apicentre
paymentsnz

API Centre
Customer Experience Guidelines

May 2021
Version 2.1

Contents

1 Introduction

The Customer Experience Guidelines ("Guidelines") have been designed to facilitate widespread use of API Standards enabled products and services in a simple, secure and Customer friendly manner.

The implementation of these Guidelines is not mandated by the API Centre and as a result, an API Provider's customer experience may differ from this document.

The API Centre's Account Information and Payments Initiation API Standards set out the base interactions and flows between the Customer, the Third Party, and the API Provider.

These guidelines;

- bring together Customer facing user experience and journey across both Third Party and API Provider when they use the API Standards.
- address the "Customer journey" that is the process that the Customer follows starting within a Third Party online app or browser, through to authentication within the API Provider domain, and completion in the Third Party domain.
- provide examples of what a good Customer experience and Customer journey looks like when the Customer interacts with services that are based on the API Standards
- and provide a starting point for API Standards Users to develop their own propositions.

Customers will only use 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 Third Party and the API Provider is as seamless as possible while providing Customer control in a secure environment. It is essential that Customers are clearly informed about the consent they are providing and the service they are receiving.

The intended audience for these Guidelines is API Standards Users (API Providers and Third Parties).

1.1 Acknowledgements

These Guidelines have been developed from the UK Open Banking Implementation Entity's Customer Experience Guidelines[1] and their associated research.

1.2 Purpose and approach

- **Illustrative guide**
  This document provides an illustrative guide, and there is no requirement on API Standards Users to comply with these Guidelines. The Guidelines help provide a starting

[1] https://standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/latest/

point for API Standards Users to develop their own propositions and implementations may differ in practice.

- **Illustrative but not exhaustive**
  These Guidelines provide the main scenarios that the v2.0 API Standard supports. There are other scenarios, flows or variants that are supported by the v2.0 API Standard that are not illustrated in these Guidelines.

- **Iterative guidance**
  This document will evolve, and iterations will be frequently released, based on additional functionality, ongoing feedback received and changing Customer expectations.

1.3Disclaimer

The Guidelines have been prepared for the sole purpose of providing indicative information and are for general purposes only. The Guidelines should be treated as a general guide or a starting point only. The Guidelines are not specific advice and do not contain all the information that an API Standards User may need for the purpose of designing and using API Standards enabled products or complying with the API Centre Terms and Conditions (**API Terms**).

Adoption of the Guidelines does not replace API Standards Users' obligations as set out in the API Terms. API Standards Users must independently ensure that they comply with the API Terms and the Customer Data Consent and Customer Payment Consent obligations. To the extent that the Guidelines conflict with the API Terms, the API Terms prevail.

The API Centre does not make any express or implied warranty, guarantee or representation regarding the Guidelines, including, without limitation, warranties that the Guidelines are fit for the purposes required by the API Standards Users, Customers or Permitted Users, that compliance with the Guidelines assures compliance with the API Centre Terms, or will ensure that any party might meet the standard of care required of them at law, or that any of the assumptions underlying the Guidance are accurate.

1.4 Relationship with API Centre Terms and Conditions

The Guidelines cover the Customer journey, interaction and hand off separately. The Guidelines include suggested steps that the Customer should navigate, including in relation to consent. The Guidelines refer to **consent** and **authentication.** The steps which API Standards Users are required to take in relation to consent and authentication are set out in clause 7 of the API Terms. In these Guidelines:

Third Party Consent in relation to **Customer Data Consent** refers to the consent given by the Customer to a Third Party under which the Customer authorises:

- a Third Party to contact the Customer's API Provider; and
- the use of the Customer Data for the purposes specified in the Customer Data Consent.

Third Party Consent in relation to **Customer Payment Consent** refers to the consent given by a Customer to a Third Party under which the Customer authorises:

- a payment under which funds will be debited from the Customer's account and credited to the beneficiary nominated in the consent; and
- a Third Party to contact the Customer's API Provider.

Authentication in relation to Customer Data Consent refers to the consent given by the Customer to an API Provider under which the Customer authorises an API Provider to act on an instruction received from the Third Party in relation to Customer data.

Authentication in relation to Customer Payment Consent refers to the consent given by the Customer to an API Provider under which the Customer authorises an API Provider to act on an instruction received from a Third Party, on behalf of the Customer in respect of that payment transaction.

1.5 Relationship with v2.1.0 API standard

The API Centre has attempted to align the Customer Experience Guidelines to the v2.1.0 API Standard. Generally, where the Customer journey diagrams use the term 'must', it reflects a requirement of the v2.1.0 API Standard. The '**must**' and '**should**' settings described in the Guidelines document are not to be relied upon as a description of the API Standard and do not impose any obligation on API Standards Users to comply with these Guidelines.

1.6 Document structure

The following principles underpin the core Customer journey described in three 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 consenting to share their payment account data with Third Parties.
- **Payment Initiation Services (PIS)**
  Service propositions enabled by Customers consenting to Third Parties initiating payments from their payment accounts.

API Providers should be familiar with their own role and that of others across all these proposition types.

Third Parties 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 others 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. It is important to note that the Guidelines do not set out every variation or possible scenario that the API Standards support. The Guidelines provide illustrative examples of the key Customer journeys. In some cases, the Guidelines indicate where there could be other variations on the Customer journey, but the Guidelines will not go into the identified variation in any detail.

Each unique journey has been broken out and described over a number of stages. They can 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 stage types are:

- **Journey Description**
  A high-level description of the specific account information, payment initiation or confirmation of funds Customer journey.
- **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.
- **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 CX considerations, where research has raised specific Customer priorities or concerns that should be addressed through the eventual solution.

1.7 The API standard Customer journey

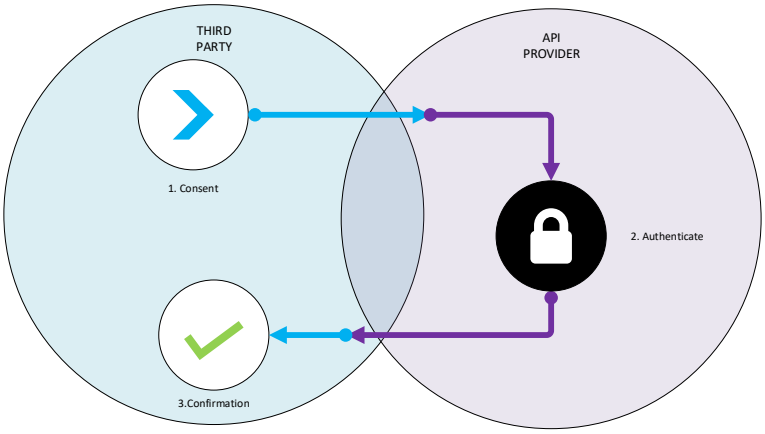
The Guidelines have been separated into a set of clear, highly simplified white label wireframes that cover the Customer journey, interaction and hand off separately.

These are intended to be platform agnostic, to place focus on only the key elements (e.g., messages, fields, checkboxes) and the steps that the Customer should navigate.

In all cases they are constructed around the primary API Standard Customer journey, which is illustrated below.

