information due to cut-off times and potential additional charges.

4.1.3 Single Domestic Payments - a/c selection @ ASPSP

User Journey | Wireframes | Requirements and Considerations



There are cases where the payment order submitted by PISPs to ASPSPs is incomplete, such as where PSU account selection has not yet occurred.

In these scenarios, OBIE considers that SCA only needs to be obtained once, as part of the initial interaction between the ASPSP and PSU. The fact that the PSU has to then carry out account selection or provide other information does not invalidate the SCA just performed by the ASPSP.

Equally, the display of the account balance by the ASPSP as part of the account selection process in the payment initiation journey should not require an additional application of SCA. We understand the FCA is comfortable with this approach, however we note that the application of SCA (and interpretation of relevant requirements) is a matter for individual ASPSPs.

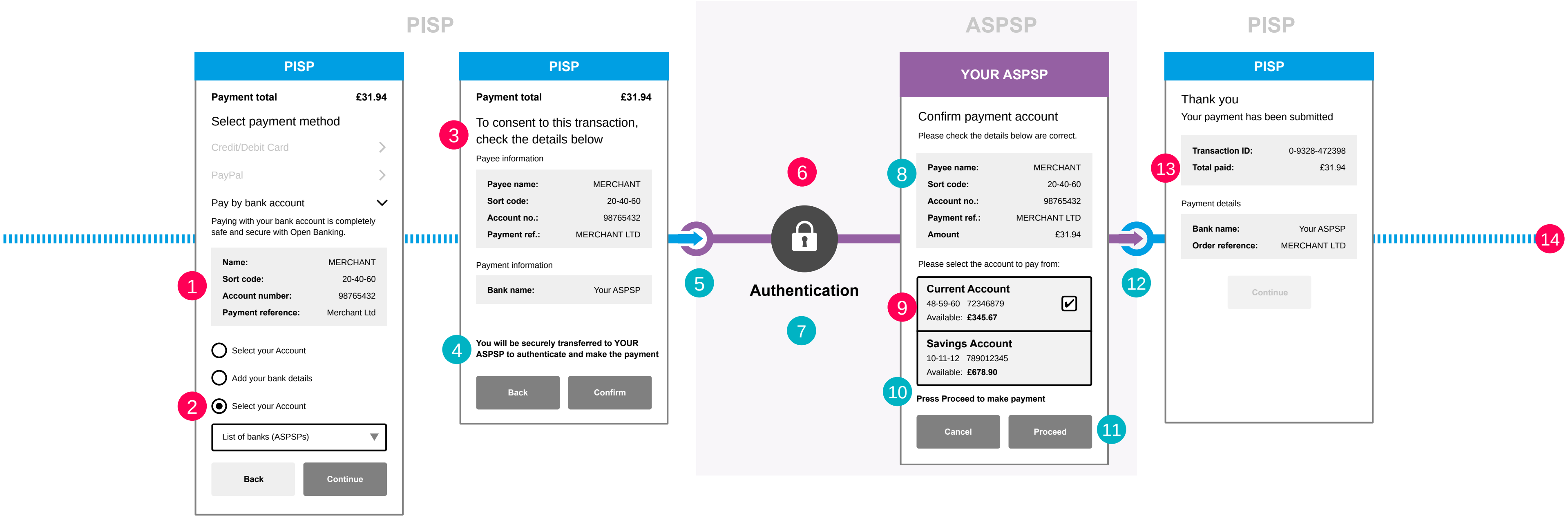
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.3 Single Domestic Payments - a/c selection @ ASPSP

User Journey | Wireframes | Requirements and Considerations



PISP

Payment total £31.94

Select payment method

Credit/Debit Card

PayPal

Pay by bank account

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your Account

○ Add your bank details

● Select your Account

List of banks (ASPSPs) ▼

Back | Continue

PISP

Payment total £31.94

To consent to this transaction, check the details below

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Confirm payment account

Please check the details below are correct.

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD
Amount	£31.94

Please select the account to pay from:

Current Account ☑
48-59-60 72346879
Available: £345.67

Savings Account
10-11-12 789012345
Available: £678.90

Press Proceed to make payment

Cancel | Proceed

PISP

Thank you

Your payment has been submitted

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment details

Bank name:	Your ASPSP
Order reference:	MERCHANT LTD

Continue

Example cases where the payment order submitted by PISP is incomplete include:

- PSU payment account has not been selected.
- Any other optional parameters of the OBIE standard required by the ASPSP to make the payment have not been selected/defined at PISP (e.g. payment scheme for bulk/batch, payment priority, charges model for international payments etc.).

What the research says

When account selection is done at the ASPSP, research amongst consumers has shown that 58% of participants prefer to be shown the balance for their selected payment account, before reviewing a payment. This was felt to assist in good personal financial management.

> See more

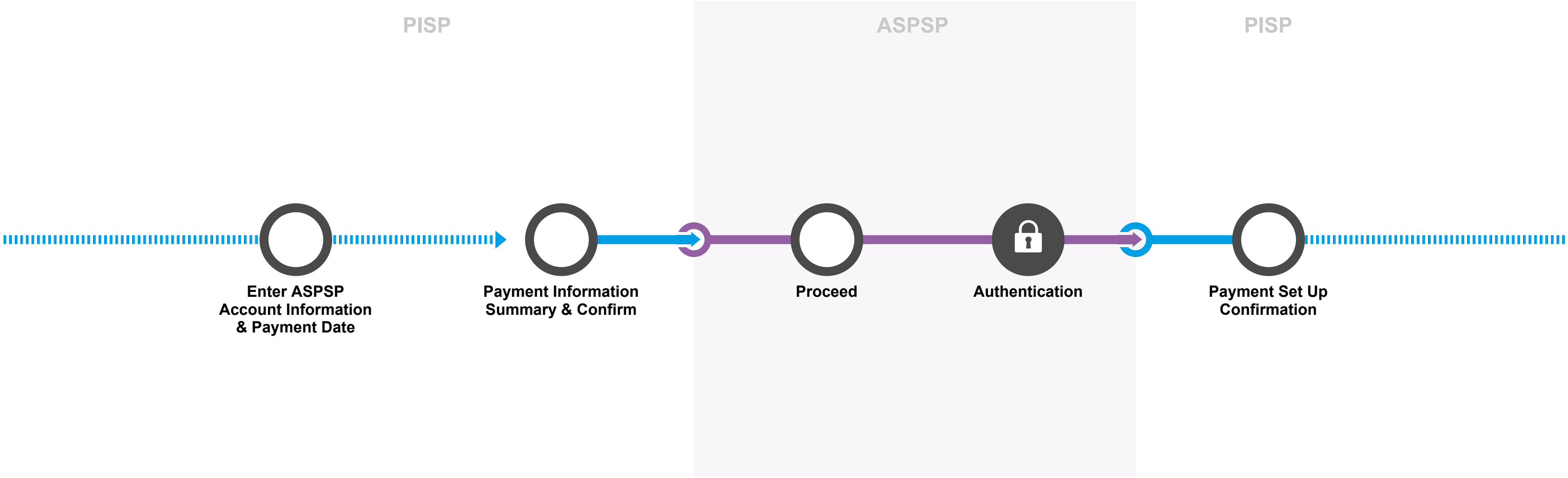
4.1.3 Single Domestic Payments - a/c selection @ ASPSP

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters:** As per 4.1.1, item #1	• RTS Art. 36(4)	22	PISP	Required
2	**PSU payment Account Selection:** As per 4.1.1, item #2	• n/a	24	PISP	Required
3	**PSU Consent to PISP** PISPs **must** request for the PSUs' consent to the payment initiation in a clear and specific manner. PISPs **must** display the following information in the consent screen: • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payment Reference, **if** it has been entered by PSUs or prepopulated by PISPs in item #1 • Selected ASPSP (based on item #2 options) For Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN): • if this has been provided by PSUs in item #1, then PISPs **must** also display this in the consent screen to allow PSUs to check and verify correctness • if this has been pre-populated by PISPs (e.g. in a eCommerce payment scenario) PISPs **could** choose whether to display this information or not	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
6	ASPSPs **must** apply SCA including dynamic linking, unless an exemption applies. The ASPSP authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP channel.	• RTS Art. 33(2) • Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
9	**Additional Parameters** ASPSPs **must** allow PSUs to select the payment account to complete the payment order for execution.	• CMA Order 10.2	23	ASPSP	Required
13	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.23-17.24 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
14	**Further Payment Status Update:** As per 4.1.1, item #13	• n/a	27	PISP	Recommended

	CX Considerations
4	As per 4.1.1, item #4
5	As per 4.1.1, item #5
7	ASPSPs **could** also display a message to prompt PSUs to authenticate to continue with their payment instruction.
8	Once the PSU has selected their account, the ASPSPs **should** display the following information to the PSU: • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payment Reference, **if** it has been entered by PSUs or prepopulated by PISPs in item #1 • The account selected by the PSU for payment • Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN)
10	ASPSPs **should** inform PSUs about their "point of no return" for making the payment and that their payment will be made after pressing the Proceed button. Example wording: "Press Proceed to make payment"
11	ASPSPs **must** allow PSUs to review as a part of the authentication process the information described in items #7 & #8. The PSU can either proceed with the payment or cancel it, on the same screen with items #7 & #8, using options. with "equal prominence".
12	As per 4.1.1, item #10

4.1.4 Single Domestic Scheduled Payments (Future Dated)


PISP
ASPSP
PISP
Enter ASPSP Account Information & Payment Date
Payment Information Summary & Confirm
Proceed
Authentication
Payment Set Up Confirmation

PSUs can setup, through PISPs, an instruction to their ASPSPs to make a one-off payment for a specific amount to a specific payee on a specific future date.

The example reference journey illustrates account selection occurring in the PISP domain. However, please note that account selection can take place at the ASPSP domain. In this scenario, please follow the approach of reference journey 4.1.3.

Note: OBIE Standards do not currently support the amendment or cancellation of Future Dated Payments via PISPs. These payments may be amended or cancelled via the ASPSP’s direct online channel (where supported). Cancellation of these payments must be consistent with available capabilities on ASPSP's existing online platform, as well as, in accordance with the provisions of the PSRs relating to revocation of payment orders.

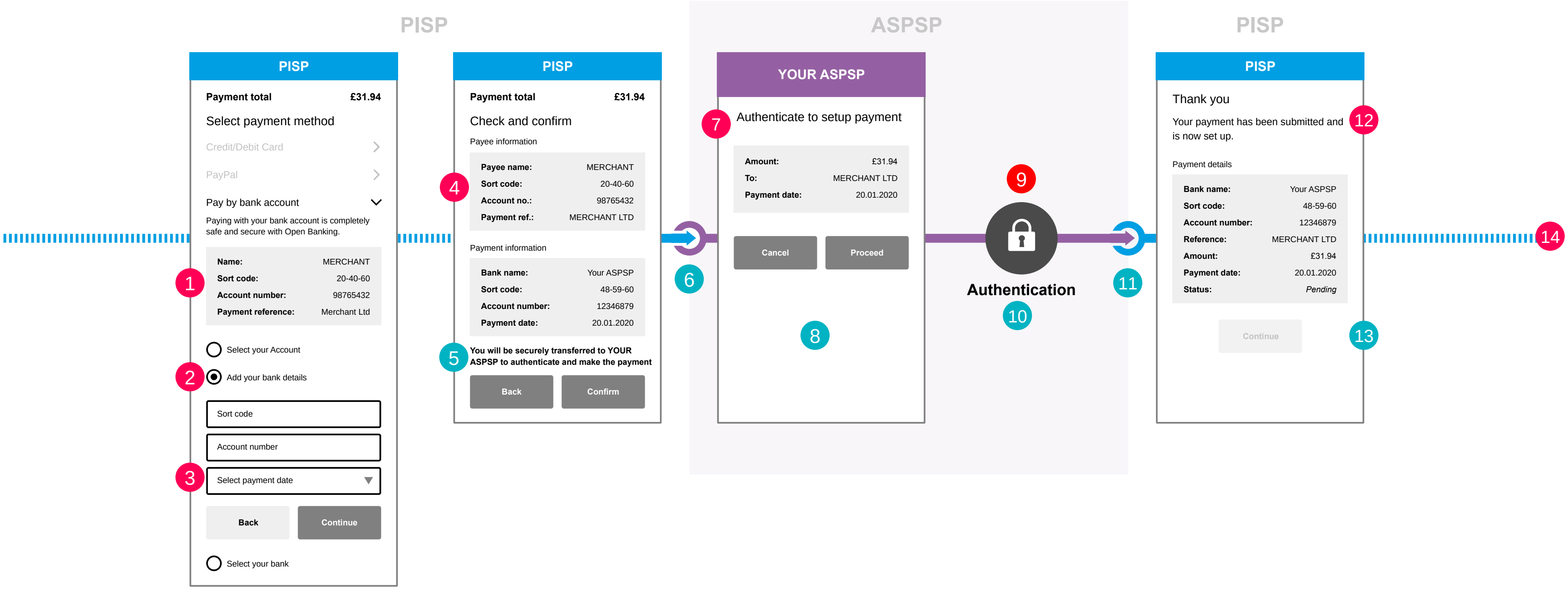
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.4 Single Domestic Scheduled Payments (Future Dated)

User Journey | Wireframes | Requirements and Considerations



PISP

Payment total	£31.94

Select payment method

Credit/Debit Card >

PayPal >

Pay by bank account ⌄

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your Account

● Add your bank details

Sort code

Account number

Select payment date ▼

Back | Continue

○ Select your bank

PISP

Payment total	£31.94

Check and confirm

Payee information

Payee name:	MERCHANT
Sort code:	20-40-60
Account no.:	98765432
Payment ref.:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879
Payment date:	20.01.2020

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Authenticate to setup payment

Amount:	£31.94
To:	MERCHANT LTD
Payment date:	20.01.2020

Cancel | Proceed

PISP

Thank you

Your payment has been submitted and is now set up.

Payment details

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879
Reference:	MERCHANT LTD
Amount:	£31.94
Payment date:	20.01.2020
Status:	*Pending*

Continue

What the research says

Consumer research has shown that 82% of consumers would like to see the payment schedule at least once in the journey.

> See more

4.1.4 Single Domestic Scheduled Payments (Future Dated)

User Journey | Wireframes | Requirements and Considerations

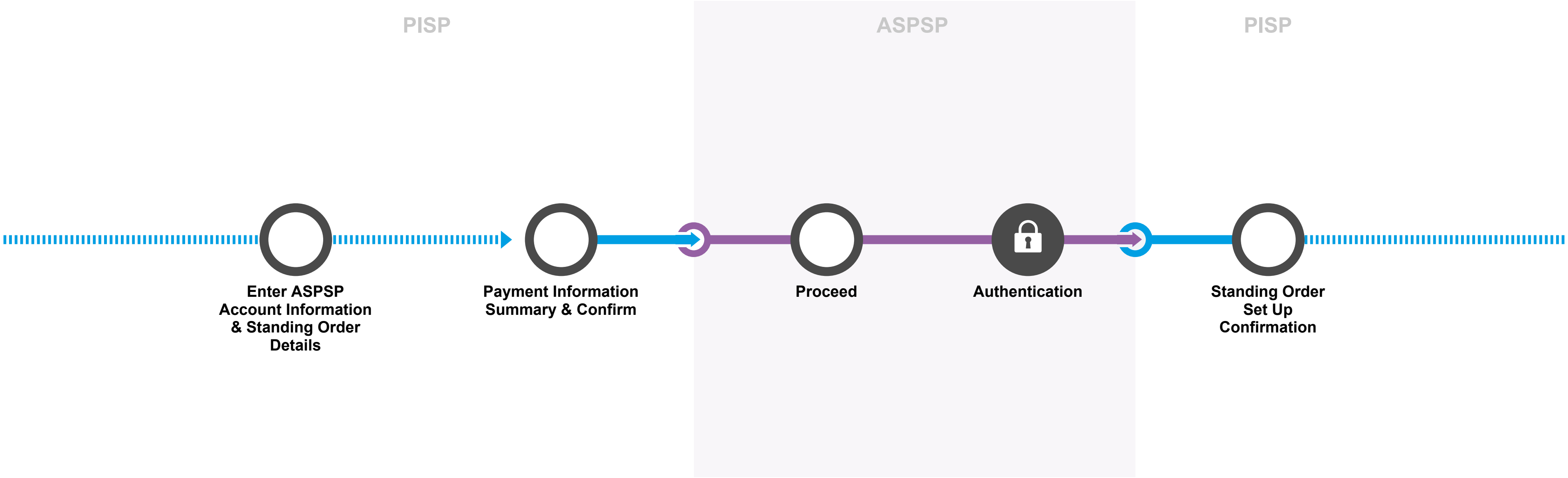
	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters:** As per 4.1.1, item #1	• RTS Art. 36(4)	22	PISP	Required
2	**PSU payment Account Selection:** As per 4.1.1, item #2	• n/a	24	PISP	Required
3	**Execution Date:** PISPs **must** allow PSUs to select the expected execution date for the payment by the ASPSPs.	• EBA Guidelines (CP) - 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraph 17.29 - 17.31	21	PISP	Required
4	**PSU Consent to PISP** PISPs **must** request for the PSUs' consent to the payment in a clear and specific manner. PISPs **must** display the following information in the consent screen: • Payment Execution Date • Payment Amount and Currency (GBP for UK implementations) • Payee Account Name • Payment Reference, **if** it has been entered by PSUs or pre-populated by PISPs in item #1 • PSU payment Account Identification **and/or** the selected ASPSP (based on item #2 options) • *Note 1: if PSU payment Account identification is selected in item #2, PISPs **should** mask the PSU payment Account details on the consent screen. Otherwise, if the PSU payment Account identification has been input by PSUs in item #2, PISPs **should not** mask these details to allow PSUs to check and verify correctness* • *Note 2: if PSU payment Account identification is provided by PSUs in item #2, PISPs **could** use this to identify and display the ASPSP without having to ask PSUs.* For Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN): • if this has been provided by PSUs in item #1, then PISPs **must** also display this in the consent screen to allow PSUs to check and verify correctness • if this has been pre-populated by PISPs (e.g. in a eCommerce payment scenario) PISPs **could** choose whether to display this information or not	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
7	ASPSPs **must** display as minimum the Payment Amount and Currency (GBP for UK implementations) and the Payee Account Name. ASPSPs **should** also display the requested execution date	• RTS Art. 5(1)(a)	28	ASPSP	Required
9	As per 4.1.1 item #9	• Trustee P3/P4 letter Action P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
12	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.23-17.24 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
14	**Further Payment Status Update:** As per 4.1.1, item #13	• n/a	27	PISP	Recommended

	CX Considerations
5	As per 4.1.1, item #4
6	As per 4.1.1, item #5
8	If SCA as described in item #9 cannot occur on the same screen as #7 of displaying the amount and the payee(e.g. for some biometric authentications methods), then ASPSPs **should** offer PSUs options to proceed or cancel the payment with "equal prominence"
10	ASPSPs **should** inform PSUs about their "point of no return" for making the payment and that their payment will be made after authentication occurs. Example wording: "Authenticate to make payment"
11	As per 4.1.1, item #10
13	PISPs **must** provide message to PSUs to inform that amendment or cancelling of the payment must be done at their ASPSP.

Note: If the payment account identifier used by PSUs to setup a future dated payment order, via PISPs, is no longer valid (e.g. expired/reported lost stolen PAN), ASPSPs should still allow the execution of the payment, on the scheduled date for which were setup.

4.1.5 Standing Orders

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations


PISP
ASPSP
PISP
Enter ASPSP Account Information & Standing Order Details
Payment Information Summary & Confirm
Proceed
Authentication
Standing Order Set Up Confirmation

PSUs can setup, through PISPs, an instruction to their ASPSPs to make a series of payments of a specific amount to a specific payee on a number of specified future dates or on a regular basis.

The example reference journey illustrates account selection occurring in the PISP domain. However, please note that account selection can take place at the ASPSP domain. In this case, please follow the approach of reference journey 4.1.3.

Note: OBIE Standards do not currently support the amendment or cancellation of Domestic Standing Orders via PISPs. These payments may be amended or cancelled via the ASPSP’s direct online channel (where supported). Cancellation of these payments must be consistent with available capabilities on ASPSP's existing online platform, as well as, in accordance with the provisions of the PSRs relating to revocation of payment orders.

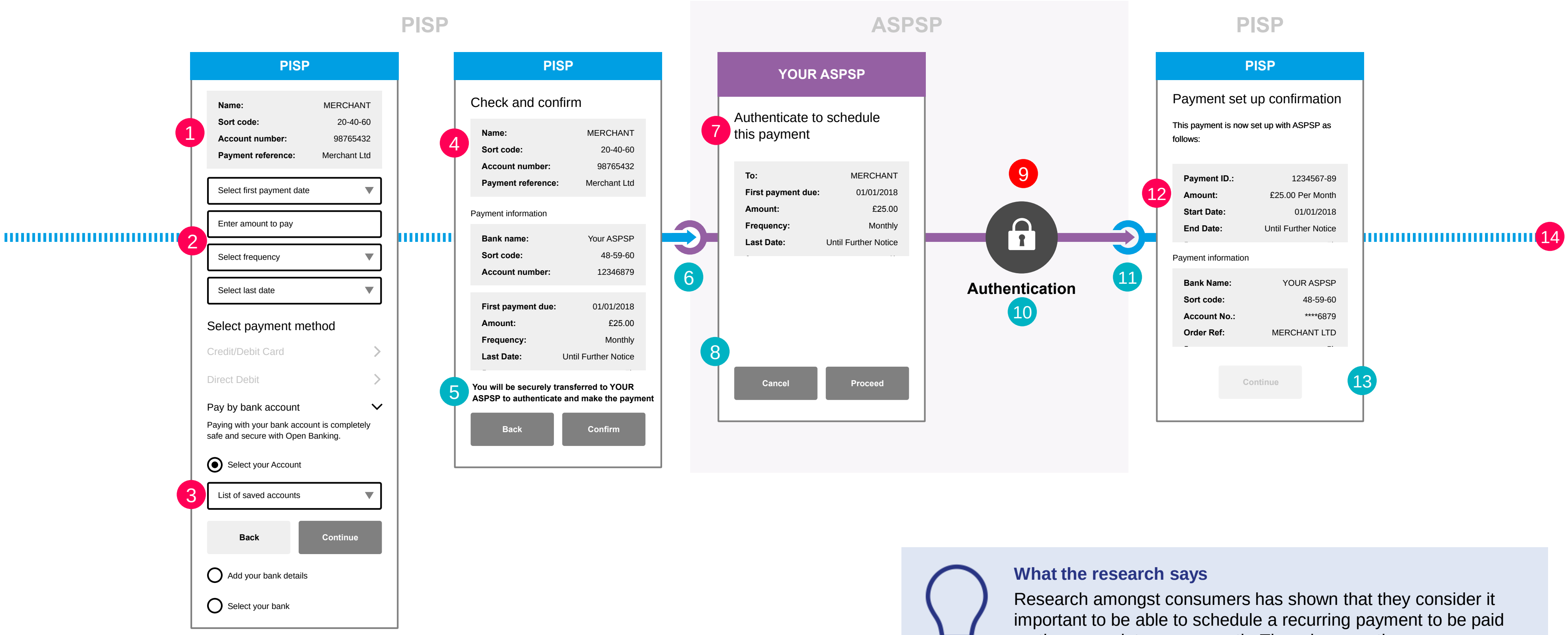
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.5 Standing Orders

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations



PISP

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

Select first payment date ▼

Enter amount to pay

Select frequency ▼

Select last date ▼

Select payment method

Credit/Debit Card >

Direct Debit >

Pay by bank account ⌄

Paying with your bank account is completely safe and secure with Open Banking.

● Select your Account

List of saved accounts ▼

Back | Continue

○ Add your bank details

○ Select your bank

PISP

Check and confirm

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879

First payment due:	01/01/2018
Amount:	£25.00
Frequency:	Monthly
Last Date:	Until Further Notice

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Authenticate to schedule this payment

To:	MERCHANT
First payment due:	01/01/2018
Amount:	£25.00
Frequency:	Monthly
Last Date:	Until Further Notice

Cancel | Proceed

PISP

Payment set up confirmation

This payment is now set up with ASPSP as follows:

Payment ID.:	1234567-89
Amount:	£25.00 Per Month
Start Date:	01/01/2018
End Date:	Until Further Notice

Payment information

Bank Name:	YOUR ASPSP
Sort code:	48-59-60
Account No.:	****6879
Order Ref:	MERCHANT LTD

Continue

What the research says

Research amongst consumers has shown that they consider it important to be able to schedule a recurring payment to be paid on the same date every month. There is currently some frustration with providers who do not take payments on set dates but rather indicate a window when payment will be taken.

> See more

4.1.5 Standing Orders

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters** PISPs **must** either allow PSUs to specify the below minimum set of parameters or pre-populate them for the PSUs: • Creditor Account Name • Creditor Account Identification (e.g. account number and sort code or roll number for UK implementations) • Reference of the payment (as per best practice)	• RTS Art. 36(4)	22	PISP	Required
2	**Standing Order Schedule(s)** PISPs **must** either allow PSUs to select at least one of following options **or** pre-populate them for the PSUs: The First payment date, payment Amount and Currency (GBP for UK implementations) The Recurring payment date, payment Amount and Currency (only if different from the first payment amount and date) If standing order is not open ended: • either the Final payment Date (only if different from the Recurring payment date), payment Amount and Currency (GBP for UK implementations) • or the Number of payments to be made by the standing order The Frequency of the payments (for available options on standing order frequency, please refer to Appendix section 7.4.1)	• EBA Guidelines (CP) - 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraph 17.29 - 17.31	21	PISP	Required
3	**PSU payment Account Selection:** As per 4.1.1, item #2	• n/a	24	PISP	Required
4	**PSU Consent to PISP** PISPs **must** request for the PSUs' consent to the payment in a clear and specific manner. PISPs **must** display the following information in the consent screen: • The Standing Order Schedule parameters including first payment, recurring payment, final payment and frequency as selected in item #3 • Payee Account Name • Payment Reference, **if** it has been entered by PSUs or prepopulated by PISPs in item #1 • PSU payment Account Identification **and/or** the selected ASPSP (based on item #2 options) • *Note 1: if PSU payment Account identification is selected in item #2, PISPs **should** mask the PSU payment Account details on the consent screen. Otherwise, if the PSU payment Account identification has been input by PSUs in item #2, PISPs **should not** mask these details to allow PSUs to check and verify correctness* • *Note 2: if PSU payment Account identification is provided by PSUs in item #2, PISPs **could** use this to identify and display the ASPSP without having to ask PSUs.* For Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN): • if this has been provided by PSUs in item #1, then PISPs **must** also display this in the consent screen to allow PSUs to check and verify correctness • if this has been pre-populated by PISPs (e.g. in a eCommerce payment scenario) PISPs **could** choose whether to display this information or not	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
7	ASPSPs **must** display as minimum the Payment Amount and Currency (GBP for UK implementations) and the Payee Account Name. ASPSPs **should** also display the Standing Order Schedule parameters.	• RTS Art. 5(1)(a)	28	ASPSP	Required
9	As per 4.1.1 item #9	• Trustee P3/P4 letter Action P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
12	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.23-17.24 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
14	**Further Payment Status Update:** As per 4.1.1, item #13	• n/a	27	PISP	Recommended

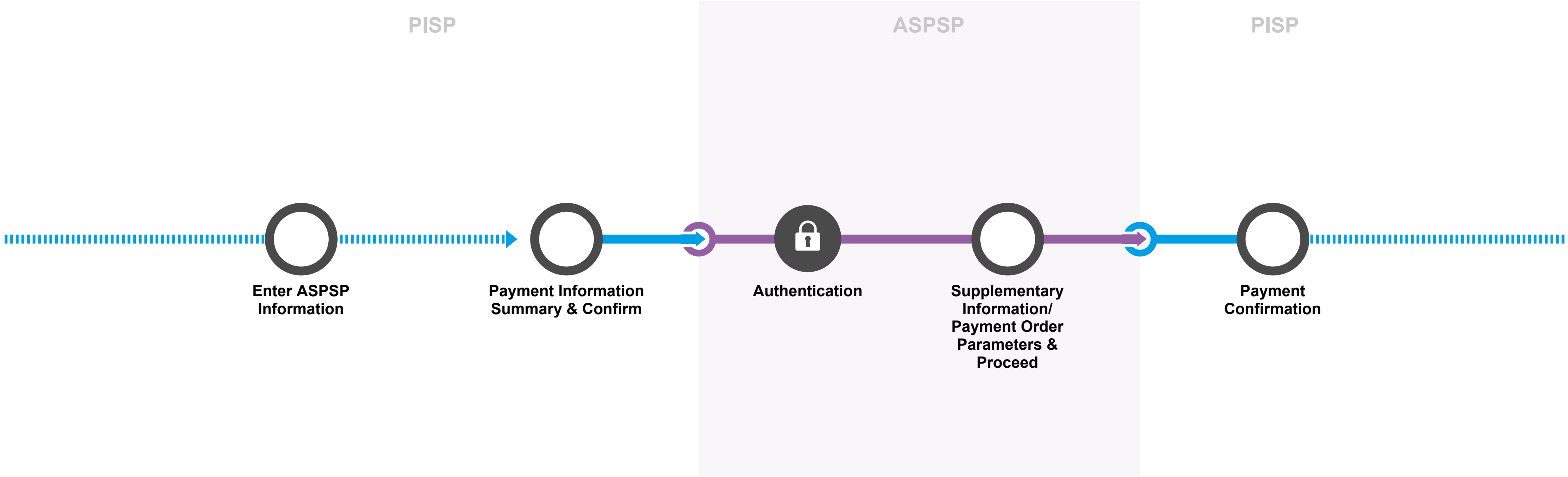
4.1.5 Standing Orders

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations

CX Considerations	
5	As per 4.1.1, item #4
6	As per 4.1.1, item #5
8	If SCA as described in item #9 cannot occur on the same screen (e.g. for some biometric authentications methods), then ASPSPs **should** offer PSUs options to proceed or cancel the payment with "equal prominence"
10	ASPSPs **should** inform PSUs about their “point of no return” for making the payment and that their payment will be made after authentication occurs. Example wording: "Authenticate to make payment"
11	As per 4.1.1, item #10
13	PISPs **must** provide message to PSUs to inform that modification or cancelling of the standing order must be done at their ASPSP.

Note: If the payment account identifier used by PSUs to setup a Standing Order payment order via PISPs is no longer valid (e.g. expired/reported lost stolen PAN), ASPSPs should still allow the execution of the standing order payments on the scheduled dates for which they were setup.

4.1.6 International Payments


PISP
ASPSP
PISP
Enter ASPSP Information
Payment Information Summary & Confirm
Authentication
Supplementary Information/ Payment Order Parameters & Proceed
Payment Confirmation

PSUs can initiate, through PISPs, single international payments from their GBP or foreign currency payment accounts. Payments can be made in any currency and to any country, using a number of routing options in order to meet the priority required, provided that functionality is available to PSUs when making international payments directly from their online payment account.

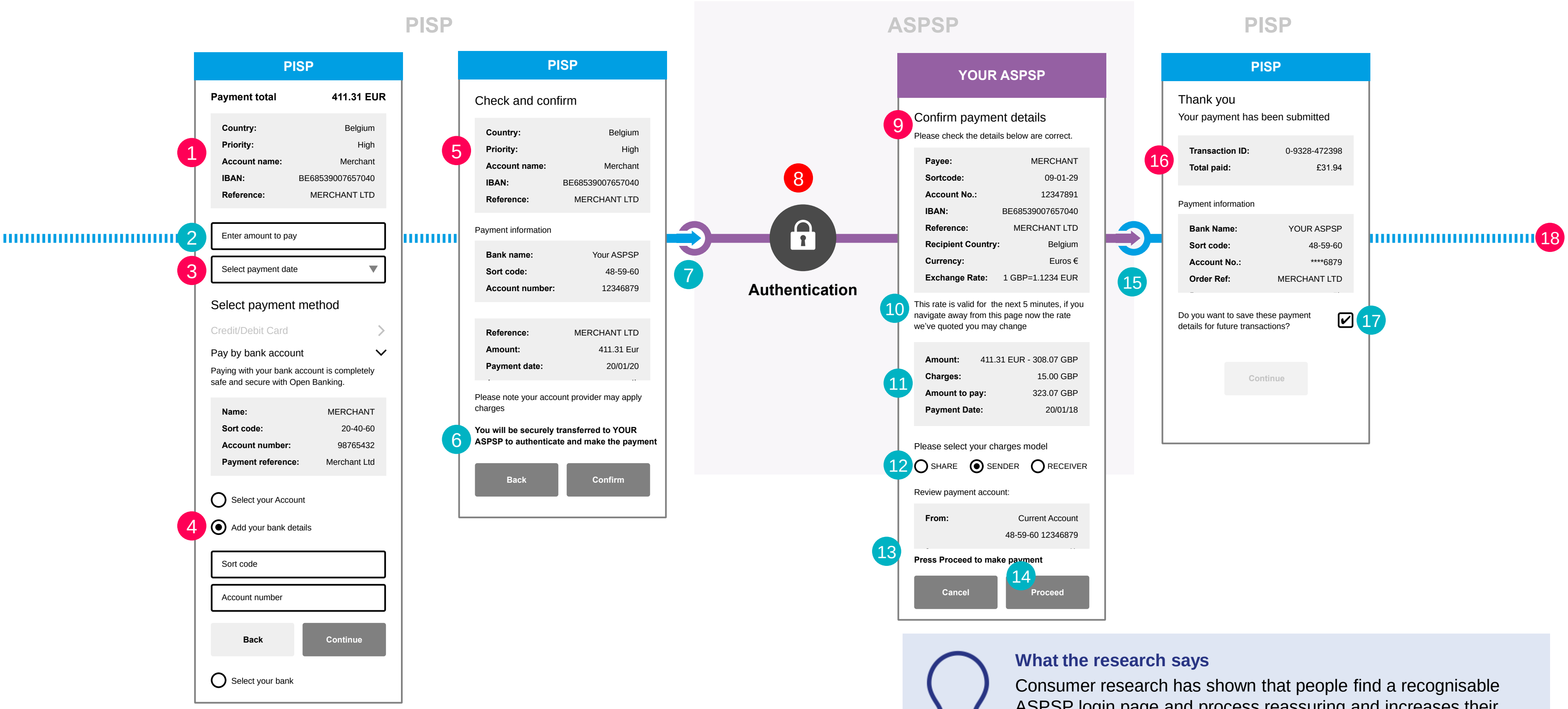
The authentication approach used in this journey replicates journey 4.1.2, where there is supplementary information to be displayed. If the payment order is incomplete then the principles of journey 4.1.3 apply. If all details of the payment order are provided by PISPs and ASPSPs decide not to display any supplementary information, then the principles of 4.1.1 may also be applied.

Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.6 International Payments



PISP

Payment total	**411.31 EUR**
Country:	Belgium
Priority:	High
Account name:	Merchant
IBAN:	BE68539007657040
Reference:	MERCHANT LTD

Enter amount to pay

Select payment date ▼

Select payment method

Credit/Debit Card >

Pay by bank account ∨

Paying with your bank account is completely safe and secure with Open Banking.

Name:	MERCHANT
Sort code:	20-40-60
Account number:	98765432
Payment reference:	Merchant Ltd

○ Select your Account

● Add your bank details

Sort code

Account number

Back **Continue**

○ Select your bank

PISP

Check and confirm

Country:	Belgium
Priority:	High
Account name:	Merchant
IBAN:	BE68539007657040
Reference:	MERCHANT LTD

Payment information

Bank name:	Your ASPSP
Sort code:	48-59-60
Account number:	12346879

Reference:	MERCHANT LTD
Amount:	411.31 Eur
Payment date:	20/01/20

Please note your account provider may apply charges

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back **Confirm**

YOUR ASPSP

Confirm payment details

Please check the details below are correct.

Payee:	MERCHANT
Sortcode:	09-01-29
Account No.:	12347891
IBAN:	BE68539007657040
Reference:	MERCHANT LTD
Recipient Country:	Belgium
Currency:	Euros €
Exchange Rate:	1 GBP=1.1234 EUR

This rate is valid for the next 5 minutes, if you navigate away from this page now the rate we've quoted you may change

Amount:	411.31 EUR - 308.07 GBP
Charges:	15.00 GBP
Amount to pay:	323.07 GBP
Payment Date:	20/01/18

Please select your charges model

○ SHARE ● SENDER ○ RECEIVER

Review payment account:

From:	Current Account 48-59-60 12346879

Press Proceed to make payment

Cancel **Proceed**

PISP

Thank you

Your payment has been submitted

Transaction ID:	0-9328-472398
Total paid:	£31.94

Payment information

Bank Name:	YOUR ASPSP
Sort code:	48-59-60
Account No.:	****6879
Order Ref:	MERCHANT LTD

Do you want to save these payment details for future transactions? ☑

Continue

What the research says

Consumer research has shown that people find a recognisable ASPSP login page and process reassuring and increases their confidence in the journey.

> See more

4.1.6 International Payments

User Journey | Wireframes | CEG Checklist Requirements | CEG Checklist Requirements and CX Considerations | Additional Information

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	<u>**Minimum Set of Parameters**</u>: PISPs **must** either allow PSUs to specify the below minimum set of parameters or pre-populate them (e.g. in cases of supplier invoice payments or eCommerce journeys): • Payment Amount and Currency • Destination Country • Instruction Priority (Normal or Urgent) • Payee Account Name • Payee Account Identification details (e.g.. IBAN) [1] • Payment Reference - This is optional filed but it is good practice to be populated for a payment	• RTS Art. 36(4)	22	PISP	Required
3	**If** PISPs want to offer PSUs the ability to make an **International Scheduled Payment (Future Dated)**,then PISPs **must** allow PSUs to select the execution date for the payment by the ASPSPs.	• EBA Guidelines (CP) - 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraph 17.29 - 17.31	21	ASPSP	Required
4	<u>**PSU payment Account Selection:**</u> As per 4.1.1, item #2	• n/a	24	PISP	Required
5	<u>**PSU Consent to PISP:**</u> PISPs **must** request for the PSUs' consent to the payment in a clear and specific manner. PISPs **must** display the following information in the consent screen: • Payment Amount and Currency • Destination Country • Instruction Priority (Normal or Urgent) • Payee Account Name • Payment Execution Date (same day processing or future date) • Payment Reference, **if** it has been entered by PSUs or pre-populated by PISPs in item #1 • PSU payment Account Identification **and/or** the selected ASPSP (based on item #2 options) • *Note 1: if PSU payment Account identification is selected in item #2, PISPs **should** mask the PSU payment Account details on the consent screen. Otherwise, if the PSU payment Account identification has been input by PSUs in item #2, PISPs **should not** mask these details to allow PSUs to check and verify correctness* • *Note 2: if PSU payment Account identification is provided by PSUs in item #2, PISPs **could** use this to identify and display the ASPSP without having to ask PSUs* For Payee Account Identification details (e.g. IBAN) [1] • **if** this has been provided by PSUs in item #1, then PISPs **must** also display this in the consent screen to allow PSUs to check and verify correctness • **if** this has been pre-populated by PISPs (e.g. in a eCommerce payment scenario) PISPs **could** choose whether to display this information or not	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	PISP	Required
8	As per 4.1.1 item #9	• RTS Art. 33(2) • Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
9	<u>**Supplementary Information / Additional Payment Order Details**</u> ASPSPs may need to include supplementary information to be displayed to the PSU. Alternatively, if the payment order is not complete, ASPSPs **must** allow PSUs to provide these additional payment order details (e.g. PSU payment account). In these instances, a step after authentication to display the information associated with the payment may required. This information may include: • PSU payment Account Identification • Payee Account Name • Payment Reference • Payee Account Identification details (e.g. account number and sort code or additionally roll number or full IBAN) • Country • Payment Currency • Payment Amount • FX • Charges model (BEN/SHA/OUR) (for definitions please refer to appendix section 7.4.2.1) • Payment priority (Normal or Urgent) • Payment Execution Date (same day processing or future date)	• EBA Draft Guideline 5.2(d)	20	ASPSP	Required

4.1.6 International Payments

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
16	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.23-17.24 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
18	**Further Payment Status Update:** As per 4.1.1, item #13	n/a	27	PISP	Recommended

	CX Considerations
2	PISPs **could** display an indicative FX rate for the payment currency pair **if**: • PSUs selected a PSU payment Account or provided PSU payment Account details in item #2 • PSUs provided the currency of the selected PSU payment Account In that case, PISPs **must** clearly indicate to PSUs that the FX rate displayed is indicative and may be different to the FX rate to be provided by their ASPSPs
6	As per 4.1.1, step 4
7	As per 4.1.1, step 5
10	ASPSPs **must** display to the PSU the FX currency conversion rate to be used for the payment order. This FX rate can be: • Indicative - In this case ASPSPs **must** clearly inform PSUs that the FX rate is indicative and may be different than the actual rate that will be used for the payment order • Actual - ASPSPs **must** clearly inform PSUs for the validity period of this actual FX rate. If the payment order is not submitted within the validity window of the FX, then a new actual FX quote must be displayed. If PSUs confirm the payment but the payment order submitted by PISPs is not submitted within validity period, ASPSPs **could** choose to either reject the payment or process it at the agreed FX rate. ASPSPs **could** display the payment amount in the PSU payment Account currency (from applying the FX rate)
11	ASPSPs **must** ensure that charges related to international payments are provided to PSUs as agreed in the framework contract. Note1: Any provision of charges can only be those of the ASPSP as the Beneficiary's bank charges are not known in many cases. Note 2: Where the final charges are not known to the ASPSP, the responsibility should remain with the ASPSP for notifying the customer of the charges as per the PSD2 regulatory requirements.
12	Other Options: • ASPSPs **should** display the Final Debit Amount (including charges) in PSU payment Account currency • ASPSPs **could** display the expected Value Date for the international payment
13	ASPSPs **should** inform PSUs about their "point of no return" for making the payment and that their payment will be made after pressing the Proceed button. Example wording: *"Press Proceed to make payment"*
14	ASPSPs **must** allow PSUs to review the information described in items #9, #10, #11 & #12. The PSU can either proceed with the payment or cancel it, on the same screen using options with "equal prominence".
15	As per 4.1.1, item #10
17	As per 4.1.1, item #12

4.1.6 International Payments

Examples of international payments covered by OBIE PIS functionality include:

- SEPA Credit Transfer payments
- SEPA Instant Credit Transfer payments (where appropriate)
- Correspondent payments / SWIFT Payments - Single Customer Credit Transfer MT103 (single payment)
- International transfers (PSU's domestic account to PSU's overseas account)
- Currency account transfers (i.e. IATs in currency)
- RTGS on Target2 payments
- EBA Euro1 payments

The FX currency conversion rates applicable to international payments and the charges incurred by PSUs constitute supplementary information and thus the international payments journey follows the same approach as the one-off domestic single payment with supplementary information.