At the core of each API Standard Customer journey is the mechanism by which the Customer gives consent to a Third Party to access account information held at their API Provider or to initiate payments from their API Provider account.

In general, simplified terms:



1. the consent request is initiated in the Third Party domain (step 1 right).
2. the Customer is then directed to the domain of its API Provider for authentication (step 2 right).
3. then, once authentication is complete, the API Provider will be able to respond to the Third Party's account information or payment initiation request and redirect the Customer back to the Third Party for confirmation and completion of the journey (step 3 left).

2 Customer journey

2.1 Customer in control

So that Customers can make informed decisions while enjoying a simple and easy navigation and a secure Customer journey, a key principle is to ensure clarity of information that is presented and described in a manner that ensures that each API Standard Customer journey is easy to understand.

2.2 Useful elements in the Customer journey

Many Customers skim through the information presented to them when setting up online products when the information is not well presented.

In their desire to achieve the benefit, insufficient notice is taken of the implications of their actions, or the terms and conditions. It is common to find that they cannot describe what they have just agreed to.

Research carried out by the Open Banking Implementation Entity (OBIE), based in the UK, shows that better understanding can be achieved by carefully designing the Customer journey. It reveals that the solution is about:

- effective, intuitive presentation of information,
- not introducing steps to slow the Customer down or repeat information.

The following methods have been found to be the most effective:

- Clear messages and navigation in the redirection screens that pass the Customer from the Third Party to the API Provider and back again.
- The redirection screen should create a clear sense of separation as the Customer enters the API Provider domain to authenticate, and as they return to the Third Party. Use redirect screens as signposts so Customers know and trust where they are in the journey.
- Present information in an intuitive and easily understood way.
- Keep it to a minimum.
- When it is necessary to present more complex information it is easier for the Customer to understand when:
    - presented in a series of smaller amounts,
    - across more than one screen.
- Avoid text heavy single screens.
- 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 reduce drop off.
- Experience and branding should mirror existing online Customer channels.

2.3 Unhelpful elements in the Customer journey

Research by OBIE 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 an increase in Customer drop off.

The following unhelpful elements were identified in the research and should 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.
- Customers having to scroll up and down the screen to progress the Customer journey.
- Unnecessary 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, web pages or apps that have not been effectively debugged, and unexpected crashing of web pages or apps.
- 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.
- Asking for information when it is not needed.
- Forcing the Customer to open a new browser window during the Customer journey.
- Asking a Customer to input information that they do not readily have to hand, such as unique Customer reference numbers.
- Requesting input of information that could be pre-populated once the Customer has authenticated.
- Inconsistency in selecting an online channel when multiple channels are supported e.g., differentiating between personal and business banking.

2.4 Customer experience principles

The API Standard Customer experience should balance informed decision making while remaining understandable, intuitive and effective. The Customer experience should be shaped and positioned into content and functionality that clearly communicates and facilitates purpose, intent and relevance and meets the appropriate legal tests relating to the customer disclosure.

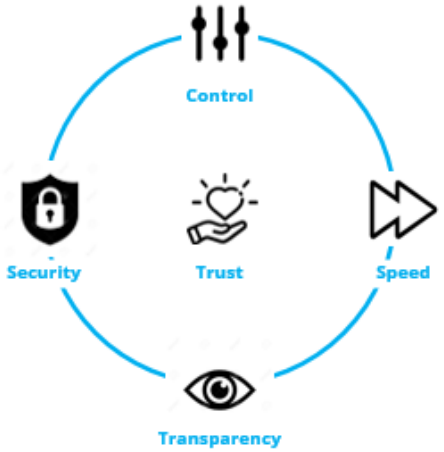
This is especially true in the act of giving consent context, where Customers always need to know and understand:

- 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; and
- a clear 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 the act of giving consent is structured, but also how it is expressed, designed and organised around a range of changing human needs.

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

These guiding experience principles are deeply Customer centred. 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 a simple and effective way.



Extensive Customer research undertaken by OBIE has demonstrated certain recurring themes that Customers deeply care, or are worried, about. To support and achieve the goal of creating trust, these themes have been combined and made into a few key experience principles when implementing API enabled Customer solutions. These principles underpin the range of core journeys and key Customer interactions described throughout the Guidelines.

2.4.1 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 driven by a loss of control in the process.

If Customers understand what is going on in a process, they can make informed decisions and choices on their own terms – including the option to change their mind. It provides 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 API Standards, control comes from providing Customers with 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 cancel consents given when they feel it is appropriate to do so).

Standards Users need to consider how they provide ownership and control to Customers throughout – enabling Customers to understand and take ownership of the decisions made through this process and that this is something that they are choosing and in charge of.

2.4.2 Speed

Speed should 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 difficult than Customers are used to [or expecting] is going to degrade adoption. Each interaction should be managed and optimised, as well as hand-off between systems for speed, clarity and efficiency, but without sacrificing the principles of security and control.

In addition, be mindful that speed of transaction or interaction is not necessarily about the 'fastest possible' experience. As we have indicated, informed decision making needs to be supported through comprehension and clarity (especially in the context of Account Information Services), allowing Customers to, above all, move at a pace that suits them and ensuring that the Customer knows what they are consenting to.

Third Parties and API Providers need to ensure that API Standard 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.

2.4.3 Transparency

Transparency of choice, action, and, importantly, the consequences of actions or sharing of data is crucial to promoting the benefits of API Standards.

In new transactional scenarios where Customers are being encouraged to share personal information this is critical. Be clear on what is required from the Customer, why, for what purpose and what the consequences could be.

Sharing information is a trade-off for convenience and benefits. The value exchange for the consumer should be made explicitly clear.

This is, however, a balancing act. We do not want to overburden the Customer or weigh down the experience with excessive explanations. Transparency is therefore about providing progressive levels of information, in plain language, that inform and support Customer decisions

2.4.4 Security

In the context of Security, the key concerns for Customers are fraud and data privacy.

Many will understand fraud, but data privacy may be less well defined in the minds of consumers. Not everyone has the same idea about what 'my data' 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 have access to it. Such concerns can be even deeper with newer brands, lacking established consumer confidence.

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

In addition to personal data, transactional (data) security is the critical factor to ensure long term use of Third Party services. As a minimum, Third Parties and API Providers should ensure this is no less than consumers expect today.

As a new service, all security messaging should be clear.

2.4.5 Trust

Building trust with early adopting Customers is crucial and can be done by communicating clearly what is going to happen and ensuring their experience matches that.

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

Standards Users need to consider, create and promote values of trust through every part of their API Standard Customer journeys, to foster understanding, acceptance and adoption of new innovative products and services.

2.5 Protection for vulnerable Customers

Standards users should be thinking of making their services suitable for vulnerable Customers. Those who are seen 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.

For reference, the NZBA and NZHRC have published guidelines that specifically relate to the provision of services to vulnerable persons:

- https://www.nzba.org.nz/consumer-information/code-banking-practice/older-and-disabled-Customer-guidelines/.
- hrc.co.nz/our-work/economic-and-social-rights/past-work/canterbury-earthquake-recovery/red-zones-report/best-practice-guidelines-prioritisation-vulnerable-Customers/

It should be noted, however, that Guidelines still apply to the provision and communication of services to vulnerable persons. A Standards User should look to enhance the service provided in ways that would benefit an identified vulnerable group i.e., using large print or clear fonts for users with impaired vision.

3 Authentication methods

3.1 Overview

The API Standards will support both redirection and decoupled authentication to allow a Customer to use the same authentication mechanisms while using a Third Party as they use when accessing the API Provider directly.

The general principles that apply relating to authentication are:

1. API Providers authenticate a Customer: This needs to go through a Strong Customer Authentication (SCA) at the Customer's API Provider for a Third Party request (i.e., access to information or payment initiation) and must be actioned by the API Provider.
2. Customers should have their normal authentication methods available: A Customer should be able to use the elements they prefer to authenticate with their API Provider if supported when interacting directly with their API Provider.
3. Parity of experience: The Customer experience when authenticating within a journey with a Third Party should involve no more delay or friction than the equivalent experience with their API Provider.
4. Once per session SCA: SCA should not be required more than once for a single session of access to account information or a single payment initiation.
5. No Obstacles: API Providers should not create unnecessary delay or friction during authentication including unnecessary or superfluous steps, attributes, or unclear language, e.g., advertising of API Providers products or services, language that could discourage the use of Third Party services or additional features that may divert the Customer from the authentication process (with the potential exception of services provided to vulnerable Customers).

3.2 Redirection based authentication

3.2.1 Browser based redirection – Account Information Services

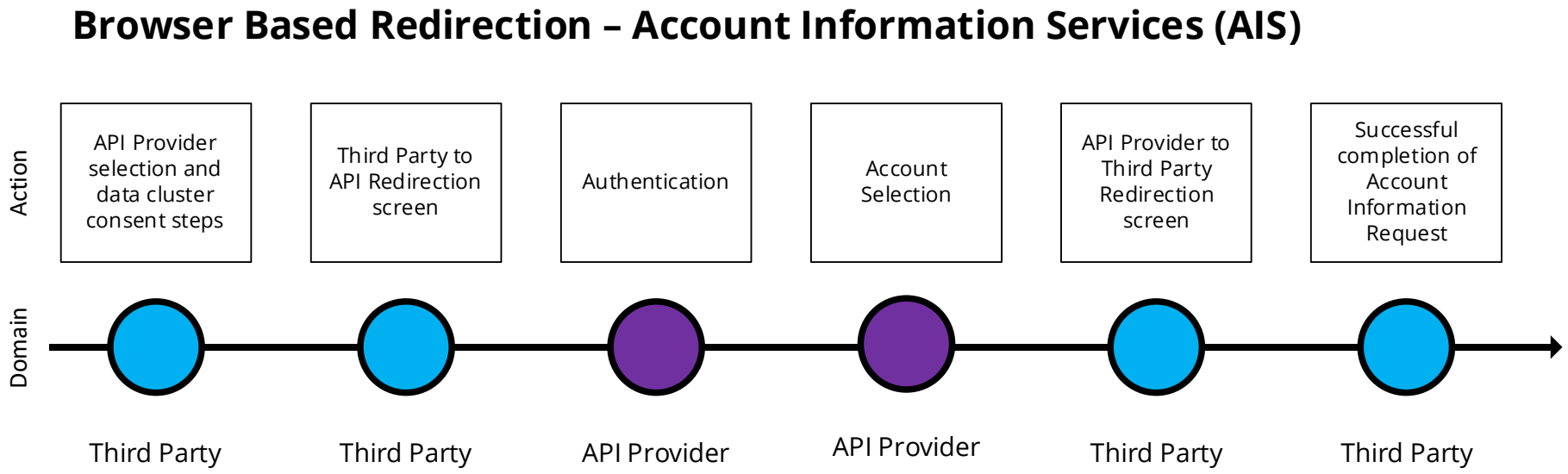
3.2.1.1 Journey description

Customer authentication with the API Provider using browser based redirection from a Third Party for an Account Information Services request.

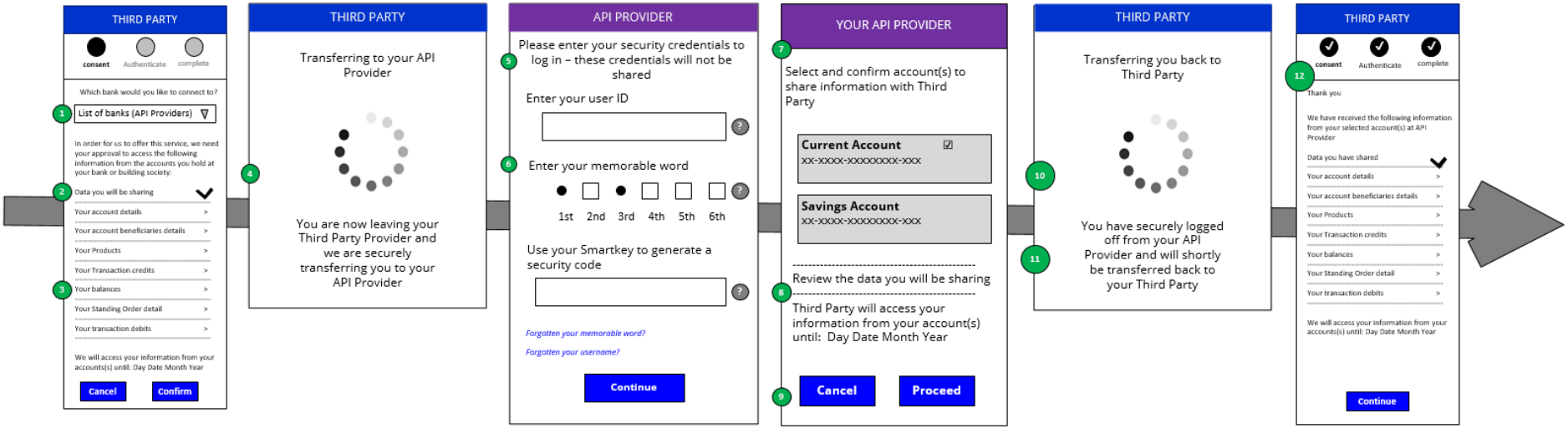
This enables a Customer to authenticate with their API Provider while using a Third Party for Account Information Services, using the same web based authentication method which the Customer uses when accessing the API Provider web channel directly.

This model works when the Customer is consuming the Third Party service on a device that does not have the API Provider app, or the Customer does not have the API Provider mobile app.