There are a large number of parameters that may need to be specified for an international payments journey. These depend on a number of factors such as the beneficiary country, currency, payment scheme, charges model and others. The basic journey shown below is based on a single SEPA Euro payment in the EEA. Further options are explained in the options section and in the Appendix section 7.4.3.

Note:
OBIE Standards do not currently support the amendment or cancellation of Future Dated International Payments via PISPs. PSUs have to go to their ASPSPs' direct online channel in order to amend or cancel these payments, where supported. In these cases cancellation must be allowed up to and including the business day prior to execution of the payment order by the ASPSP.

The cancellation can only happen in cases where the FX conversion of the payment is executed on settlement date. If the FX payment is executed (i.e. the PSU account debited) in advance of settlement, then the payment cannot be cancelled.

4.1.6.1 Scheduled International Payments (Future Dated)

Journey 4.1.6 can be used to initiate single future dated international payments. In this case, the execution date of the payment is captured by PSUs and included in the payment order. Thus:

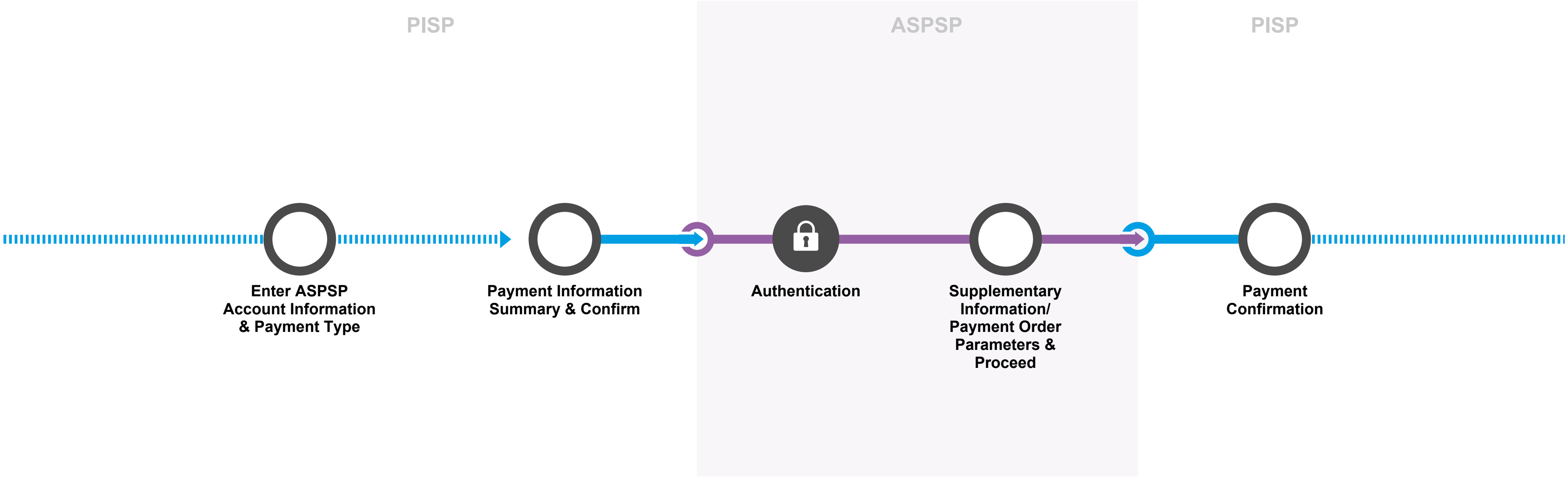
- **Minimum Set of Parameters:** PISPs **must** either allow PSUs to specify the selected execution date for the payment by the ASPSPs **or** pre-populate this information for the PSUs (in use cases where applicable).
- The execution date will then be included in the PSUs' consent screen and will be forwarded to ASPSPs as part of the payment order.
- OBIE Standards do not currently support the amendment or cancellation of Future Dated International Payments via PISPs. PSUs have to go to their ASPSPs' direct online channel in order to amend or cancel these payments, where supported. In these cases cancellation must be allowed up to and including the business day prior to execution of the payment order by the ASPSP.
- The cancellation can only happen in cases where the FX conversion of the payment is executed on settlement date. If the FX payment is executed (i.e. the PSU account debited) in advance of settlement, then the payment cannot be cancelled.

In general for this type of payment, both principle of journey 4.1.6 and 4.1.4 apply.

4.1.6.2 International Standing Orders

International Standing Orders can be setup by combining the principles described in journeys 4.1.6 and 4.1.5. In this case, the Standing Order Schedule for the international payments is captured by PSUs and included in the international payments order. Please refer to item #2 of journey 4.1.5.

4.1.7 Bulk/Batch Payments


PISP
ASPSP
PISP
Enter ASPSP Account Information & Payment Type
Payment Information Summary & Confirm
Authentication
Supplementary Information/ Payment Order Parameters & Proceed
Payment Confirmation

Business PSUs can initiate, through PISPs, bulk/batch payments allowing them to make multiple payments from their payment accounts.

The authentication approach used in this journey replicates journey 4.1.2, where there is supplementary information to be displayed. If the payment order is incomplete then the principles of journey 4.1.3 apply. This is due to the fact that there are certain cases where one of the parameters required for the bulk/batch payments may not have been specified or not included in the submitted file, or specific charges may apply.

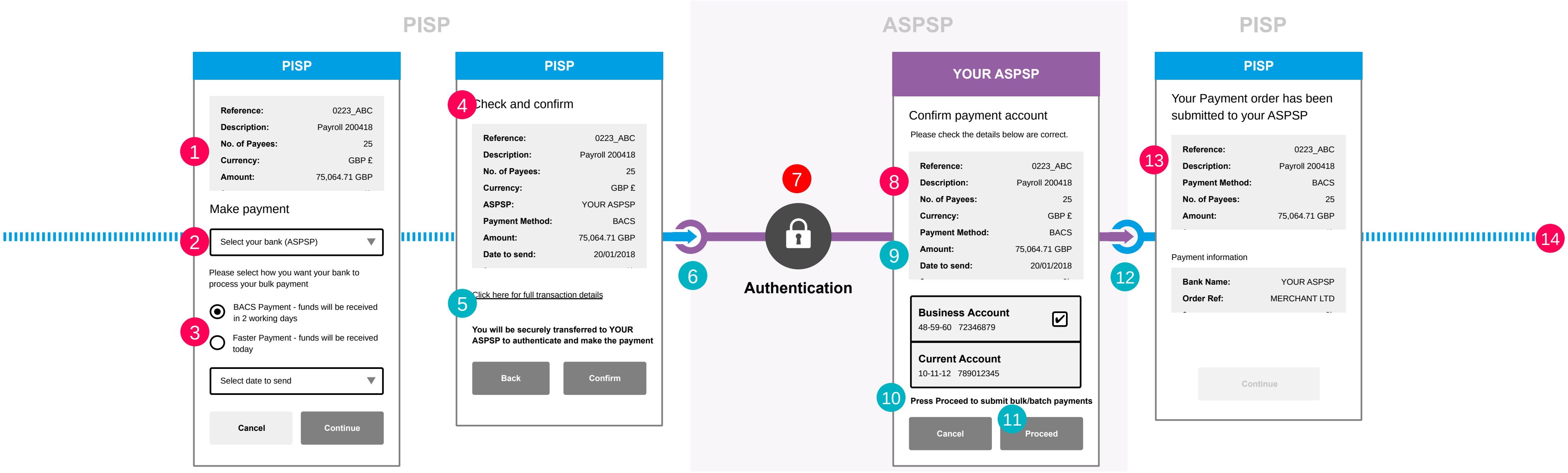
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.7 Bulk/Batch Payments

User Journey | Wireframes | CEG Checklist Requirements | CEG Checklist Requirements and CX Considerations | Additional Information



PISP

Reference:	0223_ABC
Description:	Payroll 200418
No. of Payees:	25
Currency:	GBP £
Amount:	75,064.71 GBP

Make payment

Select your bank (ASPSP) ▼

Please select how you want your bank to process your bulk payment

● BACS Payment - funds will be received in 2 working days

○ Faster Payment - funds will be received today

Select date to send ▼

Cancel | Continue

PISP

Check and confirm

Reference:	0223_ABC
Description:	Payroll 200418
No. of Payees:	25
Currency:	GBP £
ASPSP:	YOUR ASPSP
Payment Method:	BACS
Amount:	75,064.71 GBP
Date to send:	20/01/2018

Click here for full transaction details

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Confirm payment account

Please check the details below are correct.

Reference:	0223_ABC
Description:	Payroll 200418
No. of Payees:	25
Currency:	GBP £
Payment Method:	BACS
Amount:	75,064.71 GBP
Date to send:	20/01/2018

Business Account ☑
48-59-60 72346879

Current Account
10-11-12 789012345

Press Proceed to submit bulk/batch payments

Cancel | Proceed

PISP

Your Payment order has been submitted to your ASPSP

Reference:	0223_ABC
Description:	Payroll 200418
Payment Method:	BACS
No. of Payees:	25
Amount:	75,064.71 GBP

Payment information

Bank Name:	YOUR ASPSP
Order Ref:	MERCHANT LTD

Continue

What the research says

Research indicates that SMEs value having a summary information step page as part of the bulk / batch payment process to act as a check, including a 'cancel' option to minimise the chance of errors.

> See more

4.1.7 Bulk/Batch Payments

User Journey | Wireframes | CEG Checklist Requirements | CEG Checklist Requirements and CX Considerations | Additional Information

CEG Checklist Requirements		Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	PISPs **should** either allow PSUs to specify any of the below information or pre-populate this information on their behalf for the bulk & batch payments: • Total amount of all payments in the bulk/batch and currency • Number of payments included in the bulk/batch • Reference for the file (as per best practice)	• EBA Guidelines (CP) - 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraph 17.29 - 17.31	21	ASPSP	Required
2	**PSU payment Account Selection: If** PISPs allow PSUs to import/upload a batch/bulk file of payments, then the file may contain one PSU payment Account (for bulk) or multiple PSU payment Accounts (for batch). In this case PISPs **should not** allow the customer to define a PSU payment Account for the bulk or batch. PISPs **could** read the file and pre-populate the PSU payment Account in the case of bulk payments. Moreover, PISPs **could** use the PSU payment Account sort code(s) to identify and pre-populate the PSU's ASPSP that the bulk/batch needs to be submitted for processing. **Otherwise**, if no external file upload or PSU payment Account(s) in the file, PISPs **should** allow PSUs to either: • enter the PSU payment Account details • select their account details (assumes they have been saved previously) • select their ASPSP in order to select their PSU payment Account from there	• CMA Order 10.2 • n/a	23 24	ASPSP PISP	Required Required
3	**Minimum Set of Parameters: If** PISPs allows PSUs to import/upload a batch/bulk file of payments, then the file may contain the payment scheme(s) and the requested execution date(s) for the bulk/batch of payments. In this case, PISPs **should not** allow the customer to define the payment scheme and the requested execution date. PISPs **could** read the file and pre-populate the payment scheme and the requested execution date in the case of bulk payments and also for the batch payments if the same throughout the file. **Otherwise**, if no external file upload or payment scheme and the requested execution date in the file, PISPs **should** allow PSUs to to specify the below information: • Instruction instrument (payment scheme) • Requested Execution date *Note: For batch payments this will only hold if these parameters will need to apply to all the transactions within the batch.*	• RTS Art. 36(4)	22	PISP	Required
4	**PSU Consent to PISP**: PISPs **must** request for the PSU's consent to the payment clearly displaying any of the following information if specified by PSUs or pre-populated by PISPs: • Total amount of all payments in the bulk/batch and currency (subject to item #2 options) • Number of payments included in the bulk/batch (subject to item #2 options) • Reference for the file (as per best practice) (subject to item #2 options) • Instruction instrument (payment scheme) (subject to item #1 options) • Requested Execution date (subject to item #1 options) • PSU payment Account or selected ASPSP (subject to item #3 options) • *Note 1: if PSU payment Account is selected in previous screen, PISPs **should** mask the account details* • *Note 2: if PSU payment Account details are provided, PISPs **could** use the account sort-code to derive and display the ASPSP*	• EBA Guidelines (CP) - 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraph 17.29 - 17.31	21	ASPSP	Required
7	• As per 4.1.1 item #9	• RTS Art. 33(2) • Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
8	**Supplementary/ Missing Payment Information**: Although the payee details and total amount are known to the ASPSP before the PSU is authenticated, • ASPSPs **must** introduce a step after authentication to allow PSUs to provide additional information associated with the bulk/batch payment in order to complete the payment instructions, if the payment order is incomplete. This information may include: • PSU payment Account Identification details (for bulk payments only) • Instruction instrument (payment scheme) (for bulk payments and for batch only if it applies to all payments in the batch) • Requested Execution date (for bulk payments and for batch only if it applies to all payments in the batch) • ASPSPs **should** be able to introduce a step after authentication to display additional /supplementary information in relation to the bulk \batch payment instructions such as expected execution date, specific terms related to this payment type, charges etc.	• EBA Draft Guideline 5.2(d)	20	ASPSP	Required

4.1.7 Bulk/Batch Payments

User Journey | Wireframes | CEG Checklist Requirements | CEG Checklist Requirements and CX Considerations | Additional Information

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
13	**PISP Confirmation:** As per 4.1.1, item #11	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.26 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
14	**Further Payment Status Update:** As per 4.1.1, item #13	• n/a	27	PISP	Recommended

CX Considerations

5	As per 4.1.1, step 4
6	As per 4.1.1, step 5
9	ASPSPs **should** also display to PSUs all the payment instruction information received from PISPs.
10	ASPSPs **should** inform PSUs about their “point of no return” for making the payment and that their payment will be made after pressing the Proceed button. Example wording: *“Press Proceed to make payment“*.
11	ASPSPs **must** allow PSUs to review the information described in items #8, #9 & #10. The PSU can either proceed with the payment or cancel it, on the same screen using options with "equal prominence".
12	As per 4.1.1, step 10

4.1.7 Bulk/Batch Payments

OBIE Bulk/Batch payments proposition

For the purposes of this paper the following definitions of bulk and batch payments are used:

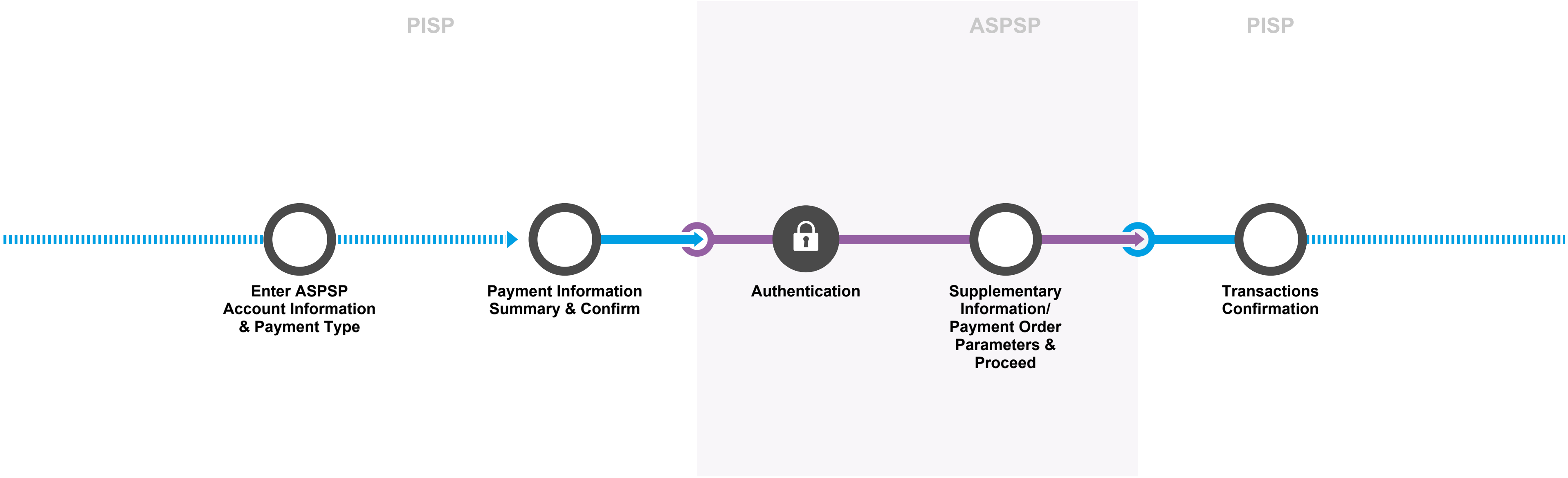
- Bulk = A group of payments (e.g. in a file) to be paid to multiple creditor accounts from the same debtor account, on the same date, with the same currency and through the same payment scheme
- Batch = A group of payments (e.g. in a file) to be paid to multiple creditor accounts from multiple debtor accounts. These may involved different payment execution dates, currencies and payment schemes.

Please also note the following working assumptions:

- For bulk payments, the PSU maybe able to select the PSU payment Account and other parameters of the bulk payment instruction at the ASPSP, if they are not included in file submitted by the PISP
- For batch payments, the PSU may not be able to select the PSU payment Account and other parameters of the bulk payment instruction at the ASPSP, if they are not included in the file submitted by the PISP.

4.1.8 Multi-authorisation Payments

User Journey | Wireframes | Requirements and Considerations


PISP
ASPSP
PISP
Enter ASPSP Account Information & Payment Type
Payment Information Summary & Confirm
Authentication
Supplementary Information/ Payment Order Parameters & Proceed
Transactions Confirmation

PSUs can setup, through PISPs, payments which require multiple parties with delegated user authority to authorise a payment order. This functionality can be used by the ASPSPs for any payment initiation that requires multiple authorities (including consumers, SMEs and Corporates).

The authentication approach used in this journey replicates journey 4.1.2, where there is supplementary information to be displayed. If the payment order is incomplete then the principles of journey 4.1.3 apply. The principles of 4.1.1 may also be applied if all details of the payment order are provided by PISPs, and ASPSPs decide not to display any supplementary information.