3.2.1.2 Journey map

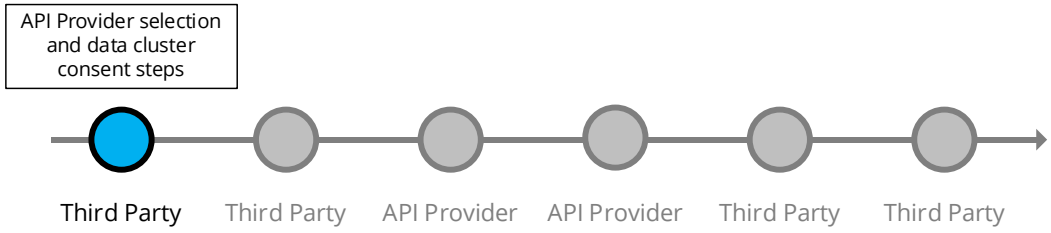


3.2.1.3 Wireframe journey



3.2.1.4 Wireframe annotations

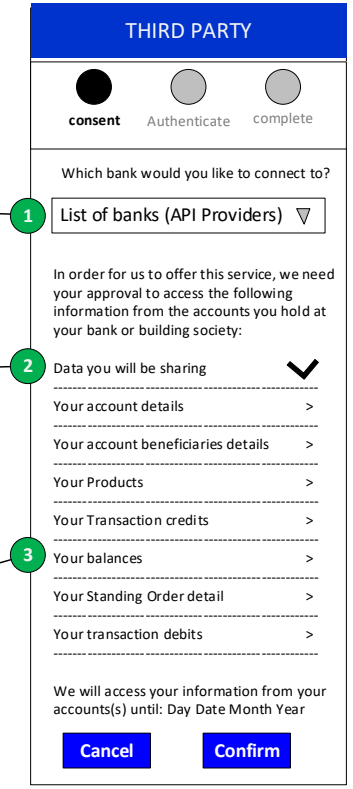
3.2.1.4.1 API Provider selection



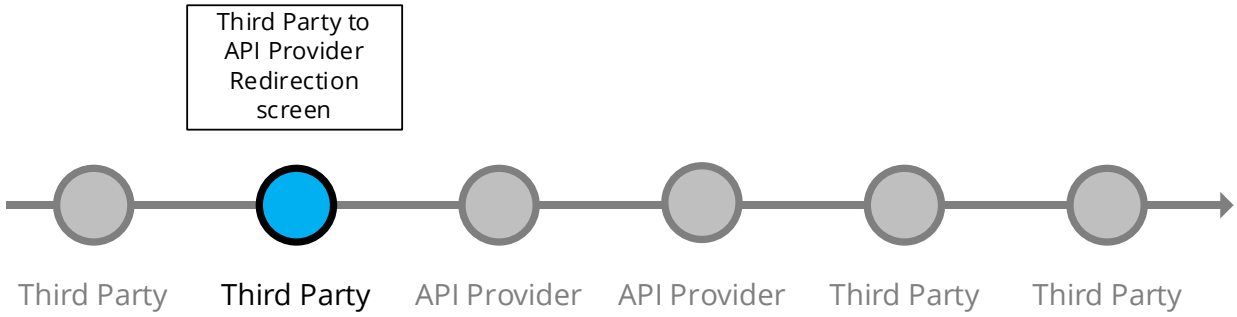
The Third Party **should** ask the customer to identify their API Provider before requesting consent so that the consent request can be constructed in line with the API Provider's data capabilities (which the API Provider must make available to the Third Party).

The Third Party **should** provide the customer sufficient information to enable the customer to make an informed decision. At a minimum this must include requirements in clause 7.4(a)(i) of the API Centre terms and conditions; the nature of information that may be disclosed, the persons to whom it may be disclosed and the purpose for which information may be used and should also include the period over which it has been requested and when the consent for the account information will expire (consent could be ongoing or one-off).
If the customer facing entity is acting on behalf of a Third Party as it's agent, the customer must be made aware that the agent is acting on behalf of the Third Party.

The Third Party **should** provide the Customer with a description of the data being requested using the structure and the language recommended by the API Centre and ensure that this request is specific to only the information required for the provision of their Account Information Service to the customer.
The Third Party **should** present the data at a Data Cluster level and allow the Customer to expand the level of detail to show each Data Permission. The Third Party should only present those data clusters relevant for the product type in question. Where the request is for multiple product types then the detail shown in the data cluster should explain to the customer the product types to which it applies or state that it is shared across multiple product types.
Once Customer has consented, the Customer will be directed to their API Provider.

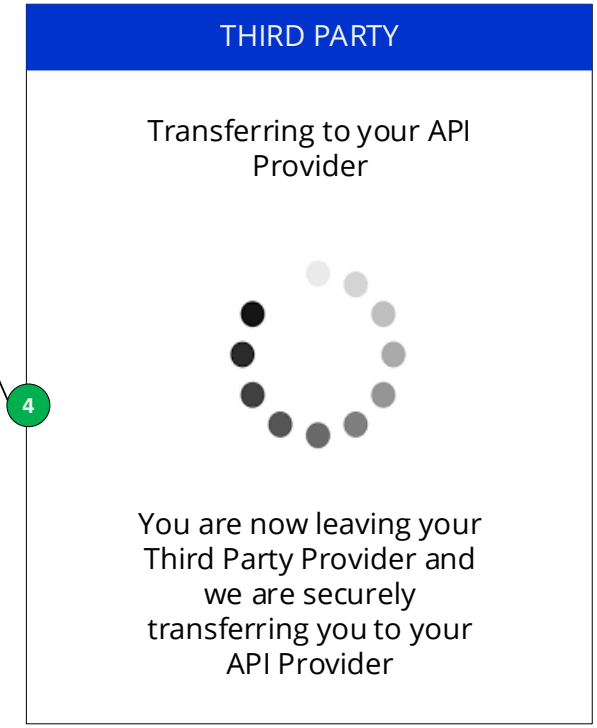


3.2.1.4.2 Third Party redirection

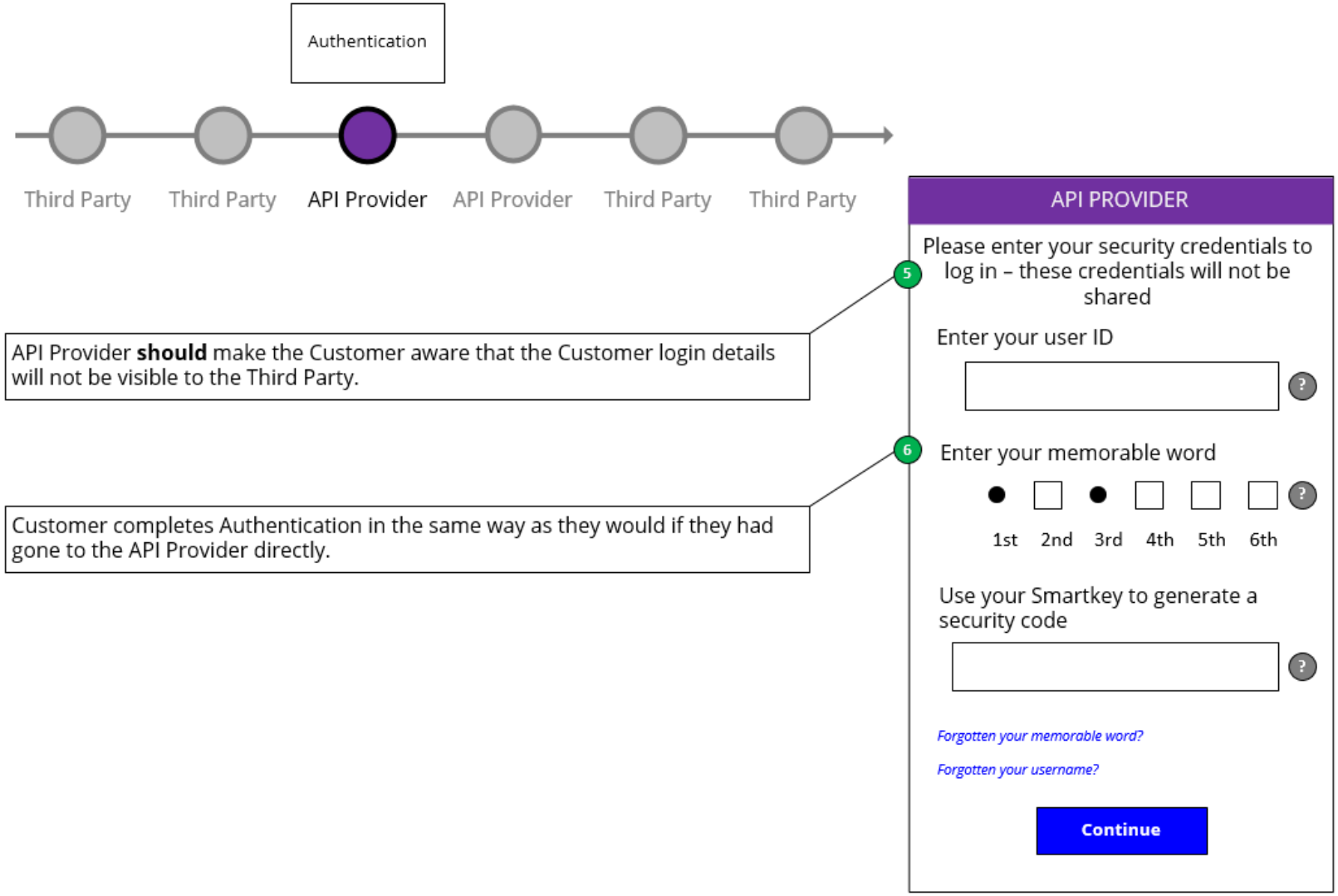


The redirection **should** take the Customer to the API Provider web page (desktop/ mobile) for authentication purposes only without introducing any additional screens.

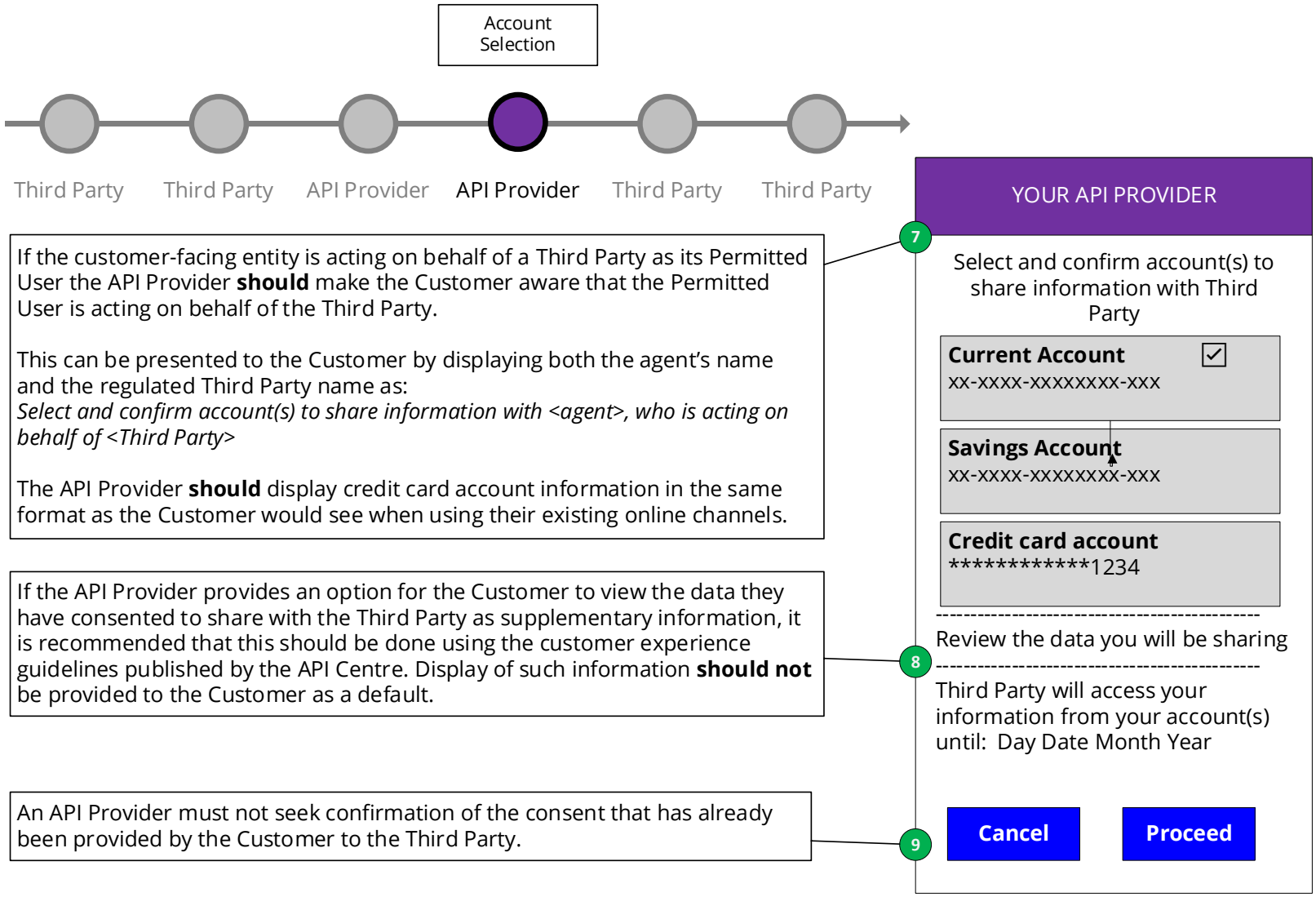
The web based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the web based API Provider channel (desktop/mobile).