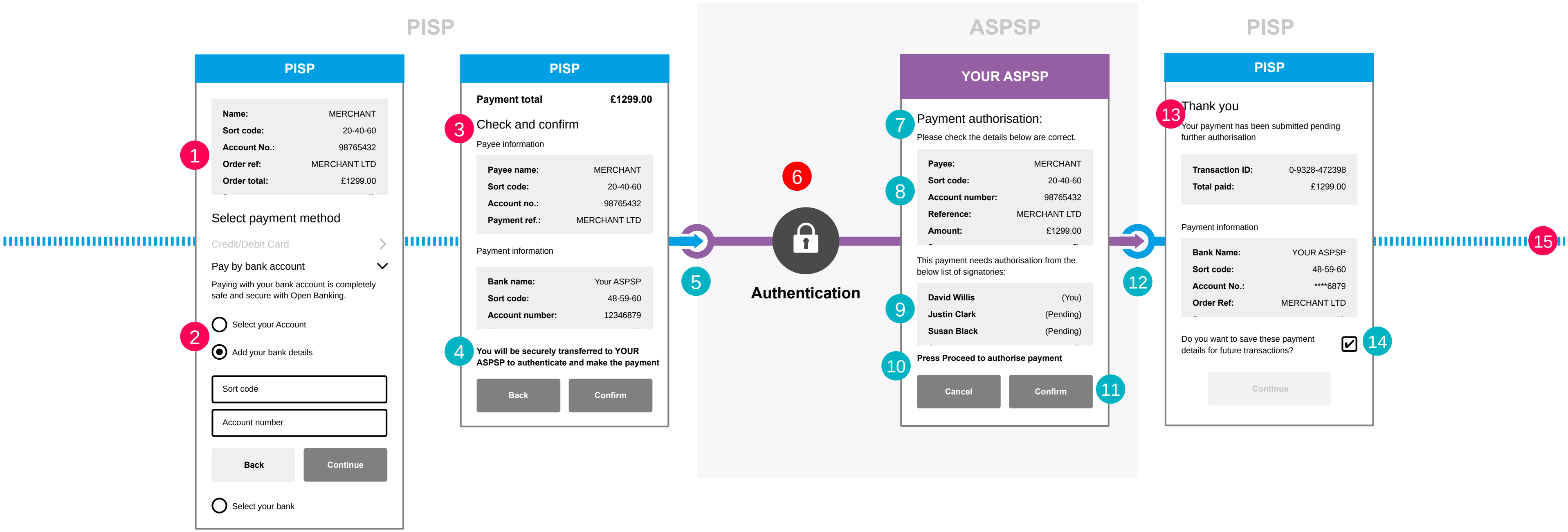
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

4.1.8 Multi-authorisation Payments

User Journey | Wireframes | Requirements and Considerations



PISP

Name: MERCHANT
Sort code: 20-40-60
Account No.: 98765432
Order ref: MERCHANT LTD
Order total: £1299.00

Select payment method

Credit/Debit Card

Pay by bank account

Paying with your bank account is completely safe and secure with Open Banking.

○ Select your Account

● Add your bank details

Sort code

Account number

Back | Continue

○ Select your bank

PISP

Payment total £1299.00

Check and confirm

Payee information

Payee name: MERCHANT
Sort code: 20-40-60
Account no.: 98765432
Payment ref.: MERCHANT LTD

Payment information

Bank name: Your ASPSP
Sort code: 48-59-60
Account number: 12346879

You will be securely transferred to YOUR ASPSP to authenticate and make the payment

Back | Confirm

YOUR ASPSP

Payment authorisation:

Please check the details below are correct.

Payee: MERCHANT
Sort code: 20-40-60
Account number: 98765432
Reference: MERCHANT LTD
Amount: £1299.00

This payment needs authorisation from the below list of signatories:

David Willis (You)
Justin Clark (Pending)
Susan Black (Pending)

Press Proceed to authorise payment

Cancel | Confirm

PISP

Thank you

Your payment has been submitted pending further authorisation

Transaction ID: 0-9328-472398
Total paid: £1299.00

Payment information

Bank Name: YOUR ASPSP
Sort code: 48-59-60
Account No.: ****6879
Order Ref: MERCHANT LTD

Do you want to save these payment details for future transactions? ☑

Continue

4.1.8 Multi-authorisation Payments

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters:** As per 4.1.1, item #1	• RTS Art. 36(4)	22	PISP	Required
2	**PSU payment Account Selection:** As per 4.1.1, item #2	• n/a	24	PISP	Required
3	**PSU Consent to PISP** : As per 4.1.1, item #3	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47	8	TPP	Required
6	• As per 4.1.1 item #9	• RTS Art. 33(2) • Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	19 1	ASPSP	Required
13	**PISP Confirmation** PISPs **must** display the information received from the ASPSP. This information may include: • whether the payment requires multiple authorisations • the status of the multiple authorisations • the number of required authorisations (total required at the start of the multi authorisation journey) • number of authorisations complete • the date and time of last authorisation update • the date and time the authorisation flow must be completed	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraph 17.26 • PSR 44(1)(a)	25 26	ASPSP PISP	Required Required
15	**Further Payment Status Update:** As per 4.1.1, item #12	• n/a	27	PISP	Recommended

	CX Considerations
4	As per 4.1.1, item #4
5	As per 4.1.1, item #5
7	Although some of the payment instruction order details are known to ASPSPs before PSUs are authenticated, ASPSPs **must** introduce a step after authentication to display supplementary information associated with the payment such as for example to inform the PSU that the PSU payment Account requires multiple authorisations before the payment can be executed.
8	ASPSP **should** display to the PSU all the payment instruction information received from the PISP together with the supplementary information required for the multi-authorisation payment.
9	ASPSPs **should** display to PSUs the same information about the multi-auth payment as displayed for multi-auth payments initiated by the PSU directly via the ASPSP's online channels. This information **could** include the number and name of the authorisers that need to authorise the payment before it can be processed and executed by the ASPSP.
10	ASPSPs **should** inform PSUs about their "point of no return" for making the payment and that their payment will be made after pressing the Proceed button. Example wording: *"Press Proceed to make payment"*.
11	ASPSP **must** allow the PSU to proceed with these additional items for the payment initiation or cancel it, on the same screen with steps 7,8 & 9.
12	As per 4.1.1, step 10.
14	**If** PSUs provided payment account identification details (as per item #2 options), PISP could save the account details for future transactions ,provided that this is explicitly agreed by the PSU.

5.0 Card Based Payment Instrument Issuers (CBPIIs)

One of the primary ambitions of these guidelines is to provide simplification and consistency throughout each stage of the Open Banking implementation.
As such, we have defined a core set of PSU journeys for CBPIIs.

Regulation 68 of the PSRs provides a mechanism whereby payment service providers (PSPs) issue a card based instrument which is linked to an account or accounts held at one or more different ASPSPs (provided those accounts are accessible online) and request a confirmation on the availability of funds. The payment service provider that issues the payment instrument is known as a Card-Based Payment Instrument Issuer or CBPII.

When the PSU uses the card-based payment instrument to initiate a payment transaction, the CBPII is entitled to request a confirmation from the PSUs ASPSP to which the account is linked, to confirm whether there are sufficient funds available for the transaction amount. The ASPSP is obliged to respond with an immediate 'yes/no' answer, provided the relevant regulatory requirements are met.

Customer benefits

There may be several reasons for the customer to use the CBPII card and this will mainly depend on the actual CBPII proposition. Example benefits may include the following:

- Loyalty scheme with benefits for using the CBPII card (points, air miles, cash back etc)
- Customer has a single instrument to make payments from multiple accounts, with no need to carry a card wallet full of cards
- Customer only has to manage one card relationship, for example:
  - Remember the details for one card
  - Store the details of one card with a retailer
- Customer will only have a single combined transaction list and statement for all their purchases
- Single proxy for multiple accounts for all card usages
- Less probability to have a purchase transaction declined as multiple funding accounts may be used without having to try several different cards
- Less need to handle expiring cards from various bank accounts

Please note that the Confirmation of Funds (CoF) mechanism does not guarantee to the CBPII that they will receive the funds from the PSUs account, as CoF is only a snapshot which confirms whether the funds are available at the time of the request. The ASPSP does not block funds on the PSU's account for the CBPII card payment.

Moreover, please note that the CoF API made available to CBPIIs is for funds checking only and does not facilitate settlement of the transaction (i.e. the transfer of the funds from the PSU funding account to the CBPII). This is in the CBPII competitive space and could be fulfilled using various means such as Direct Debit, PISP push payment etc.

Finally, PSRs and RTS do not appear to place limitation into the number of payment accounts that can be linked into a single CBPII issued card. This is in the competitive space of the CBPIIs. Furthermore, PSRs and RTS do not specify which card types can be linked with the payment account, for example physical cards only or also tokenised virtual cards. Again, this is in the competitive space of the CBPIIs.

5.1 CBPII Core Journeys

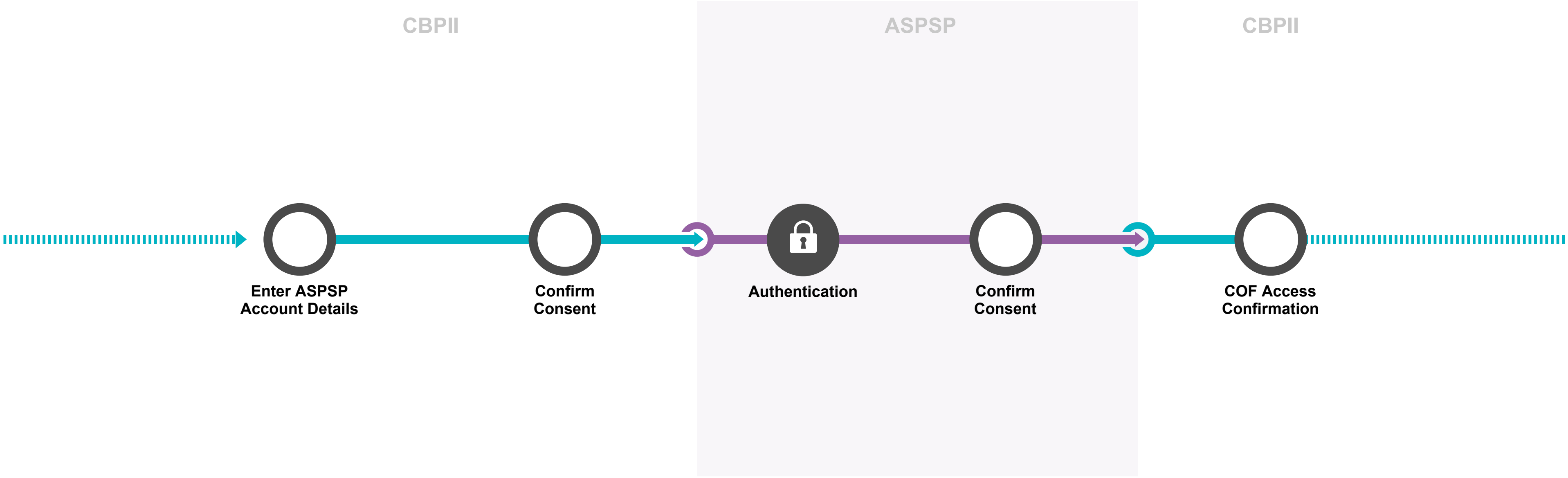
Open Banking API specifications support CoF services for Card Based Payment Instrument Issuers (CBPIIs). These services allow PSUs to provide explicit consent to an ASPSP, so that they can respond to confirmation of funds requests from CBPIIs, limited to a Y/N. CBPIIs can subsequently submit confirmation of funds requests to the ASPSP provided that the PSU has also provided their explicit consent to the CBPII and has initiated a payment transaction with the payment instrument for the amount in question.

This section describes how each of the Participants (CBPIIs and ASPSPs) in the delivery of these services can optimise the customer experience for these services. Furthermore, it provides some clarifications to these Participants on the usage of the APIs which are not covered by the technical specifications and some best practice guidelines for implementation of the customer journeys.

Please note that unlike AIS journeys, Consent given to ASPSPs and CBPIIs can be “until further notice” and does not expire after 90 days. Thus, authentication does not need to occur after the initial set up for the specific CBPII has been completed. Consent to CBPIIs access will generally be ongoing or setup for a set period of time, after which PSUs will need to renew it.

Featured journeys

5.1.1 Consent for Confirmation of Funds (CoF)



Regulation 68(3)(a) of the PSRs, requires that the CBPIIs **must** have the explicit consent of the PSU prior to making Confirmation of Funds requests to the PSUs ASPSPs.

Regulation 68(5)(b) of the PSRs requires that the ASPSPs **must** have the explicit consent of the PSU prior to responding to the first CBPII Confirmation of Funds request. This applies to each specific CBPII and each PSU payment account, that is accessible online.

The above journey illustrates the consent given by PSUs for CoF purposes.

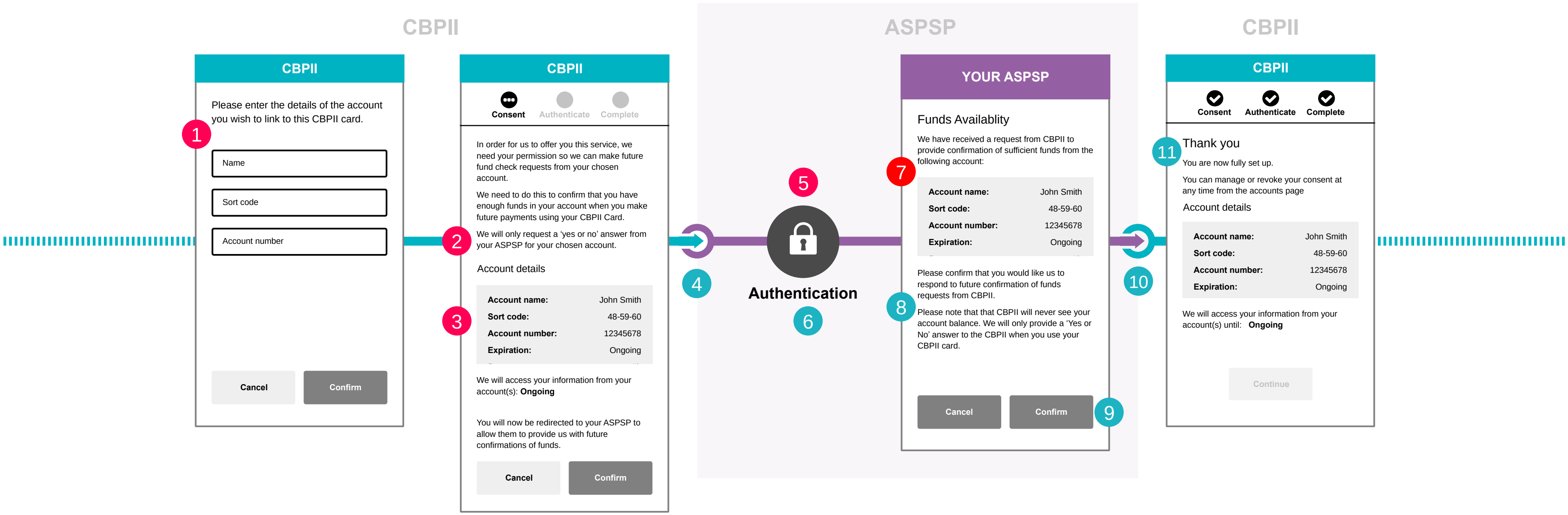
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

5.1.1 Consent for Confirmation of Funds (CoF)

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations | Additional Information



CBPII

CBPII

Please enter the details of the account you wish to link to this CBPII card.

Name

Sort code

Account number

Cancel **Confirm**

CBPII

Consent Authenticate Complete

In order for us to offer you this service, we need your permission so we can make future fund check requests from your chosen account.

We need to do this to confirm that you have enough funds in your account when you make future payments using your CBPII Card.

We will only request a 'yes or no' answer from your ASPSP for your chosen account.

Account details

Account name:	John Smith
Sort code:	48-59-60
Account number:	12345678
Expiration:	Ongoing

We will access your information from your account(s): **Ongoing**

You will now be redirected to your ASPSP to allow them to provide us with future confirmations of funds.

Cancel **Confirm**

ASPSP

Authentication

YOUR ASPSP

Funds Availablity

We have received a request from CBPII to provide confirmation of sufficient funds from the following account:

Account name:	John Smith
Sort code:	48-59-60
Account number:	12345678
Expiration:	Ongoing

Please confirm that you would like us to respond to future confirmation of funds requests from CBPII.

Please note that that CBPII will never see your account balance. We will only provide a 'Yes or No' answer to the CBPII when you use your CBPII card.

Cancel **Confirm**

CBPII

CBPII

Consent **Authenticate** **Complete**

Thank you

You are now fully set up.

You can manage or revoke your consent at any time from the accounts page

Account details

Account name:	John Smith
Sort code:	48-59-60
Account number:	12345678
Expiration:	Ongoing

We will access your information from your account(s) until: **Ongoing**

Continue

5.1.1 Consent for Confirmation of Funds (CoF)

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations | Additional Information

CEG Checklist Requirements		Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Minimum Set of Parameters** CBPIIs **must** allow PSUs to enter their payment Account Identification details in at least one of the ways specified in the OBIE V3 Read/Write API Specifications (e.g. account number and sort code - with additional roll number if required, IBAN, PAN, Paym and other formats). *Note: In some of the above cases, CBPIIs may also need PSUs to provide their ASPSP name so that CBPIIs can check whether ASPSPs will be able to match the account identifier to the underlying PSU payment account.* CBPIIs **could** also choose to allow PSUs to enter their payment account name.	• RTS Art. 36(4)	34	CBPII	Required
2	**PSU Consent to CBPII** CBPIIs **must** provide PSUs sufficient information to enable them to make an informed decision about whether to consent to the CBPII making CoF requests to their ASPSP accounts. For example, the CBPII **should** provide details on the purpose for which the funds checks will be used (including whether any other parties will have access to the information) and clear and reassuring messages about what information will be made available from the ASPSPs. This **should** include information such as the following: • Prior to making Confirmation of funds requests to their ASPSPs, CBPIIs must have been given explicit consent by PSUs. • CBPIIs will only received a 'yes/no' answer about the availability of funds at PSUs' account, sufficient to cover a specific amount of a CBPII transaction. • The Confirmation of Funds Response will not be stored by CBPIIs. • Confirmation received by CBPIIs cannot be used for any other purpose than the execution of the transaction for which the request is made. • The period over which CoF consent is requested and the reasons why. • How PSUs will be able to revoke their consent through the CBPII environment.	• FCA guidance 17.46	8	CBPII	Required
3	**PSU Consent to CBPII** CBPIIs **must** request for the PSUs' consent to in a clear and specific manner. CBPIIs **must** display the following information in the consent screen: • PSU payment Account Identification **and/or** the selected ASPSP (based on item #1 options) • *Note 1: if PSU payment Account identification is selected in item #1, CBPIIs **should** mask the PSU payment Account details on the consent screen. Otherwise, if the PSU payment Account identification has been input by PSUs in item #1, CBPIIs **should not** mask these details to allow PSUs to check and verify correctness* • *Note 2: if PSU payment Account identification is provided by PSUs in item #2, CBPIIs **could** use this to identify and display the ASPSP without having to ask PSUs.* • Expiration Date & Time: Consent **could** be on-going or for set period of time. If this parameter is provided by CBPIIs the consent will have limited life span and will expire on the specified date. CBPIIs could choose to align this expiry date with the expiration date of the card based instrument issued to PSUs. Alternatively, they **could** choose a different period for security or business reasons, or they **could** also allow PSUs to select their desired expiry date explaining however the implications this may have on the usage of their issued card. • PSU payment Account name, if provided by PSUs in item #1	• FCA guidance 17.46 • PSR Reg. 68(3)(a) & (b)	8 32	CBPII CBPII	Required Required
5	**Authentication** ASPSPs **must** apply SCA. The ASPSP authentication **must** have no more than the number of steps that the PSU would experience when directly accessing the ASPSP channel.	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)	1	ASPSP	Required
7	**ASPSP Consent** Prior to receiving the first request from each CBPII, ASPSPs **must** obtain explicit consent from the PSU to provide confirmation of funds to CBPII requests. ASPSPs **must** be able to introduce an additional screen to display Information associated with the Confirmation of Funds consent. ASPSPs **must** display to PSUs all the information related to the CoF consent. This information includes the following: • CBPII requesting CoF to the PSU account • PSU payment Account Name • PSU payment Account Identification • Consent Expiration Date & Time: (this could also be ongoing) *Note: PSU's payment account details may be shown in account number and sort-code format in cases when PSU in item #1 provided account identification details in other formats such as a PAN, IBAN, Paym mobile number, etc., subject to CBPII offering these options.*	• PSR Reg. 68(5)(b) • FCA Approach Document paragraph 17.18	31	ASPSP	Required