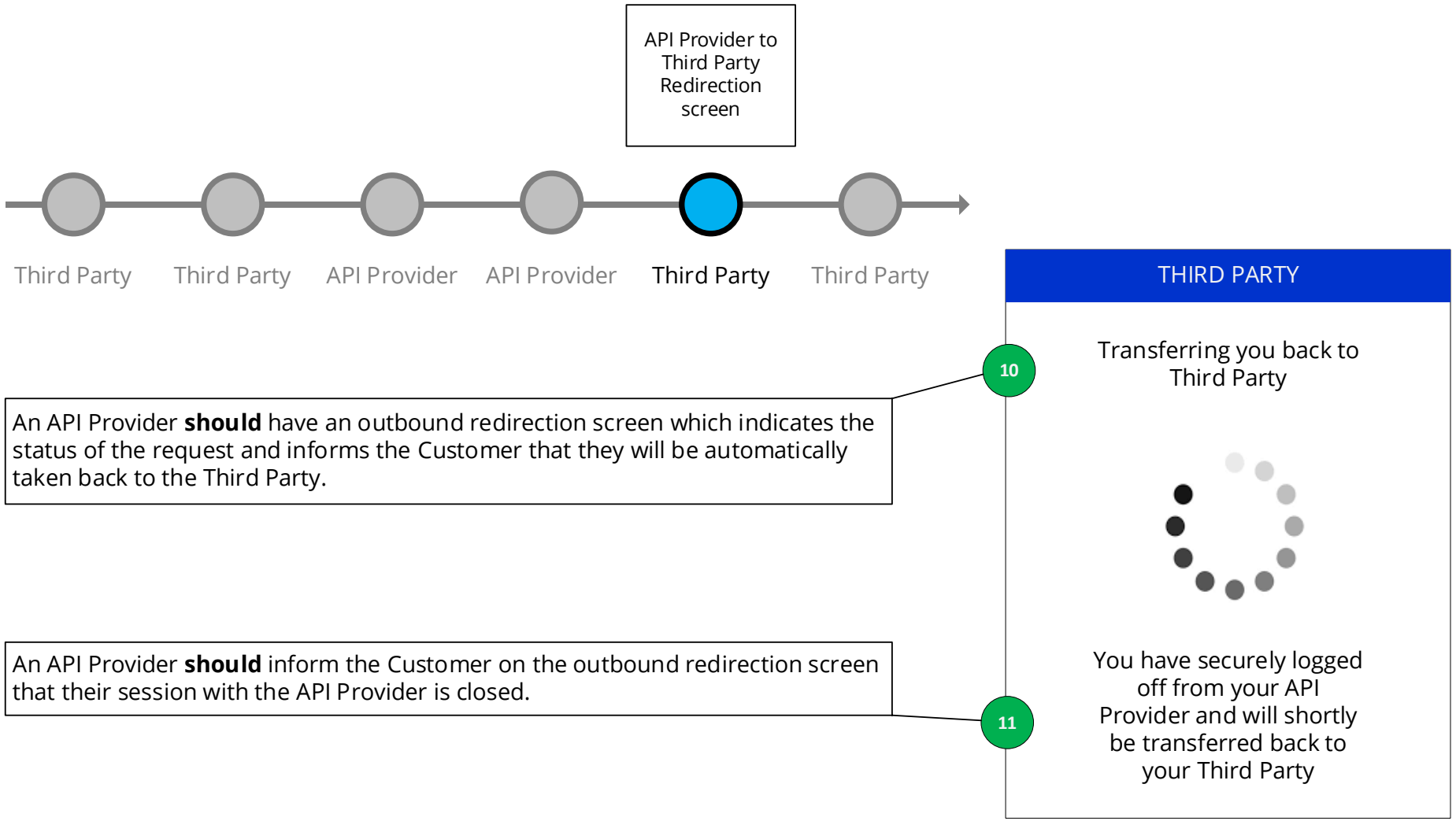
3.2.1.4.3 Authentication



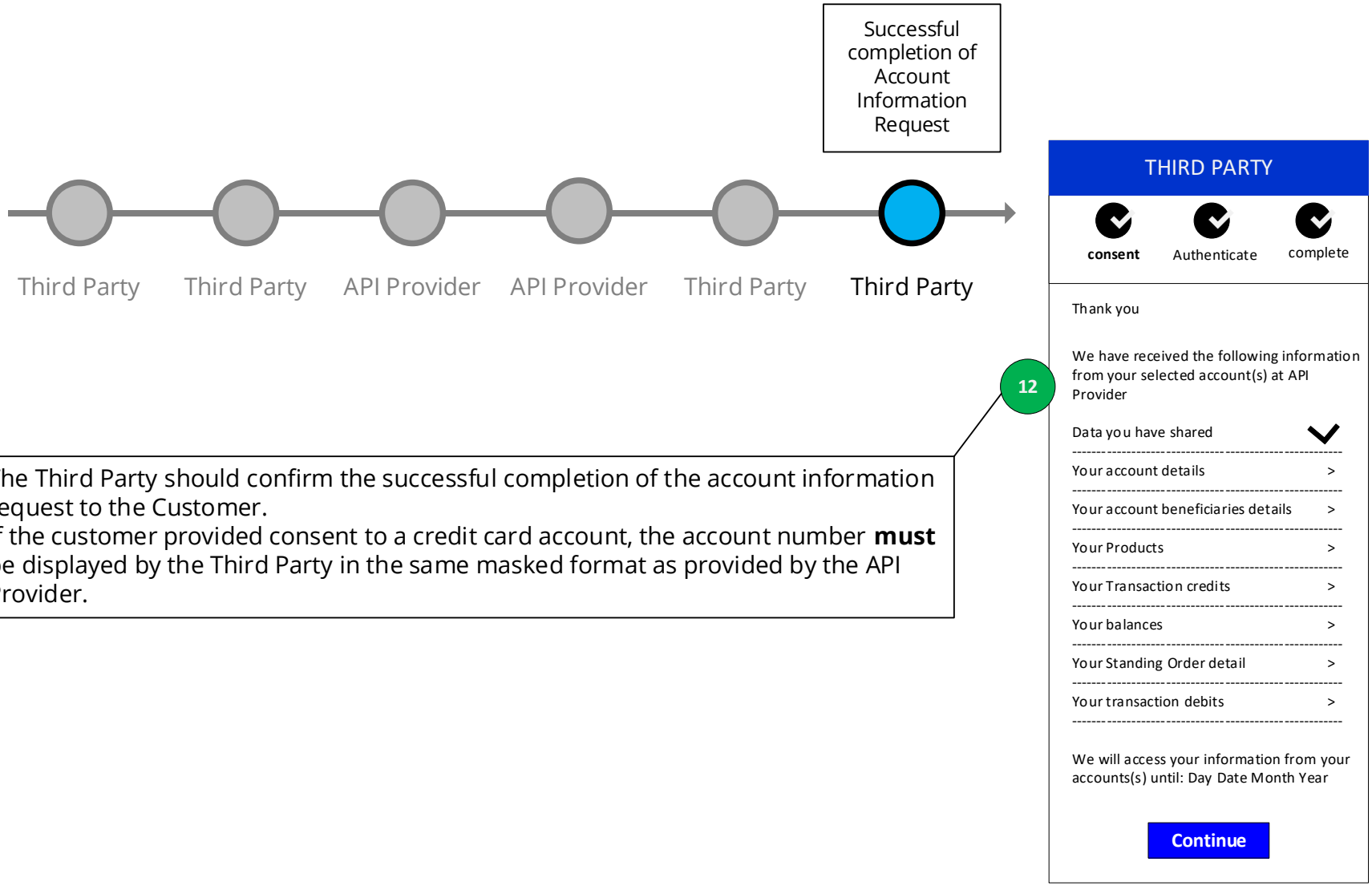
3.2.1.4.4 Account selection



3.2.1.4.5 API Provider redirection



3.2.1.4.6 Third Party Confirmation



The Third Party should confirm the successful completion of the account information request to the Customer.
If the customer provided consent to a credit card account, the account number **must** be displayed by the Third Party in the same masked format as provided by the API Provider.

3.2.2 Browser based redirection – Payment Initiation Services

3.2.2.1 Journey description

Customer authentication with the API Provider using browser based redirection for a Payment Initiation Service request.