5.1.1 Consent for Confirmation of Funds (CoF)

CX Considerations	
4	Generic CBPII to ASPSP redirection Screen and message. Please refer to Section 2.2.5.
6	**Authentication** ASPSPs **could** display a message to prompt PSUs to authenticate to continue with setting up Funds Check.
8	**ASPSP Supplementary Information** ASPSPs **should** provide some supplementary information in relation to their obligations for CoF requests and how these will be handled. This may include but not limited to the following: • ASPSPs will only respond with a 'yes/no' answer about the availability of funds at PSUs' account, sufficient to cover a specific amount of a CBPII transaction. • ASPSPs are not permitted to provide additional account information (such as the account balance) or block funds on the PSU's account for the CBPII transaction. • PSUs may be able to view their history of Confirmation of Funds requests including the identity of CBPIIs which made CoF requests and the provided response, using their Access Dashboard at their ASPSPs. • How PSUs will be able to revoke their consent from the ASPSP Access Dashboard.
9	ASPSPs **should** allow PSUs to review as a part of the authentication process all the information related to the CoF. PSUs can either proceed with the CoF consent or cancel it, on the same screen with items #7 & #8,using "equal weight" options.
10	Generic ASPSP to CBPII redirection Screen and message. Please refer to Section 2.2.5.
11	**CBPII Confirmation** CBPIIs **should** confirm to PSUs the successful completion of the Confirmation of Funds account access request. CBPIIs **could** also choose to display again: • the PSU payment account identification details (this can now be in masked form) • the expiration date of the Confirmation of Funds consent

5.1.1 Consent for Confirmation of Funds (CoF)

User Journey | Wireframes | CEG Checklist Requirements | CX Considerations | Additional Information

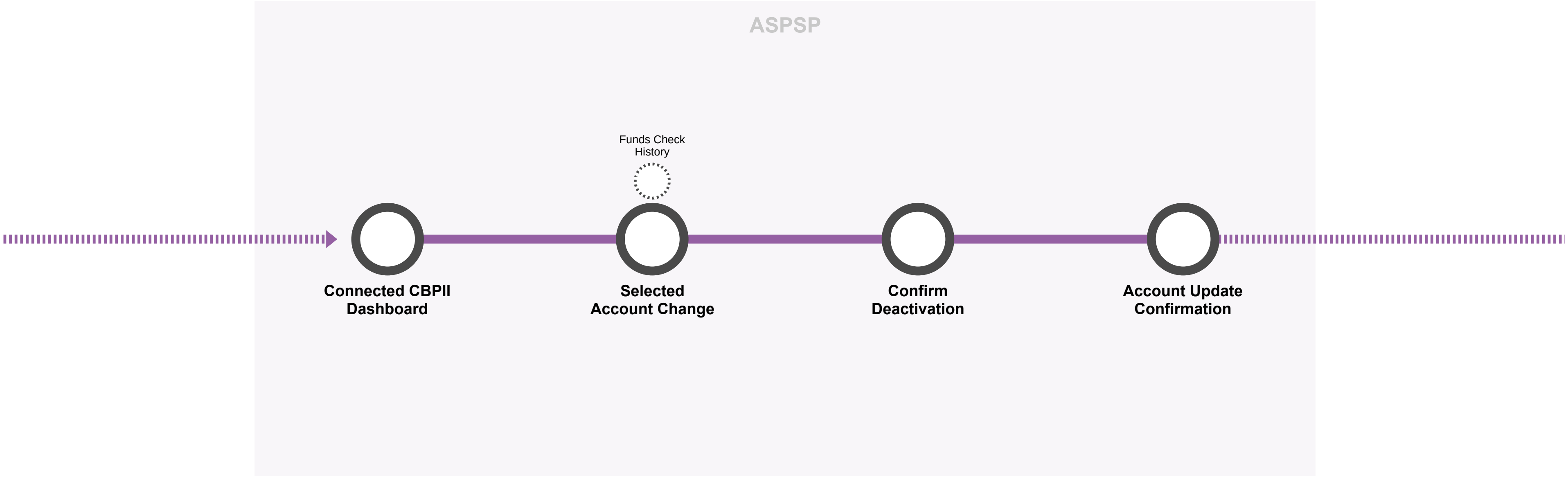
PSU Research Considerations

Research undertaken on behalf of OBIE with consumer PSUs has identified the following points:

- PSUs do not understand the term CBPII and thus other language should be used for the consent group
    - Consumers have no spontaneous awareness or understanding of CBPII. It is easiest to explain to them using a practical example of how it might operate. Thus, the term CBPII is unknown and should avoided in customer journeys.
    - Once explained, ‘Confirmation of Funds’ is a workable name for part of the process, as is ‘Funds availability check’.
    - Other suggestions included: ‘Funds check’, ’Funds confirmation’ and ‘Pre-transaction check’.
- PSUs trust and are willing to provide their consent to the CBPIIs to make CoF requests to their ASPSP accounts
    - Once the concept has been explained, PSUs are happy to provide consent to make CoF requests, although in their minds these are of secondary importance compared to payments.
- PSUs understand that CoF is ‘yes’/ ‘no’ answer and that their ASPSP will neither provide any other account information to the CBPII such as the actual balance on their account, nor allow them to initiate any payments
    - The process of CoF and what information the CBPII card issuer would have access to are both easy to understand, once explained, and make sense / reassure PSUs.

5.1.2 Access Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations



Regulation 68(6) PSRs states that if the PSU so requests, the ASPSP must inform the PSU of the CBPII which has made previous CoF and the answer given to that CBPII.

As part of enabling this, ASPSPs **must** provide PSUs with a facility to view and revoke CoF access that they have given to any CBPII for each account held at that ASPSP. This section describes how CBPII CoF access should be displayed, including CoF access history and how the customer journey to revoke them should be constructed.

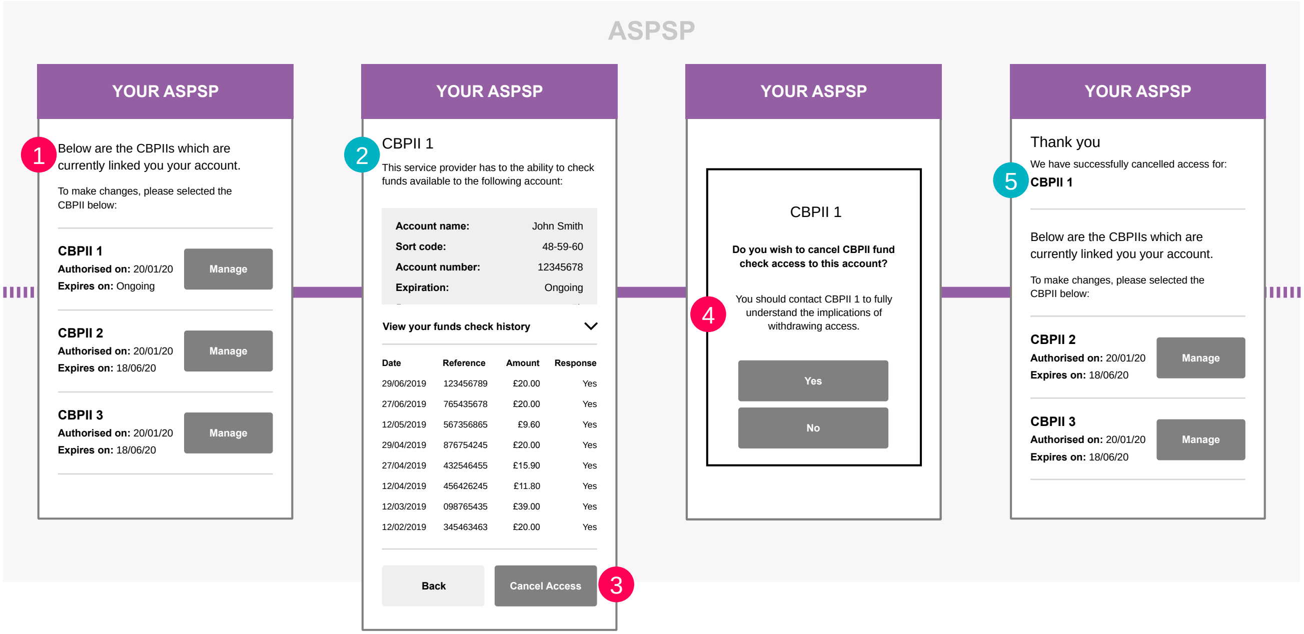
Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

5.1.2 Access Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations



ASPSP

YOUR ASPSP

1 Below are the CBPIIs which are currently linked you your account.

To make changes, please selected the CBPII below:

CBPII 1
Authorised on: 20/01/20
Expires on: Ongoing
Manage

CBPII 2
Authorised on: 20/01/20
Expires on: 18/06/20
Manage

CBPII 3
Authorised on: 20/01/20
Expires on: 18/06/20
Manage

YOUR ASPSP

2 CBPII 1

This service provider has to the ability to check funds available to the following account:

Account name:	John Smith
Sort code:	48-59-60
Account number:	12345678
Expiration:	Ongoing

View your funds check history

Date	Reference	Amount	Response
29/06/2019	123456789	£20.00	Yes
27/06/2019	765435678	£20.00	Yes
12/05/2019	567356865	£9.60	Yes
29/04/2019	876754245	£20.00	Yes
27/04/2019	432546455	£15.90	Yes
12/04/2019	456426245	£11.80	Yes
12/03/2019	098765435	£39.00	Yes
12/02/2019	345463463	£20.00	Yes

Back | Cancel Access 3

YOUR ASPSP

CBPII 1

Do you wish to cancel CBPII fund check access to this account?

4 You should contact CBPII 1 to fully understand the implications of withdrawing access.

Yes

No

YOUR ASPSP

Thank you

We have successfully cancelled access for:
5 **CBPII 1**

Below are the CBPIIs which are currently linked you your account.

To make changes, please selected the CBPII below:

CBPII 2
Authorised on: 20/01/20
Expires on: 18/06/20
Manage

CBPII 3
Authorised on: 20/01/20
Expires on: 18/06/20
Manage

What the research says

Research indicates that PSUs want to be able to review 'Confirmation of Funds'(CoF) consents via a dashboard at their ASPSP.

> See more

5.1.2 Access Dashboard & Revocation

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Access Dashboard** ASPSPs **must** provide PSUs with Access Dashboard. The ASPSP Access Dashboard **must** display all Confirmation of Funds access authorisations provided to each CBPII. Thus, for each PSU account there **must** be a corresponding explicit consent entry for each CBPII that has been granted CoF access to the account by the PSU. The Access Dashboard **must** also describe for each authorisation: • The status of the authorisation e.g. Active/Inactive • The ongoing nature of the access or when the CBPII access to the account will expire • The date the CoF access was granted by the PSU	P2 and P15 of Agreed Arrangements	10	ASPSP	Required
3	ASPSPS **must** allow PSUs to revoke the CoF access for each CBPII to a specific PSU account	P2 and P15 of Agreed Arrangements	10	ASPSP	Required
4	**Revocation Request** ASPSPs **must** allow PSUs to confirm that they want to revoke CoF access of their account to a specific CBPII. ASPSPs **should** inform PSUs that once CoF access is revoked, the CBPII will no longer be able to check the availability of funds in their account. This may cause their CBPII transactions to be declined. ASPSPs **should** also inform PSUs that they should contact the associated CBPII whose access has been revoked to inform them of the cancellation of CoF access to their account and/or fully understand the potential implications of doing so. ASPSPs **should** give equal prominence to the choices of continuing or cancelling the CBPII CoF access.	P2 and P15 of Agreed Arrangements	10	ASPSP	Required

	CX Considerations
2	**CoF Access History** For each CBPII having CoF access, ASPSPs **should** display the PSUs account details including account name, sort code, account number and expiration date and time. ASPSPs **must** also provide PSUs the ability to request all the CoF access history (CoF requests and responses) under a specific CBPII. This **must** include the identity of the CBPII who made the request, and the response (Y/N) given. The history **could** also include the following: • the date the Confirmation of Funds request has been received by the ASPSP • the unique reference of the CoF request • the amount in relation on the CoF request *Please note that in case ASPSPs are unable to provide a response to a CoF request to the CBPII, a reason **should** be provided in the history entry for this CoF request.*
5	ASPSPs **should** confirm to PSUs that CoF access to their account has been cancelled.

PSU Research Considerations

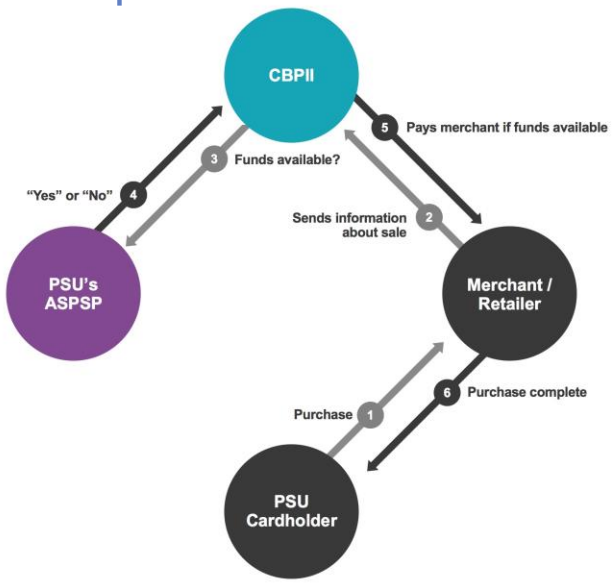
Research undertaken on behalf of OBIE with consumer PSUs has identified the following points:

- PSUs want to see the history of all the CoF requests and the response their ASPSP provided back to the CBPII.
- PSUs expect to see the details of CoF request to their ASPSP such as the date & time the request was received, the transaction reference, the CBPII, the account checked and the response by their ASPSP to the requesting CBPII
- PSUs would want to be able to view the expiration date of the CoF consent through the ASPSP dashboard or through the CBPII website or app
- PSUs want to be able to revoke their CoF consent from the ASPSP dashboard. This is the instinctive place to revoke such consents.

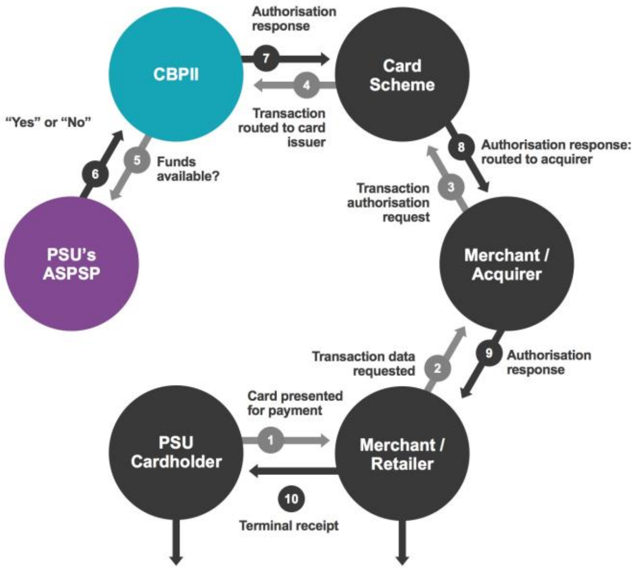
5.1.3 Confirmation of Funds - Y/N Response

User Journey | CEG Checklist Requirements | CX Considerations

Closed Loop



Open Loop



Payments networks primarily operate under two different business models that can apply to CBPIIs.

1. Open-loop payments networks, such as Visa and MasterCard that are multi-party and operate through a scheme that connects two financial institutions.
2. Closed-loop networks which issue cards directly to consumers and serve merchants directly.

As per PSD2 regulations, any authorised PSP, be it a bank or a payment institution, can issue payment instruments. Payment instruments not only cover payment cards such as debit and credit cards, but any personalised device or set of rules agreed between the issuer and the user that is used to initiate a payment.

The above diagrams illustrate at a high level the usage of the CoF by CBPIIs in both Closed and Open Loop operational models. Note that there is no PSU journey and this happens in the background.

Relevant Customer Insight and supporting regulation

> View CX Customer Research

> View CEG Checklist

5.1.3 Confirmation of Funds - Y/N Response

User Journey | CEG Checklist Requirements | CX Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
A	**Confirmation of Funds Response** In response to the CoF request, the ASPSP **must** provide a Yes/No Answer as a CoF response. This **must** include: • a Yes/No response that funds in the funding payment account checked are sufficient to cover a transaction of the specified amount. • a unique CoF response identifier. This is unique within the ASPSPs environment. A CBPII has no real use for this identifier however it is provided in order to have the ability of a full trace for audit purposes. • This **could** also include the date and time the CoF response was created.	PSR. Reg 68(4) RTS Art. 36(1)(c) RTS, Art. 35(4)(c)	33	ASPSP	Mandatory

5.1.3 Confirmation of Funds - Y/N Response

User Journey | CEG Checklist Requirements | **CX Considerations**

CX and other processing requirements	
B	**Confirmation of Funds (CoF) - BAU operation** After PSUs provide their consent for CoF access to CBPIIs, PSUs are no longer required to be involved in the CoF request and response process. As part of the ASPSP consent process, ASPSPs **must** create a long lived consent and provide to CBPIIs a unique identifier of the consent. Every subsequent CoF request falling within this consent, **must** be made using this consent identifier.
C	**Confirmation of Funds Request** Every time PSUs initiate a transaction using the CBPII issued card, CBPIIs **could** choose to make a CoF request to ASPSPs holding the PSU's funding account. The CoF request **must** include: • the identifier of the consent that the customer has previously confirmed • the transaction amount and currency to which the CoF request pertains • a unique reference for the CoF request assigned by the CBPII. This is a reference provided by the CBPII and **should** relate to the ID of the transaction initiated by the PSU using the CBPII issued payment instrument.
D	**Notifications to PSUs** As stated above, PSUs are not involved in the CoF Request/Response process at all. PSUs may not even be aware that every time they are initiating a transaction using the CBPII issued instrument (e.g. card) the above process takes place. In addition, if PSU transactions at the POS fail due to confirmation of funds failure, PSUs may not be aware that this was the reason for the transaction failure. Thus, OBIE recommends the following based on undertaken PSU research: • Every time a CoF request for a transaction results in a negative response by ASPSPs, ASPSPs should notify PSUs that a funds availability check has responded as such. This notification could take place through various means such as SMS, mobile notification through the mobile banking app, email, automated voice call etc. The notification **could** be switched off upon PSU request. • Alternately, CBPIIs **could** also decide to notify PSUs in case of negative CoF response in order to allow PSUs to take any corrective actions such as funding the account immediately and retrying the failed transaction or use another funding account for their card based instrument. • ASPSPs **could** also choose to notify their customers on every occasion of a CoF request by a CBPII and not only upon a negative response. This will allow PSUs to identify any CoF requests that may not genuinely be related to a specific CBPII instrument transaction initiated by them. However, customer research indicates that PSUs do not consider necessary/important notifications on every CoF requests. • In case ASPSPs are unable to provide responses to CoF requests back to CBPIIs, it is recommended that ASPSPs **should** send notifications to PSUs about this failure, including a reason for not being able to provide responses back to CBPIIs.
E	**CoF Request/Response Processing Considerations** • When ASPSPs receive CoF requests, ASPSP **must** immediately provide a yes or no answer on the availability of the amount necessary for the execution of the card-based payment transaction. As per the FCA approach document (paragraph 17.22) 'immediately' in this context to mean that the response should be sufficiently fast so as not to cause any material delay in the payment transaction, and therefore this is likely to mean the answer **must** be provided as soon as the request is received. • CBPIIs **should** be able to make multiple CoF requests for different transactions simultaneously to ASPSPs (provided the relevant consents have been granted). However, every CoF request must only be made where the payer has initiated a payment transaction for the corresponding amount. • CBPIIs **should** be able to send multiple CoF requests for multiple accounts without having to have first received a response from any previous CoF request message. • ASPSPs **should** be able to cope with multiple CoF requests from the same CBPII for PSUs transactions initiated at the same time. • PSUs may decide to link the same ASPSP account with multiple issued payment instruments (e.g. cards) from multiple CBPIIs. This means that there may be multiple consents for CoF requests to the same account for multiple CBPIIs. In this case, the ASPSPs **should** be able to cope with CoF requests from multiple CBPIIs for transactions initiated at the same time.
F	• ASPSPs **should** allow a CBPII request for confirmation of funds even if the identifier, used by the PSU with the CBPII as part of the original consent, is no longer valid where that identifier is not an account number and/or sort code (e.g. expired/reported lost stolen primary/secondary PAN).