This enables a Customer to authenticate with their API Provider while via a Third Party for the Payment Initiation Service, using the same web based authentication method which they use when accessing the API Provider web channel directly.

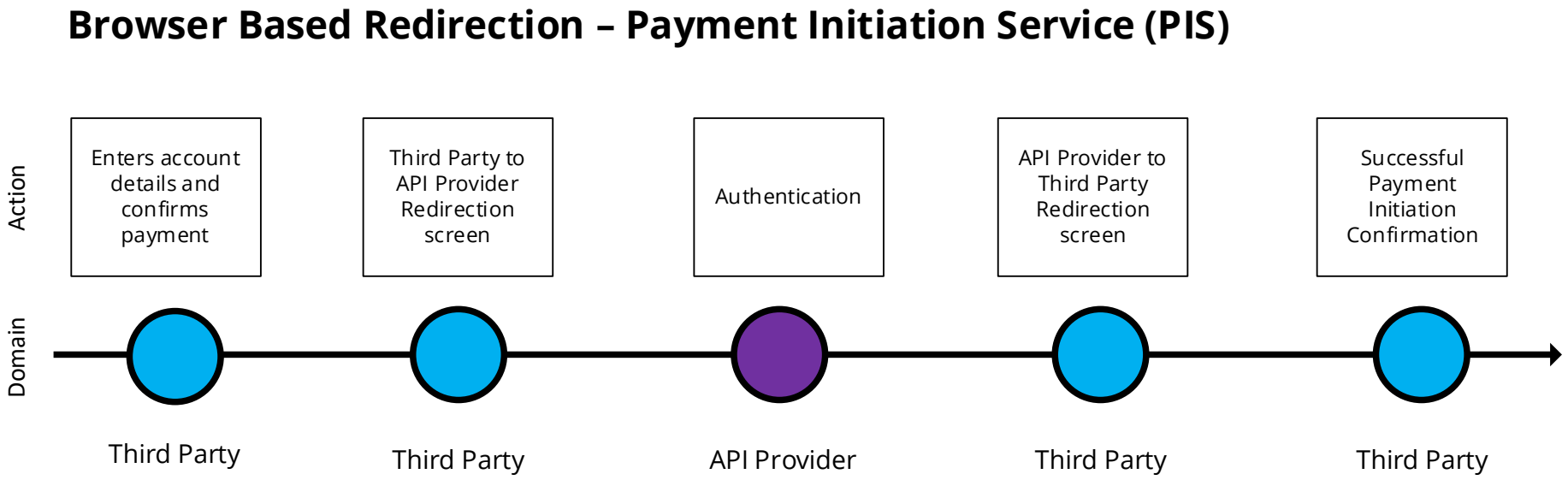
This model works when the Customer is consuming the Third Party service on a device that does not have the API Provider app, or the Customer does not have the API Provider mobile app and is appliable to both one time only payments initiation customer journeys as well as when establishing an Enduring Payment Consent.

Variations

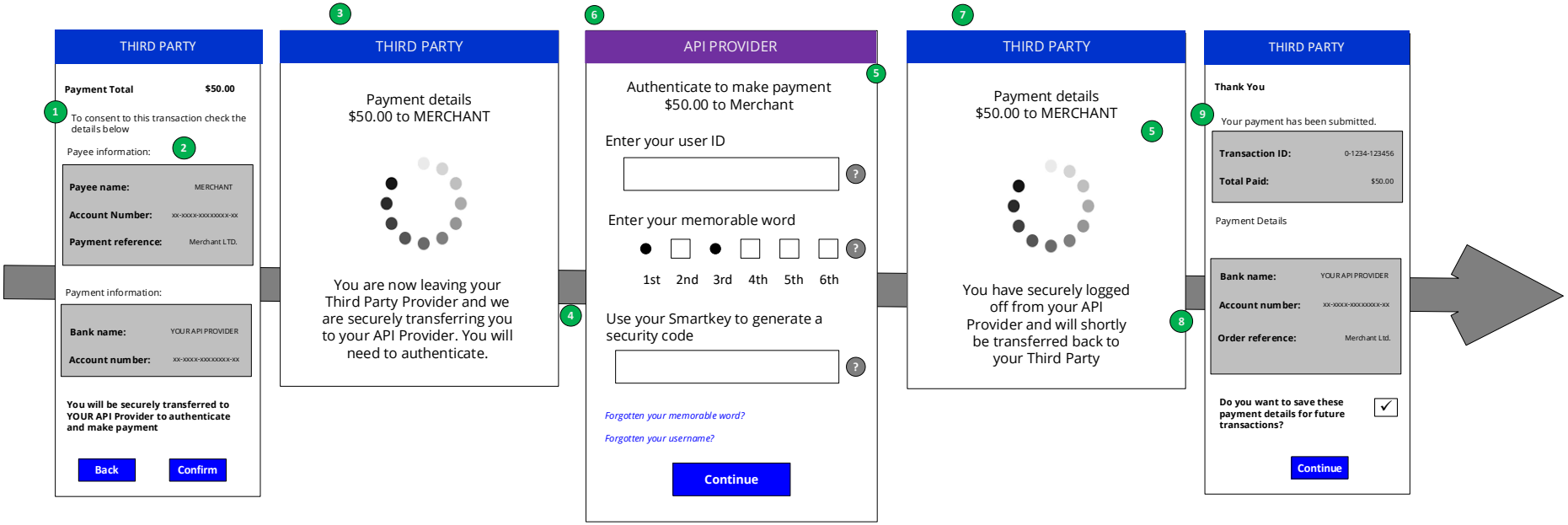
There are variations to this process. We have not shown the full journey breakdown for these variations but have listed them below (to be expanded upon as variations in use are identified):

1. The select account step (now as part of the first step – entering account details) could happen **after** the authentication step and will take place in the API Provider's environment instead of the Third Party environment.

3.2.2.2 Journey map



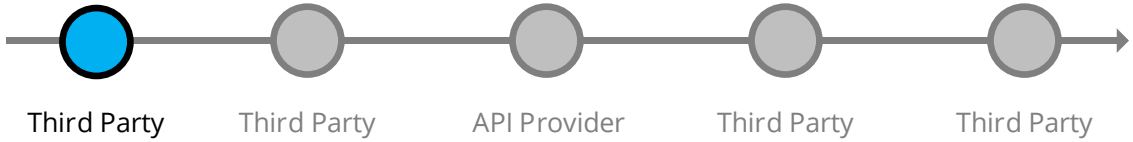
3.2.2.3 Wireframe journey



3.2.2.4 Wireframe annotations

3.2.2.4.1 API Provider selection

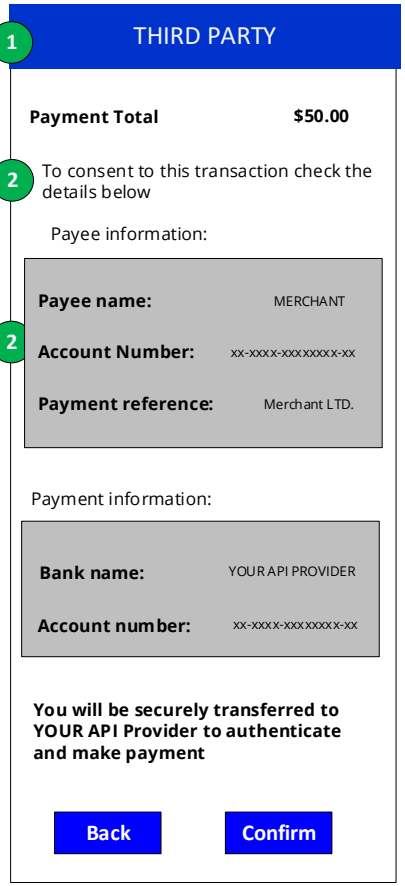
Enters account details and confirms payment