PSU Research Considerations

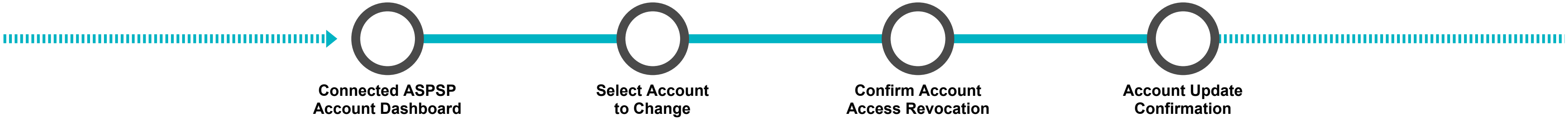
Research undertaken on behalf of OBIE with consumer PSUs has identified the following points:

- CoF is seen as a minor part of the payment process, and it is the confirmation of payments themselves that are the priority for PSUs. However, PSUs would like to know if a CoF request has resulted in a negative response / technical failure, or if there has been any suspicious activity e.g. multiple CoF requests at different amounts.

5.1.4 Revocation of Consent

User Journey | Wireframes | Requirements and Considerations

CBPII


Connected ASPSP Account Dashboard
Select Account to Change
Confirm Account Access Revocation
Account Update Confirmation

CBPIIs **must** provide PSUs with a facility to view and revoke consents that they have given to that CBPII. PSUs may have consented to CoF access to several accounts from one or more ASPSPs.

This section describes how these consents should be displayed and how the customer journey to revoke them should be constructed.

Relevant Customer Insight and supporting regulation

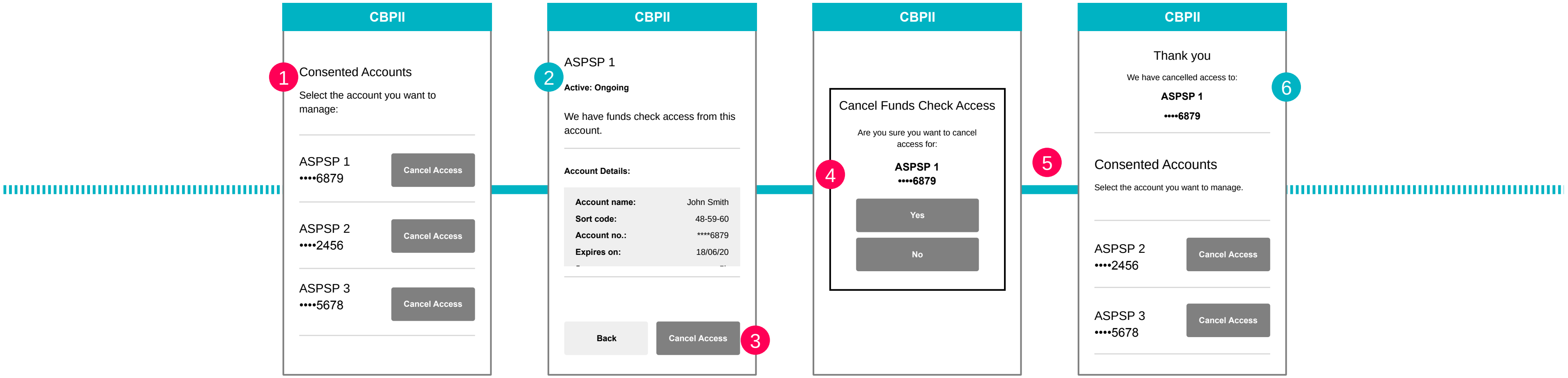
> View CX Customer Research

> View CEG Checklist

5.1.4 Revocation of Consent

User Journey | **Wireframes** | Requirements and Considerations

CBPII



CBPII

1 Consented Accounts

Select the account you want to manage:

ASPSP 1 ••••6879	Cancel Access
ASPSP 2 ••••2456	Cancel Access
ASPSP 3 ••••5678	Cancel Access

CBPII

2 ASPSP 1

Active: Ongoing

We have funds check access from this account.

Account Details:

Account name:	John Smith
Sort code:	48-59-60
Account no.:	****6879
Expires on:	18/06/20

Back | Cancel Access 3

CBPII

4 Cancel Funds Check Access

Are you sure you want to cancel access for:

ASPSP 1

••••6879

Yes

No

5

CBPII

Thank you

We have cancelled access to:

ASPSP 1

••••6879 6

Consented Accounts

Select the account you want to manage.

ASPSP 2 ••••2456	Cancel Access
ASPSP 3 ••••5678	Cancel Access

5.1.4 Revocation of Consent

User Journey | Wireframes | Requirements and Considerations

	CEG Checklist Requirements	Regulatory Reference	CEG Checklist Reference	Participant	Implementation Requirements
1	**Consent Dashboard** The CBPII Consent Dashboard **must** display all Confirmation of Funds access consents provided to the CBPII. Thus, for each PSU account, there **must** be a consent entry granting CoF access to the account for CoF purposes by the PSU. The Consent Dashboard **should** also describe for each consent: • The ASPSP • The ongoing nature of the consent and when the consent for CoF access to the account will expire • The date the CoF consent was granted by the PSU • In addition, the CBPII Consent Dashboard **could** also include details on the purpose for which the funds checks is used (including whether any other parties will have access to the information) and clear and reassuring messages about what information is made available from the ASPSPs, as per the examples described in 5.1.1, item #2.	P2 and P15 of Agreed Arrangements	9	CBPII	Required
3	CBPIIs **must** allow PSUs to revoke the CoF consent for each specific ASPSP account	P2 and P15 of Agreed Arrangements	9	CBPII	Required
4	**Cancellation Request** CBPIIs **must** allow PSUs to confirm that they want to cancel CoF consent of their account to the CBPII. CBPIIs **should** inform PSUs that once CoF consent is revoked, the CBPII will no longer be able to check the availability of funds in their account. CBPIIs **should** inform PSUs of the exact consequences of cancelling their consent, for example it may cause their CBPII transactions to be declined or they will no longer be able to receive the specific services from the CBPIIs etc CBPIIs **should** give equal prominence to the choices of continuing or cancelling the CBPII CoF consent	P2 and P15 of Agreed Arrangements	9	CBPII	Required
5	CBPIIs **must** inform ASPSPs that PSUs have withdrawn their consent by making call to the DELETE API endpoint (as described in Release 3 of the Read/Write API specifications). This will ensure that no further CoF account access will be accepted by ASPSPs. ASPSPs **must** support the Delete process as described in the Release 3 Read/Write API specifications. *Note: This activity is not visible to PSUs as it takes place in the background, however it will ensure no further CoF responses are provided by ASPSPs to CBPIIs)*	- P2 and P15 of Agreed Arrangements	9	CBPII ASPSP	Required

	CX Requirements
2	For each ASPSP account granted CoF access, CBPIIs **should** display the PSU payment account identification (such as account name, sort code and account number) and expiration date and time. *Note: PSU account number should be masked*
6	**CBPII Confirmation** CBPIIs **should** confirm to PSUs that CoF consent to their account has been cancelled.

PSU Research Considerations

Research undertaken on behalf of OBIE with consumer PSUs has identified the following points:

- PSUs would want to be able to view the expiration date of the CoF consent through the ASPSP dashboard or through the CBPII website or app
- PSUs also want to be able to revoke their CoF consent from the CBPII website or app. This could be especially convenient if there are several ASPSPs involved – they can do it all in one place, rather than have to log-in to several systems

6.0 The Customer Experience Checklist

The Customer Experience Guidelines Checklist ("the CEG Checklist") will serve as an essential tool that will enable Participants to certify against key criteria identified in the Customer Experience Guidelines, by answering specific questions used to demonstrate the Participant’s conformance to the Guidelines.

For ASPSPs in particular, this certification tool will assist in the process of applying for the contingency mechanism exemption, by serving as an integral component in showing how Open Banking Standard Implementation Requirements are appropriately met. The CEG Checklist will also be useful in aiding Participants to identify deviations from the Open Banking Standard Implementation Requirements, as contemplated by Guideline 6 of the EBA’s Draft Guidelines on the conditions to be met to benefit from an exemption from contingency measures. Of course, the views of OBIE in relation to non-CMA Order matters are indicative only and the final decision on an exemption is a matter for individual ASPSPs and their NCA. Additionally, we would note that the CEG Checklist is subject to change in the future depending on market and regulatory developments; in particular, we reserve the right to edit the CEG Checklist following the completion of the EBA consultation on their guidelines for granting an exemption from the contingency mechanism.

The CEG Checklist has been developed in parallel with the Customer Experience Guidelines, and for each customer journey that is detailed in the Guidelines, the relevant CEG Checklist criteria and questions have been highlighted. Items on the CEG Checklist are marked as Mandatory and Conditional and references are made to the relevant rationale of the CEG Checklist item, whether CMA Order, PSD2/RTS (including the recent EBA Opinion and the Draft Guidelines) or the Open Banking Standard Implementation Requirements.

We would note that while non-CMA9 ASPSPs are not required to comply with the CMA Order, it is at the discretion of Open Banking to define the Open Banking Standard Implementation Requirements and any item marked "required" is compulsory for successful certification. We note that non-CMA9 ASPSPs may choose not to comply with some or any of the Open Banking Standard Implementation Requirements, but it is expected that any deviations would need to be explained to the relevant competent authority as per the current EBA guidelines, where that ASPSP is seeking the contingency mechanism exemption. Similarly, TPPs have no legal responsibility to conform to the CEG Checklist and, assuming they meet their regulatory requirements, may adopt the Open Banking Standards and use the Directory without meeting items marked as “required”. However, they would not then meet the Standard Implementation Requirements and therefore not certify as meeting the Open Banking Standard.

Participants will be invited to submit videos of their customer journeys demonstrating their conformance with the CEG Checklist, and each submission will be assessed by the OBIE. For CMA9 ASPSPs, these videos will assist the Trustee in confirming to the CMA that the CMA remedies are being met. The OBIE Monitoring Function is due to be operational by 31st October 2018 under the Office of the Trustee.

6.1 Explanation of the Customer Experience Guidelines Checklist

The CEG Checklist is ultimately intended to drive certain behaviours and functionality in the ecosystem in order to:

- Deliver excellent customer experiences that are simple and secure
- Promote innovation
- Ultimately, encourage adoption of Open Banking by both TPPs and consumers

This includes ensuring that:

- Any supplementary information that is ancillary to the journey provides clear customer benefit
- ASPSPs are able to demonstrate that their implementations “do not give rise to unnecessary delay, friction or any other attributes that would mean that PSUs are directly or indirectly dissuaded from using the services of PISPs, AISPs and CBPIIs"
- ASPSPs provide the full level of functionality available to PSUs available through the direct online channel irrespective of the TPP channel and authentication method

It should be noted that for the CMA9 – and any other ASPSP that adopts the Open Banking standard – it is expected that a completed CEG Checklist is submitted at least for a.) each dedicated interface, and b.) each brand and segment (Personal Current Accounts and Business Current Accounts). We note that brands may have the same implementations and dedicated interfaces, which means the same CEG Checklist can be submitted. Further, we encourage those completing the CEG Checklist to consider if any further submissions may be appropriate, for example if an ASPSP has "app-only" customers, where having a consolidated CEG Checklist could lead to different answers being provided. Each CEG Checklist submission should be signed off by the relevant business owner.

The CEG Checklist is not intended to be a check on technical functionality or technical performance. The CEG Checklist relates to the Customer Experience Guidelines only.

In developing the CEG Checklist questions, we have defined some key principles that each question must adhere to:

- OBJECTIVE – be fact based and not rely upon the judgement of the ASPSP or TPP
- CLEAR – standalone, single clause, closed questions which demand a “yes or no” answer
- DEFINED – unambiguous and tightly constructed with links to definitions where appropriate
- TRACEABLE – based on regulatory requirements and/or the OB Standard Implementation Requirements (rationale for inclusion and classification will be made explicit)

The usual governance process as followed for development of the Evaluations and Proposition papers or changes to the Open Banking Standards will be followed in order to sign off this CEG Checklist, culminating in the Customer Experience Guidelines (including the CEG Checklist) being taken for sign-off at Implementation Entity Steering Group (IESG). Future changes to the CEG Checklist will accompany future releases of the Open Banking Standards.

6.2 Customer Experience Guidelines Checklist

Definitions:

The following terms are used in the column marked Open Banking Implementation Requirements:

Required – Participants **must** respond in accordance with the specified response in the 'Notes' column for successful conformance with Open Standard Implementation Requirements.

Recommended – Participants **should** respond in accordance with the specified response in the 'Notes' column to enable the desired customer outcomes described in the Customer Experience Guidelines, however, this may not be required for successful conformance with Open Standard Implementation Requirements.

The following terms are used in the columns marked CMA Order and PSD2/RTS:

Mandatory - Required in all cases for regulatory compliance and/or to deliver essential customer outcome

Conditional - Required if these are made available to the PSU in the ASPSP's existing Online Channel

n/a - not applicable

General

Reference	Topic	Participant (TPP, ASPSP)	Checklist question	Notes	Open Banking Implementation Requirements	CMA Order	PSD2 / RTS	Regulatory reference(s)
1.	Authentication	ASPSP	Is your Open Banking authentication journey equivalent to the journey experienced by a PSU when authenticating directly within your existing online channel(s) (e.g. browser and app)?	Answer must be "Yes"	Required	Mandatory	Mandatory	• Trustee P3/P4 letter Actions P3 A2 and P3 A6 • EBA Draft Guideline 5.2 (d)
2.		ASPSP	At any point during the Open Banking customer journey, do you ask the PSU for consent for the TPP to access account information or initiate a payment?	Answer must be "No"	Required	Mandatory	Mandatory	• EBA Opinion paragraph 13 • EBA Draft Guideline 5.2 (c) and paragraph 34 (c) • RTS Art. 32(3) • FCA Approach Document paragraph 17.48
3.		ASPSP	Can a PSU identify your firm as genuine and legitimate within the authentication journey?	Answer should be "Yes"	Recommended	n/a	n/a	• Consumer priorities
4.		ASPSP	Can a PSU authenticate using all channels (e.g. browser, app) offered by the ASPSP for authentication, irrespective of the channel via which the TPP is presenting their service?	Answer should be "Yes"	Recommended	n/a	Conditional	• EBA Draft Guideline 5.1(b) • EBA Opinion paragraph 50
5a.		ASPSP	Do you support app-to-app redirection?	Answer must be "Yes“ for CMA9, and should be “Yes” for other ASPSPs	Required	Mandatory	Conditional	• EBA Draft Guideline 5.1(b) • EBA Opinion paragraph 50 • Trustee P3/P4 letter Action P3 A6
5b.		TPP	If your proposition includes a mobile app, do you support app-to-app redirection?	Answer should be "Yes"	Recommended	n/a	n/a	• n/a
6.		ASPSP	Do you support Decoupled authentication?	Answer could be "Yes"	Recommended	n/a	Conditional	• EBA Opinion paragraph 50 • Trustee P3/P4 letter Action P4 A2
7.	Error codes	ASPSP	Do you provide error codes to the TPP as per the error codes specified in the Read/Write Data API Specification v3.0 for failed requests?	Answer must be "Yes"	Required	Mandatory	Mandatory	• RTS Art. 36(2) • EBA Opinion Table 1
8.	Consent	TPP	Do you gather consent in a clear, specific and straightforward manner as per the principles described in Sections 3.1.1 (AIS), 4.1.1 (PIS) and 5.1.1 (CBPII) of the Customer Experience Guidelines?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Regs. 68(3)(a), 69(2) and 70(3)(a) • FCA Approach Document paragraphs 17.46 and 17.47
9.	Consent dashboard	TPP	Can a PSU view and revoke on-going consent in a Consent Dashboard (as per Sections 3.1.3 and 5.1.4 of the Customer Experience Guidelines)?	Answer must be "Yes"	Required	n/a	n/a	• P2 and P15 of Agreed Arrangements
10.	Access dashboards	ASPSP	Do you make available an access dashboard which allows PSUs to view and revoke TPP access which has been previously granted (as per Section 3.1.4 of the Customer Experience Guidelines)?	Answer must be "Yes"	Required	Mandatory	n/a	• P2 and P15 of Agreed Arrangements
11.	Complaints	Both	Do you provide an easy way for the PSU to understand the complaints and dispute resolution process?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Reg. 101

6.2 Customer Experience Guidelines Checklist continued

Account Information Services

Reference	Topic	Participant (TPP, ASPSP)	Checklist question	Notes	Open Banking Implementation Requirements	CMA Order	PSD2 / RTS	Regulatory reference(s)
12.	Consent	AISP	Do you make it clear when the consent to access account information will expire (including if it is one-off access or ongoing access)?	Answer must be "Yes"	Required	n/a	n/a	• FCA Approach Document paragraph 17.46
13a.	Data clusters	ASPSP	Do you use the OBIE language shown under the Customer Experience Guidelines Section 3.2.3 to describe the data clusters when communicating with the PSU?	Answer must be "Yes"	Required	Mandatory	n/a	• CMA Order 10.2
13b.		AISP	Do you use the OBIE language shown under the Customer Experience Guidelines Section 3.2.3 to describe the data clusters when communicating with the PSU?	Answer must be "Yes"	Required	n/a	n/a	• n/a
14.	Functionality	ASPSP	Do you provide access to all account information made available to the PSU through your existing online channel(s), irrespective of the channel through which the TPP is presenting their service to the PSU?	Answer must be "Yes"	Required	Mandatory	Mandatory	• RTS Art. 36(1)(a) • EBA Opinion paragraphs 18 and 20
15.		ASPSP	Do you apply the same access control rules to joint and multi-signatory accounts when accessed through a TPP as are applied when these accounts are accessed directly by the PSU?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Reg. 70(2)(b)
16.	Authenticating to refresh access	AISP	Do you notify the PSU when authentication is required to refresh AISP access at the ASPSP?	Answer should be "Yes" This could occur for example every 90 days where the ASPSP is applying the RTS Article 10 exemption	Recommended	n/a	n/a	• P2 and P15 of Agreed Arrangements
17.		ASPSP	When a PSU is authenticating to refresh AISP access without making any changes to the original consent request, does your journey include any steps or screens other than those required for authentication of the PSU, for example, re-selection of the account(s) to which access was originally granted?	Answer must be "No"	Required	n/a	Mandatory	• RTS Art. 33(2)
18.	Completion	AISP	Do you provide confirmation of a successful account information data request following each PSU authentication?	Answer must be "Yes" e.g. through a receipt or confirmation within TPP domain	Required	n/a	n/a	• n/a

6.2 Customer Experience Guidelines Checklist continued

Payment Initiation Services

Reference	Topic	Participant (TPP, ASPSP)	Checklist question	Notes	Open Banking Implementation Requirements	CMA Order	PSD2 / RTS	Regulatory reference(s)
19.	Functionality	ASPSP	For payments that do not require the display of supplementary information (as defined in the Customer Experience Guidelines 4.1.2) does your journey involve any further steps (as defined in the Customer Experience Guidelines 4.1.1) or screens following authentication?	Answer must be "No"	Required	Mandatory	Mandatory	• Trustee P3/P4 letter Action P3 A2 • RTS Art. 33(2)
20.		ASPSP	Do you provide supplementary information where it is required, in an equivalent way, to direct interactions with PSUs?	Answer must be "Yes"	Required	n/a	Mandatory	• EBA Draft Guideline 5.2(d)
21.		ASPSP	Can a PSU using a PISP utilise all PIS functionality offered by the ASPSP to the PSU in their online channel, irrespective of the channel or method used for authentication?	Answer must be "Yes"	Required	Mandatory	Mandatory	• EBA Draft Guidelines 2.3(c) • PSR Reg. 69(2)(c) • FCA Approach Document paragraphs 17.29 to 17.31
22.		PISP	Do you capture the minimum set of parameters required for the payment instruction to be completed for each payment type?	Answer must be "Yes" Minimum set of parameters are defined in the Section 4 of the Customer Experience Guidelines	Required	n/a	Mandatory	• RTS Art. 36(4)
23.		ASPSP	In cases where the payment instruction is incomplete because the account details have not been provided by the PSU to the PISP, do you allow the PSU to select the account from which they wish to make the payment?	Answer must be "Yes"	Required	Mandatory	n/a	• CMA Order 10.2
24.		PISP	Do you offer the PSU at least one of the available options for selecting the payment account during the payment initiation as defined in the Customer Experience Guidelines Section 4?	Answer must be "Yes" The available options for selecting an account are defined in Section 4 as: • enter their Account Identification details directly to the PISP • select their Account Identification details at the PISP (this assumes they have been saved previously) • select their ASPSP in order to select their account from within the ASPSP's domain later in the journey	Required	n/a	n/a	• n/a

6.2 Customer Experience Guidelines Checklist continued

Payment Initiation Services continued

Reference	Topic	Participant (TPP, ASPSP)	Checklist question	Notes	Open Banking Implementation Requirements	CMA Order	PSD2 / RTS	Regulatory reference(s)
25.	Status of payment	ASPSP	Do you provide or make available all information regarding initiation and execution of the payment to the PISP immediately after receipt of the payment order?	Answer must be "Yes"	Required	Mandatory	Mandatory	• PSR Reg. 69(2)(b) • RTS Art. 36(1)(b) • FCA Approach Document paragraphs 17.23 – 17.24
26.		PISP	Do you display all the required information to the PSU immediately after the initiation of the payment order?	Answer must be "Yes" Types of information are defined in Section 4.1	Required	n/a	Mandatory	• PSR Reg. 44(1)
27.		PISP	After receiving the initial payment status information, do you follow up with the ASPSP in order to get the latest status of the payment and inform the PSU accordingly?	Answer should be "Yes"	Recommended	n/a	n/a	• n/a
28.	Display of payment details	ASPSP	Do you make the PSU aware of the amount/currency/payee as part of the authentication journey?	Answer must be "Yes", unless an SCA exemption is being applied	Required	n/a	Conditional	• RTS Art. 5(1)(a)
29.	Confirmation of funds ("yes/no" response)*	ASPSP	Do you provide immediate confirmation of whether or not there are funds available at the PISP's request, in a 'yes or no' format?	Answer must be "Yes" See asterix (*) below table	Required	n/a	Mandatory	• RTS Art. 36(1)(c) • EBA Opinion paragraph 22
30.	Future Dated Payments & Standing Orders	PISP	Do you inform the PSU that amendment or cancellation of standing orders and future dated payments must be performed directly with their ASPSP?	Answer must be "Yes"	Required	n/a	n/a	

CBPII

Reference	Topic	Participant (TPP, ASPSP)	Checklist question	Notes	Open Banking Implementation Requirements	CMA Order	PSD2 / RTS	Regulatory reference(s)
31.	Explicit consent	ASPSP	Do you, prior to receiving the first request from each CBPII, obtain explicit consent from the PSU to provide confirmation of funds in response to CBPII requests (as shown under the Customer Experience Guidelines Section 5)?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Reg. 68(5)(b) • FCA Approach Document paragraph 17.18
32.	Explicit consent	CBPII	Do you obtain explicit consent from the customer to request the confirmation of funds?	Answer must be "Yes" Minimum set of parameters are defined in the Section 5 of the Customer Experience Guidelines	Required	n/a	Mandatory	• PSR Reg. 68(3)(a)
33.	Functionality	CBPIII	Do you only request confirmation of funds when the PSU has initiated a payment transaction for the amount in question using the card based instrument?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Reg. 68(3)(b)
34.	Confirmation of funds ("yes/no" response)	ASPSP	Do you provide immediate confirmation of funds in the form of a 'yes' or 'no' answer to a CBPII request where the payment account is accessible online?	Answer must be "Yes"	Required	n/a	Mandatory	• PSR Reg. 68(4) • RTS Art. 36(1)(c) • EBA Opinion paragraph 22

Note: CMA Order includes the Trustee's P3/P4 Evaluation letter and PSD2 / RTS includes the EBA Opinion and (draft) Exemption Guidelines

* The Release 3.0 candidate does not include provision of this for PISPs, however, the FCA are clear on the requirement for this and the current plan is to deliver this as part of Release 3.1. For this reason we have included this item in the Checklist.

6.2.1 Examples and additional detail for CEG Checklist questions

Ref	Topic
1	**Equivalence covers a range of topics including:** • functionality • access rights (if a joint account holder can access all account information or initiate payments without any action on the part of the other account holder directly with the ASPSP, then this functionality should be available when using a TPP) • authentication methods (and the order in which they are presented) • the process covering mistakes when inputting an authentication element (e.g. typo of a password) • length of journey / number of steps (this means that having to manually open a browser or an app must be avoided as that is not required in a direct experience, except for the generation of a code on a mobile app) • visual display including branding, imaging, fonts and text formatting • version control and equivalence for authentication i.e. authentication works with all available versions of the app For clarity, the experience should match the associated channel e.g. if biometric can be used on an app, then this should be available to the PSU when a TPP is involved
2	**Additional checks of consent** While an ASPSP may provide additional information and clarification throughout the journey, at no stage should the ASPSP seek to reconfirm or check that the PSU wants the TPP to perform the activity they have consented to. For example, language such as "Are you sure you want to grant access to TPP..." or "TPP has asked us to initiate a payment, please confirm you are happy with this..." should be avoided, Further explanation and clarification of this point is found throughout the Customer Experience Guidelines journeys.
3	**Identifying your firm as genuine** For example have personalised greetings during authentication so that someone knows they are authenticating with their own ASPSP and not a fake
5a	**App-to-app redirection** As provided in the P3/P4 Evaluation letter, the OBIE definition of App-to-App is: 'App-to-App' redirection allows the TPP to redirect a PSU from the TPP application (in a mobile web browser or mobile app) to the ASPSP's mobile app, installed on the PSU's device, where the TPP is able to transmit details of the request along with PSU preferences (e.g. product type, one-step authentication) and deep link the PSU into the ASPSP app login screen or function. The PSU is then authenticated through their app using the same credentials/methods as normally used when the PSU directly accesses their account using the app (typically biometric). This must not involve any additional steps (such as being redirected first to a web page to select which ASPSP app to use) and must not require the PSU to provide any PSU identifier or other credentials to the ASPSP if their current ASPSP app does not require this. Where the PSU does not have the ASPSP's mobile app, they should experience a redirection flow which should not involve additional steps than would be the case when the PSU authenticates with the ASPSP directly (e.g. be redirected to the ASPSP's mobile website).
7	**Error Codes:** ASPSPs must provide TPPs with the error codes included in the Read/Write API specification for failed requests (see Appendix 7.6). TPPs should then use the error code provided to determine the content of the message displayed to the PSU. This message should describe, in user-friendly language, what has gone wrong and what the PSU should do next. (OBIE will carry out research into effective PSU error/failure messaging from the TPP and include the output in the next revision of these guidelines).
8	**Consent** PSUs must be able to understand the nature of the service being provided to them, and the consent should be clear and specific
14	**Functionality – account information** Note this refers to account information as defined in the PSRs. Please consult Section 3.2.4 for clarity around "Optional Data" (e.g."Party data")
15	**Functionality – joint accounts** If a joint account holder can access all account information without any action on the part of the other account holder directly with the ASPSP, then this functionality should be available when using an AISP.
17	**Authenticating to refresh access** There an example in Section 3.1.2 that clarifies this - In this example nothing in the consent request has changed (e.g. the PSU gave consent for account information to be shared for the payment account and wishes the TPP to continue to have access to the account) If the PSU has an opportunity to reselect or change the consent request and accounts being shared, this requires a full end to end journey as per the initial consent journey including account selection as in 3.1.1. The point of this question is to ensure that the journey in 3.1.2 is shorter than that in 3.1.1.

6.2.1 Examples and additional detail for CEG Checklist questions

Ref	Topic
19 & 20	**Supplementary Information:** ASPSPs **should** determine the situations where Supplementary Information is required to be shown to the PSU, having regard to the principle that parity should be maintained between Open Banking journeys and ASPSP direct online channel journeys. Supplementary Information may be required: • Where fees and charges apply (e.g. for single CHAPS payment) • Where interest rates apply • To facilitate confirmation of payee (for UK implementations, where ASPSPs applied COP validation and found inconsistency between payee account name • To display a PSU warning that the relevant payment account will become overdrawn / exceed an overdraft limit as a result of the intended payment • If the relevant payment submission cut-off time has elapsed and the ASPSP wishes to offer an execution date/time • Where the PSU has been identified by the ASPSPs as a vulnerable customer (who therefore receives tailored journeys and messages in ASPSP's own online platforms) • To show value-add information based on functionality implemented by ASPSPs in competitive space which provides positive customer outcome (e.g. cashflow prediction engine) • For high value transactions using a different payment scheme • Where the payments may be duplicated by the customer in a short period (e.g. ASPSP may display a warning that payment appears to be duplicated).
21.	**Functionality – payment initiation** For example, even if an international payment can only be made through a web browser when a PSU accesses the ASPSP directly, the PSU should be able to make an international payment via a PISP irrespective of authentication channel.
25.	**Functionality – payment status** This deals with the status of payment and more specifically, to meet the regulatory requirement as per PSR Reg. 69(2)(b). Currently, the "Payment Status End point" allows an ASPSP to provide the TPP with a status message regarding the payment initiation and payment execution (pending, rejected, or accepted) at the point in time, when the ASPSP receives the payment order from the PISP for execution.

7.0 Appendices

Appendices

7.1 Themes identified from consumer and SME research

7.1 Themes identified from consumer and SME research

The Open Banking Implementation Entity (OBIE) has undertaken considerable customer research over 18 months; this section draws out the themes and principles identified from this consumer and SME research. These are the principles that should be considered when establishing Open Banking Customer Journeys.

1. Trust

There is a natural tendency for consumers to feel unsure about, or even sceptical about, new ways of doing things. This is especially so when it comes to financial management and making financial transactions, areas where consumers tend to be inherently cautious. There is a recognition that the consequences of dealing with a company which is untrustworthy or experiencing the effects of a data breach can be severe for consumers.

The research reveals a clear link between the transparency of any new product or service and the willingness of potential users to trust it. With both consumers and SMEs trust can be earned around Open Banking enabled services if ASPSPs and TPPs are open and clear in explaining the steps in the process, what is happening throughout the journey, where consent needs to be given and in reassuring about security.

Consumers will be reassured by a clear consent process that explains what they are consenting to. A three-step process, involving the PSU giving consent to a TPP, authentication at ASPSP and a final step at the TPP that summarises the sharing of information or initiation of payment offers this clarity. More truncated processes can also provide reassurance but, with fewer steps, the need for absolute clarity of information presentation is increased.

Trust is essential in encouraging the use of AIS, but it is PIS journeys where it is most critical since the risk associated with potential loss of funds is more immediately recognised than the risks associated with loss of data. Review steps during a journey can help to build trust. This trust is equally important to individual consumers and SMEs. The research shows that, for both audiences, the larger the purchase, the greater the need for trust.

The research indicates that PSUs have a greater tendency to trust ASPSPs, with whom they will already have relationships relating to their finances, than TPPs. ASPSP processes are familiar, and they are known established brands. Many TPPs, especially those without an existing brand or presence in the market, will need to work harder to prove their trustworthiness with consumers. They need to ensure, in developing services and the communications that go with them, that they are at least as clear and transparent as ASPSPs. Using an ASPSPs logo, for example on redirection screens, will make consumers feel more trust in the process, and provide reassurance regarding authenticity.

Trust can also be built by using different and multiple channels for receipts, for example, SMS, email or letter, as well as within the PISP and ASPSP screens.

2. Security

Concerns about security were a consistent theme across all the research conducted. Consumers and SMEs recognise that there are risks inherent in sharing banking information and data. However, their understanding of the nature of such risks and what can be done to mitigate them is limited.

Concerns stem from uncertainty and focus on issues such as data sharing and privacy, fears about cybersecurity and fraud. Providing reassurance about the security of processes and journeys will be fundamental to the success of the Open Banking ecosystem.

The research shows that concerns about security tend to be expressed more strongly concerning PIS journeys. Security is vital for both consumers and SMEs, but it is especially critical for SMEs, due to the nature and scale of the transactions involved. SMEs are more likely to be making more payments of higher value, and their businesses may depend on these being made securely. There may also be reputation considerations involved.

There is a link between security and control, as being reassured about security gives PSUs a sense of being in control, which will increase their willingness to explore products, services and benefits available more fully.

There is also a link between security and ease. Consumers would prefer not to have to enter details manually but for details to be prepopulated or dropdown boxes provided. Not only is this easier for the consumer, but it also minimises the risk of them making errors.

Consumers want guarantees and protection to be built into Open Banking customer journeys. They tend to look to both ASPSPs and TPPs to provide this. However, they recognise that there could be a trade-off involved between the need for protection and potential offers, discounts or benefits, and may be willing to take more risk in some circumstances, particularly when making smaller transactions.

Consumers need security messages to be clear and well sign-posted, and they value confirmation and reconfirmation. Some customers also value the extra step involved in decoupled journeys.

Providing supplementary information plays a vital role in delivering reassurance and a sense of security for consumers. Consumers express concern if some journeys feel ‘too easy’. Consumers would feel more comfortable if, for example, the process of initiating more substantial payments had more positive friction within it than that for smaller transactions.

7.1 Themes identified from consumer and SME research

3. Speed

While supplementary information is welcome in some journeys, the research shows that, in general, consumer PSUs prefer shorter journeys. Those with too many steps or which appear too repetitive are likely to discourage adoption. Consumers recognise the potential trade-off between speed, clarity and security.

Open Banking journeys should feel smooth, with services easy for consumers to use, and with minimal scrolling, clicking and wait times. Consumers will also find journeys that feel familiar to be simpler to understand and navigate, allowing them to complete them more quickly and efficiently. New or unfamiliar journeys should feel seamless and intuitive, analogous to existing financial services journeys.

Many consumers find app-based journeys easier than web-based, due to less information being shown on screen, as well as the general high mobile usage and comfort amongst consumers, and the intuitive nature of a touchscreen.

4. Transparency

The research showed the need for transparency around Open Banking customer journeys. Consumer PSUs are reassured when they understand what is happening at each stage of the process and find that there is a logical flow to the steps within a journey. Transparency requires that the journey enables the consumer to comprehend what is happening, is clear about what they are agreeing to and find the process convenient. Transparency is also key to building trust, as discussed above.

Amongst the things that research indicates ASPSPs and TPPs can do to deliver transparency for PSUs are explaining things clearly, confirming payments and providing helpful information and prompts.

Key to delivering transparency is the way in which information is presented. The provision of technical information and extensive detail can sometimes undermine transparency. For example, some of the detail around international payment methods and FX, if not explained clearly, can lead PSUs to feel confused.

TPPs and ASPSPs should be clear as to why they require customers to share the information they are requesting. If the customer is transparent with their data, so the providers should be clear about what they will do with it. This sense of reciprocity will also help engender trust.

The research has shown that the language used to explain PIS and AIS services and the steps involved in the journeys needs to be consumer-friendly and not open to misinterpretation. Communication needs to be familiar, if possible, so consumers can identify what it is and link it to something they know, or may already use. Entirely new concepts should be explained in clear, plain English and with consistent use of terms, and minimal technical language/jargon.

5. Control

Throughout the research conducted for OBIE, the need for customers to feel in control, throughout an AIS or PIS journey, was a recurrent theme.

There are clear links between control, security and ease of use / navigability. Where customers trust the security, they feel in control. Where they can understand what is happening, they will feel a sense of control over the process.

Being able to review, check and confirm (positive friction) are all sources of control for consumers. Enabling revocation is also important. The knowledge that a decision can be reversed adds reassurance, particularly when doing something for the first time.

Control is also linked to transparency. If ASPSPs and TPPs are transparent, the PSU feels more in control. Dashboards also help consumers feel a sense of control. Dashboards provide consumers with evidence of activity and the ability to review in case of problems or issues.

7.2 CX Guidelines Consultation – Research Data

7.2 CX Guidelines Consultation – Research Data

S. No.	Journey Ref.	Research Findings	Theme
Ref. no.		Research evidence - what, who, why, and quantitative stats where available	
1	2.2.1	Research amongst consumers has shown that 29% of participants actively prefer a browser-based PIS journey for a single domestic payment, while 32% prefer an app based journey. Those preferring a browser-based journey refer to security and ease to explain their choice. Those preferring the app based alternative select it because they deem it easier than the web-based experience, with fewer mentioning security.	Security Speed Control
2	2.2.2	Research amongst consumers has shown that 29% of participants actively prefer a browser-based PIS journey for a single domestic payment, while 32% prefer an app based journey. Those preferring a browser-based journey refer to security and ease to explain their choice. Those preferring the app based alternative select it because they deem it easier than the web-based experience, with fewer mentioning security.	Security Speed Control
3	2.2.2	Consumer research has shown that people feel authentication via Fingerprint ID adds a reassuring sense of security to the journey.	Security
4	2.2.2	Research amongst consumers has shown that within a TPP domain in an app to app context, 45% of participants want to have a 'proceed' button to click after reviewing account information, to confirm payment and begin the biometric authentication process. They feel this is secure and gives them control.	Security Control
5	2.2.5	Research amongst consumers and SME PSUs has shown that the presence of the ASPSP's logo on the PISP to ASPSP redirection screen is important (70% and 74% respectively saying this) and that it makes them trust the process more (66% and 77%) respectively.	Trust Transparency
6	2.3.1	Research shows that consumers are familiar with decoupled authentication when making a payment or setting up a new payment. This means that, if PIS journey designs follow similar patterns, consumers will be comfortable with them. Many welcome the additional level of security decoupled authentication provides.	Security
7	2.3.2	Research shows that consumers are familiar with decoupled authentication when making a payment or setting up a new payment. This means that, if PIS journey designs follow similar patterns, consumers will be comfortable with them. Many welcome the additional level of security decoupled authentication provides.	Security
8	2.3.2	Consumer research has shown that although 62% of people feel having to generate a one-time code on a mobile app is 'annoying'.	Security
9	3.1.3	In addition, consumer research has shown that respondents prefer confirmation of a revocation in writing via email in addition to text on the website.	Trust Control
10	3.1.4	Consumer research has shown that people feel most confident that a revocation has been actioned when it is has taken place with an ASPSP. Their perception is that they are 'stopping' the information at 'source' rather than instructing a TPP not to 'take' the information.	Trust Control
11	3.2.2	Research amongst consumers has shown that utilising simple, familiar language enables consumers to understand the broad categories of account data that may be required by AISPs. 'Your Account Details', 'Your Regular Payments', 'Your Account Transactions' and 'Your Account Features and Benefits' (as opposed to '...Services') were all shown by research to offer appropriate levels of clarity.	Transparency

7.2 CX Guidelines Consultation – Research Data

S. No.	Journey Ref.	Research Findings	Theme
Ref. no.		**Research evidence - what, who, why, and quantitative stats where available**	
12	4.1.1	Research amongst consumers has shown that 64% of participants prefer to be shown confirmation that payment has been received at the TPP. This would provide reassurance that the process has worked.	Transparency
13	4.1.1	Research amongst consumers has shown that 26% of participants would prefer a payment process with a single summary step in one domain. They felt that it was the easiest method.	Speed
14	4.1.1	Research amongst consumers has shown that 37% of participants wish to select the account from which to make a payment within the TPP's domain. The reasons for this relate to the following conventions they are both used to and comfortable with. However, 32% of participants had no preference of how/where to select an account.	Security Speed
15	4.1.3	When account selection is done at the ASPSP, research amongst consumers has shown that 58% of participants prefer to be shown the balance for their selected payment account, before reviewing a payment. This was felt to assist in good personal financial management.	Control
16	4.1.4	Consumer research has shown that 82% of consumers would like to see the payment schedule at least once in the journey.	Trust
17	4.1.4	The term 'Pending', when employed in this context, is clear and understood by consumers.	Trust
18	4.1.4	Consumer research has shown that 73% of consumers prefer to see exactly when a payment will be taken.	Trust
19	4.1.4	Consumer research has shown that 64% of people would prefer to see a message at the top of the ASPSP page which states that the TPP cannot see the information here.	Security
20	4.1.5	Research amongst consumers has shown that they are not always able to differentiate between Standing Orders and Direct Debits. This means it is important to be clear about the details of a new payment arrangement when it is being set up.	Transparency Control
21	4.1.5	Consumer research has shown that 73% of consumers prefer to see exactly when a payment will be taken.	Trust
22	4.1.5	Research has shown that 63% of consumers and 75% of SMEs, feel 'ok' about having to go direct to their bank's website to amend a Standing Order.	Security
23	4.1.5	Research amongst consumers has shown that a 3 step process of Consent - Authentication - Summary Information step gives the customer an assurance they are engaging with their bank, creating confidence. This feeling comes from an impression that they have 'overseen' the entire set-up process.	Trust Security

7.2 CX Guidelines Consultation – Research Data

S. No.	Journey Ref.	Research Findings	Theme
Ref. no.		**Research evidence - what, who, why, and quantitative stats where available**	
24	4.1.5	Research amongst consumers has shown that they consider it important to be able to schedule a recurring payment to be paid on the same date every month. There is currently some frustration with providers who do not take payments on set dates but rather indicate a window when payment will be taken.	Control
25	4.1.5	Research amongst consumers has shown that the summary information step acts as a confirmation of exactly what they have consented to. This also creates a 'safety net' preventing inadvertent/unauthorised permissions and offers the opportunity for greater financial discipline due to the time afforded to review a standing order commitment.	Trust Security Control
26	4.1.6	Consumer research has shown that people find a recognisable ASPSP login page and process reassuring and increases their confidence in the journey.	Trust Security
27	4.1.6	Research has shown that consumers find it reassuring to receive confirmation of precisely what has been paid when they are returned to the PISP's page.	Trust
28	4.1.6	For international payments, consumer research indicates that people find it both appropriate and time saving to be able to choose which account to pay with and review the account balance once logged onto the ASPSP's domain.	Speed
29	4.1.6	Research indicates that consumers would like to see the final cost breakdown for an international payment at the TPP after payment has been authorised. This would provide transparency and reassurance.	Transparency
30	4.1.6	Both consumer and SME PSUs show a strong preference for the TPP/Merchant to prepopulate their details, as is 'less hassle' for them and reduces the risk of PSU error.	Speed Control
31	4.1.6	Consumer research shows that, while PSUs would prefer to see an actual FX rate, they generally accept an indicative rate.	Transparency Control
32	4.1.6	Research shows that SMEs want to know when the payee will receive a payment. They want to be able to select the execution date for the payment in the ASPSP's domain.	Speed
33	4.1.6	Consumer research shows that PSUs want to see the FX currency conversion rate and, ideally, the amount of the payment in £.	Transparency
34	4.1.6	Consumers wish to see the details of urgency (timings and/or method), charges and FX rates before consenting to international payments. Research shows they appreciate extra levels of detail, such as the expected date of the payment reaching its destination. Any additional information should be clearly explained.	Transparency
35	4.1.7	Research amongst SMEs has shown that those with experience of bulk/batch transfers have a clear understanding of issues such as cut-off times and the importance of accuracy in preparing batches of payments. There is a clear expectation that new processes (both at PISP and ASPSP) will be as closely analogous to existing methods as possible.	Transparency Control
36	4.1.7	Research amongst SMEs has shown that those with experience of bulk/batch transfers would value the facility to view the details of payments included in a bulk/batch file once it has been uploaded to their ASPSP.	Control

7.2 CX Guidelines Consultation – Research Data

S. No.	Journey Ref.	Research Findings	Theme
Ref. no.		**Research evidence - what, who, why, and quantitative stats where available**	
37	4.1.7	Research amongst SME PSUs indicates they would like to be able to select multiple payment accounts when setting up bulk/batch payments.	Control
38	4.1.7	Research indicates that SME PSUs value having a summary information step page as part of the bulk/batch payment process to act as a check, including a 'cancel' option to minimise the chance of errors.	Control
39	4.1.7	Research indicates that most SMEs would like the opportunity to check details at each stage of the bulk/batch payments journey, to minimise the risk of mistakes.	Control
40	4.2	Consumer research has shown that 80% of people would prefer a warning about breach of contract at the point before they confirm the consent revocation.	Transparency
41	5.1.1	Research has shown that consumers have no initial understanding of CBPIIs, or a Confirmation of Funds process, indicating that the process needs to be clearly explained during any journeys.	Trust Transparency
42	5.1.2	Research indicates that PSUs want to be able to review 'Confirmation of Funds'(CoF) consents via a dashboard at their ASPSP.	Transparency Control
43	5.1.3	Research indicates that PSUs do not wish to receive notifications of all requests, but would like to be informed of declined or failed requests with the reasons why these occurred.	Transparency Control
44	5.1.4	PSUs would like to be able to view the expiration date of their CoF consents through both the ASPSP dashboard and through the CBPII website or app. PSUs want to be able to revoke their consent from their ASPSP as this is the instinctive place to revoke such consents. They would also like the option to be able to revoke consent from their CBPII.	Trust Security

7.3 Deep Linking for App-to-App redirection

7.3 Deep Linking for App-to-App redirection

Problem statement

As provided in the P3/P4 Evaluation letter, the OBIE definition of App-to-App is:

'App-to-App' redirection allows the TPP to redirect a PSU from the TPP application (in a mobile web browser or mobile app) to the ASPSP's mobile app, installed on the PSU's device, where the TPP is able to transmit details of the request along with PSU preferences (e.g. product type, one-step authentication) and deep link the PSU into the ASPSP app login screen or function. The PSU is then authenticated through their app using the same credentials/methods as normally used when the PSU directly accesses their account using the app (typically biometric). This must not involve any additional steps (such as being redirected first to a web page to select which ASPSP app to use) and must not require the PSU to provide any PSU identifier or other credentials to the ASPSP if their current ASPSP app does not require this. Where the PSU does not have the ASPSP's mobile app, they should experience a redirection flow which should not involve additional steps than would be the case when the PSU authenticates with the ASPSP directly (e.g. be redirected to the ASPSP's mobile website).

There have been a number of technical and security challenges regarding the implementation of App-to-App. These are addressed below.

This document does not cover the standards nor implementation of de-coupled flows.

How the redirect flow works

When using a service based on the OBIE API standard for redirection, the PSU will be re-directed twice:

1. From the TPP interface to the ASPSP interface (to authenticate and authorise). The authorisation server URI is specified by each ASPSP in their .well-known endpoint.

2. Back from the ASPSP interface to the TPP interface (to complete any transaction with the TPP). This redirect is specified by the TPP as part of the first redirect.

Implementation of deep links

A seamless journey for the PSU, which bypasses the built in browser (e.g. Safari) on their mobile device, can be implemented for any URL, ie BOTH a) for the initial redirect which the TPP sends the PSU to on the ASPSP's servers, AND b) the redirect URL which the ASPSP sends the PSU back to after authentication/authorisation.

Both ASPSPs and TPPs should follow the guidance from Apple and Google below:

iOS: https://developer.apple.com/ios/universal-links/ (covers over 99% of all iOS users[1], who are on iOS 9 or greater).

Android: https://developer.android.com/training/app-links/index.html (covers 65% of all Android users[2], who are on Android 6.0 or later).

In the event that a PSU does not have the app installed on their device, or if they have an older (or non iOS/Android, e.g. Windows Mobile) operating system, these methods will allow the PSU to be re-directed to a mobile web page.

Open Banking Directory implications

In order to support multiple apps for a given brand (e.g. Brand X Personal App, Brand X Business App), ASPSPs will need to configure multiple 'virtual' .well-known configuration endpoints for each physical authorisation server listed on the Open Banking Directory. The Open Banking Directory will be updated to facilitate this functionality.

Security considerations

Security considerations are addressed here: https://tools.ietf.org/html/rfc8252.

You can find the most updated paper version of this here: Deep linking for App-to-App redirection

7.4 Payment Initiation Services (PIS) parameters and considerations

7.4 Payment Initiation Services (PIS) parameters and considerations

7.4.1 Domestic Standing Orders

Standing Order Frequency Examples
Every day
Every working day
Every week, on the 3rd day of the week
Every 2nd week, on the 3rd day of the week
Every month, on the 2nd week of the month, and on the 3rd day of the week
Every month, on the last day of the month
Every 6th month, on the 15th day of the month
Paid on the 25th March, 24th June, 29th September and 25th December

7.4.2 International Payments

7.4.2.1 Charge Models

Payments initiated by PISPs using Open Banking Write APIs, should be able to cover the following international payments charge models:

- **"SHARE" transfer:** The sender PSU of the payment will pay fees to the sending bank for the outgoing transfer charges. The receiver PSU will receive the amount transferred, minus the correspondent (intermediary) bank charges.
- **"OUR" transfer:** All fees will be charged to the sender PSU of the payment - i.e. the receiver PSU gets the full amount sent by the sender of the payment. Any charges applied by the receiving bank will be billed to the sender of the payment (usually sometime after sending the payment)
- **"BEN" transfer:** BEN (beneficiary) means that the sender PSU of the payments does not pay any charges.. The receiver PSU of the payment receives the payment minus all transfer charges, including the sending bank charges if any.

7.4 Payment Initiation Services (PIS) parameters and considerations

7.4.3 AML - Required bank details

In order to make an International Payment, the ASPSP will need some of the following details relating to the Beneficiary's bank account:

Data Field	Description
The Account Holders Name	The recipient's full name
SWIFT/BIC Code	A SWIFT Code consists of 8 or 11 characters, both numbers and letters e.g. RFXLGB2L.
Sort Code	UK Bank code (6 digits usually displayed as 3 pairs of numbers), optional if within EEA
Routing Number	The American Bankers Association Number (consists of 9 digits) and is also called a ABA Routing Number
Routing Code	Any other local Bank Code - e.g. BSB number in Australia and New Zealand (6 digits)
IFSC Code	Indian Financial System Code, which is a unique 11-digit code that identifies the bank branch i.e. ICIC0001245.
IBAN	The International Bank Account Number
Bank Name	The name of the bank where the recipient's account is held
Bank Address	The address of the Beneficiary's bank
Account Number	The recipient's bank account number

The information required is different for each country. For further information please see the table below:

Receiving Country	Currency	Information Required	Optional Information
UK	GBP	Account Holder's Name Account Number Sort Code	IBAN SWIFT/BIC code
UK	All Other Currencies	Account Holder's Name IBAN SWIFT/BIC code	Sort Code
All European Countries	All Currencies	Account Holder's Name IBAN SWIFT/BIC code	
Hong Kong	USD, EUR, GBP	Account Holder's Name IBAN SWIFT/BIC code	
China	USD, EUR, GBP	Account Holder's Name Account Number SWIFT/BIC code Bank Name Bank Address	

7.4 Payment Initiation Services (PIS) parameters and considerations

Receiving Country	Currency	Information Required	Optional Information
Australia / New Zealand / South Africa	All Currencies	Account Holder's Name Account Number Routing Code Bank Name Bank Address	SWIFT/BIC code
Canada	All Currencies	Account Holder's Name Account Number SWIFT/BIC code Bank Name Bank Address	Routing Code
USA	All Currencies	Account Holder's Name Account Number ABA Number Bank Name Bank Address	SWIFT/BIC code

Receiving Country	Currency	Information Required	Optional Information
India	INR	Account Holder's Name Account Number IFSC Code Bank Name Bank Address	SWIFT/BIC code
India	All Other Currencies	Account Holder's Name Account Number SWIFT/BIC code Bank Name Bank Address	IFSC Code
All Other Countries	All Currencies	Account Holder's Name Account Number Bank Name Bank Address	SWIFT/BIC code

Note: Whilst the SWIFT BIC is required to route the payments, for payments in Euro the customer does not have to provide this, the sending bank must derive it from the beneficiary IBAN.

7.5 Card-specific Permissions and Data Clusters for AIS journeys

7.5 Card-specific Permissions and Data Clusters for AIS journeys

If an AISP is asking for data access solely to a card account they should adjust the language they use to describe the ASPSP (e.g. “card provider” rather than “bank”) and certain data clusters and permissions. Card specific language is shown in blue.

Data Cluster Language	API End Points	Permissions	Permissions Language	Information available
Your Card Details	Accounts	Accounts Basic	*Any other name by which you refer to this account*	Currency of the account, Nickname of account (e.g. ‘Jakes Household account’)
		Accounts Detail	*Your account name, number and sort-code*	Account Name, Sort Code, Account Number, IBAN, Roll Number (used for Building Society) (plus all data provided in Accounts Basic)
	Balances	Balances	*Your account balance*	Amount, Currency, Credit/Debit, Type of Balance, Date/Time, Credit Line
	All where PAN is available	PAN	*Your long card number*	PAN masked or unmasked depending on how ASPSP displays online currently
Your Regular Payments	Beneficiaries	Beneficiaries Basic	*Payee agreements you have set up*	List of Beneficiaries
		Beneficiaries Detail	*Details of Payee agreements you have set up*	Details of Beneficiaries account information (Name, Sort Code, Account) (plus all data provided in Beneficiaries Basic)
	Standing Orders	Standing Order Basic	*Your Standing Orders*	SO Info, Frequency, Creditor Reference Info, First/Next/Final Payment info
		Standing Order Detail	*Details of your Standing Orders*	Details of Creditor Account Information (Name, Sort Code, Account) (plus all data provided in Standing Order Basic)
	Direct Debits	Direct Debits	*Your Direct Debits*	Mandate info, Status, Name, Previous payment information,
	Scheduled Payments	Scheduled Payments Basic	*Recurring and future dated payments from your card account*	Scheduled dates, amount, reference. Does not include information about the beneficiary
		Scheduled Payments Detail	*Details of recurring and future dated payments from your card account*	Scheduled dates, amount, reference. Includes information about the beneficiary
Your Card Transactions	Transactions	Transactions Basic Credits	*Your incoming transactions*	Transaction Information on payments made into the customer’s account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Does not include information about the entity that made the payment.
		Transactions Basic Debits	*Your outgoing transactions*	Same as above, but for debits
		Transactions Detail Credits	*Details of your incoming transactions*	Transaction Information on payments made into the customer’s account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Includes information about the entity that made the payment.
		Transactions Detailed Debits	*Details of your outgoing transactions*	Same as above but for debits

7.5 Card-specific Permissions and Data Clusters for AIS journeys

Data Cluster Language	API End Points	Permissions	Permissions Language	Information available
Your Statements	Statements	Statements Basic	*Information contained in your statement*	All statement information excluding specific amounts related to various balance types, payments due etc.
		Statements Detail	*Details of information contained in your statement*	All statement information including specific amounts related to various balance types, payments due etc.
Your Card Features and Benefits	**Products**	Product	*Product details - fees, charges, interest, benefits/rewards of your card account*	Refers to customer account product details defined in the Open data API (the fees, charges, interest, benefits/rewards)
	Offers	Offers	*Offers available on your card account*	Balance transfer, promotional rates, limit increases, start & end dates
Your contact details	**Party**	Party	*Your address, telephone numbers and email address as held by your bank/card provider*	Address, telephone numbers and email address as held by your bank/card issuer, party type (sole/joint etc.)

7.6 Open Banking Read/Write API Specification v3.0 - Standard Error Codes

7.6 Open Banking Read/Write API Specification v3.0 - Standard Error Codes

HTTP Status Category	Code	Description
400	UK.OBIE.Field.Expected	For the scenario, when a field-value is not provided in the payload, that is expected in combination with preceding field-value pairs. The corresponding path must be populated with the path of the unexpected field. e.g. ExchangeRate must be specified with Agreed RateType. ExchangeRate should be specified in the path element. InstructionPriority must be specified with Agreed RateType. InstructionPriority should be specified in the path element.
400	UK.OBIE.Field.Invalid	An invalid value is supplied in one of the fields. Reference of the invalid field should be provided in the path field, and url field may have the link to a website explaining the valid behaviour. The error message should describe the problem in detail.
400	UK.OBIE.Field.InvalidDate	An invalid date is supplied, e.g., When a future date is expected, a date in past or current date is supplied. The message can specify the actual problem with the date. The reference of the invalid field should be provided in the path field, and URL field may have the link to a website explaining the valid behaviour
400	UK.OBIE.Field.Missing	A mandatory field, required for the API, is missing from the payload. This error code can be used, if it is not already captured under the validation for UK.OBIE.Resource.InvalidFormat. Reference of the missing field should be provided in the path field, and URL field may have the link to a website explaining the valid behaviour
400	UK.OBIE.Field.Unexpected	For the scenario, when a field-value is provided in the payload, that is not expected in combination with preceding field-value pairs. E.g. ContractIdentification must not be specified with [Actual/Indicative] RateType. ContractIdentification should be specified in the path element ExchangeRate must not be specified with [Actual/Indicative] RateType. ExchangeRate should be specified in the path element. InstructionPriority must not be specified with LocalInstrument. InstructionPriority should be specified in the path element.
400	UK.OBIE.Header.Invalid	An invalid value is supplied in the HTTP header. HTTP Header should be specified in the path element.
400	UK.OBIE.Header.Missing	A required HTTP header has not been provided. HTTP Header should be specified in the path element.
400	UK.OBIE.Resource.ConsentMismatch	{payment-order-consent} and {payment-order} resource mismatch. For example, if an element in the resource’s Initiation or Risk section does not match the consent section. The path element should be populated with the field of the resource that does not match the consent.
400	UK.OBIE.Resource.InvalidConsentStatus	The resource’s associated consent is not in a status that would allow the resource to be created. E.g., if a consent resource had a status of AwaitingAuthorisation or Rejected, a resource could not be created against this consent. The path element should be populated with the field in the consent resource that is invalid.
400	UK.OBIE.Resource.InvalidFormat	When the Payload schema doesn't match to the endpoint, e.g., /domestic-payments endpoint is called with a JSON Payload, which cannot be parsed into a class OBWriteDomestic1
400	UK.OBIE.Resource.NotFound	Returned when a resource with the specified id does not exist (and hence could not be operated upon).
400	UK.OBIE.Rules.AfterCutOffDateTime	{payment-order} consent / resource received after CutOffDateTime
400	UK.OBIE.Signature.Invalid	The signature header x-jws-signature was parsed and has a valid JOSE header that complies with the specification. However, the signature itself could not be verified.
400	UK.OBIE.Signature.InvalidClaim	The JOSE header in the x-jws-signature has one or more claims with an invalid value. (e.g. a kid that does not resolve to a valid certificate). The name of the missing claim should be specified in the path field of the error response.
400	UK.OBIE.Signature.MissingClaim	The JOSE header in the x-jws-signature has one or more mandatory claim(s) that are not specified. The name of the missing claim(s) should be specified in the path field of the error response.
400	UK.OBIE.Signature.Malformed	The x-jws-signature in the request header was malformed and could not be parsed as a valid JWS.
400	UK.OBIE.Signature.Missing	The API request expected an x-jws-signature in the header, but it was missing.

7.6 Open Banking Read/Write API Specification v3.0 - Standard Error Codes

HTTP Status Category	Code	Description
400	UK.OBIE.Signature.Unexpected	The API request was not expecting to receive an x-jws-signature in the header, but the TPP made a request that included an x-jws-signature.
400	UK.OBIE.Unsupported.AccountIdentifier	The account identifier is unsupported for the given scheme. The path element should be populated with the path of the AccountIdentifier.
400	UK.OBIE.Unsupported.AccountSecondaryIdentifier	The account secondary identifier is unsupported for the given scheme. The path element should be populated with the path of the AccountSecondaryIdentifier.
400	UK.OBIE.Unsupported.Currency	The currency is not supported. Use UK.OBIE.Field.Invalid for invalid Currency. The path element should be populated with the path of the Currency. The URL should be populated with a link to ASPSP documentation listing out the supported currencies.
400	UK.OBIE.Unsupported.Frequency	Frequency is not supported. The path element should be populated with the path of the Frequency. The URL should be populated with a link to ASPSP documentation listing out the supported frequencies.
400	UK.OBIE.Unsupported.LocalInstrument	Local Instrument is not supported by the ASPSP. The path element should be populated with the path of the LocalInstrument. The URL should be populated with a link to ASPSP documentation listing out the supported local instruments.
400	UK.OBIE.Unsupported.Scheme	Identification scheme is not supported. The path element should be populated with the path of the scheme. The URL should be populated with a link to ASPSP documentation listing out the supported schemes.
5xx	UK.OBIE.UnexpectedError	An error code that can be used, when an unexpected error occurs. The ASPSP must populated the message with a meaningful error description, without revealing sensitive information.

OPEN BANKING