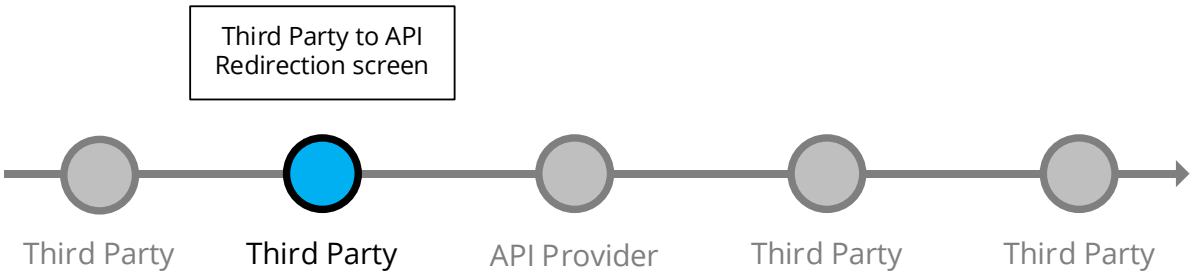
<u>Customer payment Account Selection</u>
A Third Party **must** provide the Customer at least one of the following options:
Enter their Payer payment Account Identification details.
Select their Account Identification details (this assumes they have been saved previously).

A Third Party **should** display the details of the payment to be authorised and the nominated party to whom the funds will be credited.

A Third Party **should** communicate information clearly to the Customer when obtaining consent in order to initiate the payment order.



3.2.2.4.2 Third Party redirection

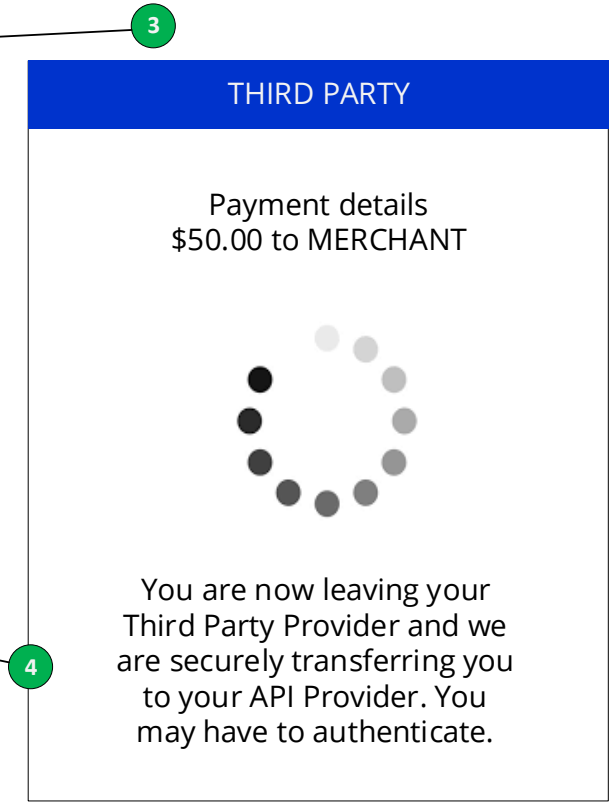


A Third Party **should** make the Customer aware through an inbound redirection screen that they are being taken to their API Provider for authentication to complete the payment.

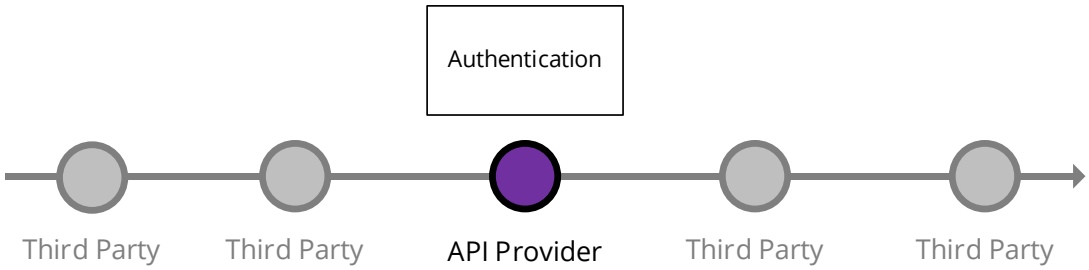
A Third Party **should** display in the Redirection screen the Payment Amount, Currency and the Payee Account Name to make the Customer aware of these details.

The redirection **must** take the Customer to an API Provider web page (desktop/ mobile) for authentication purposes only without introducing any additional screens.

The web based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the web based API Provider channel (desktop/mobile).



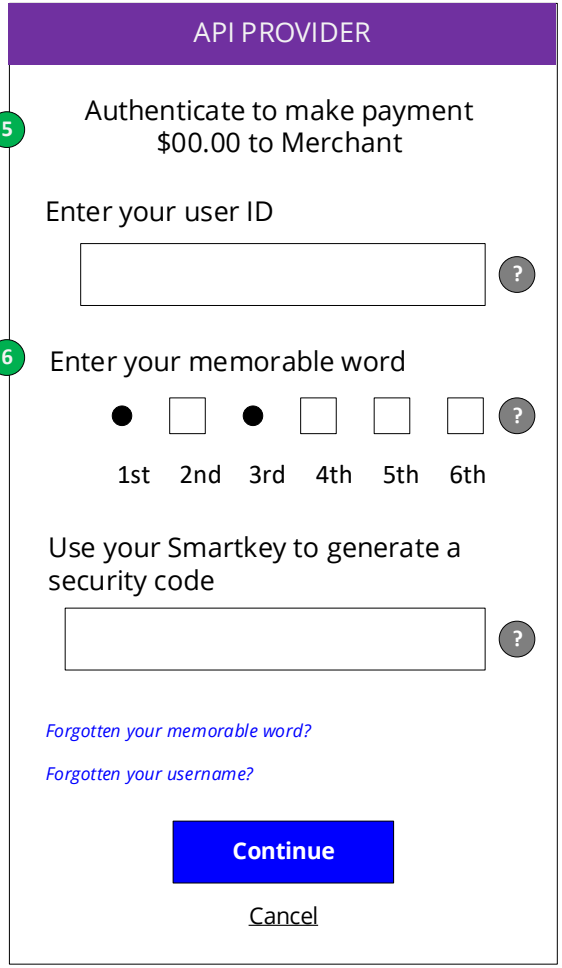
3.2.2.4.3 Authentication



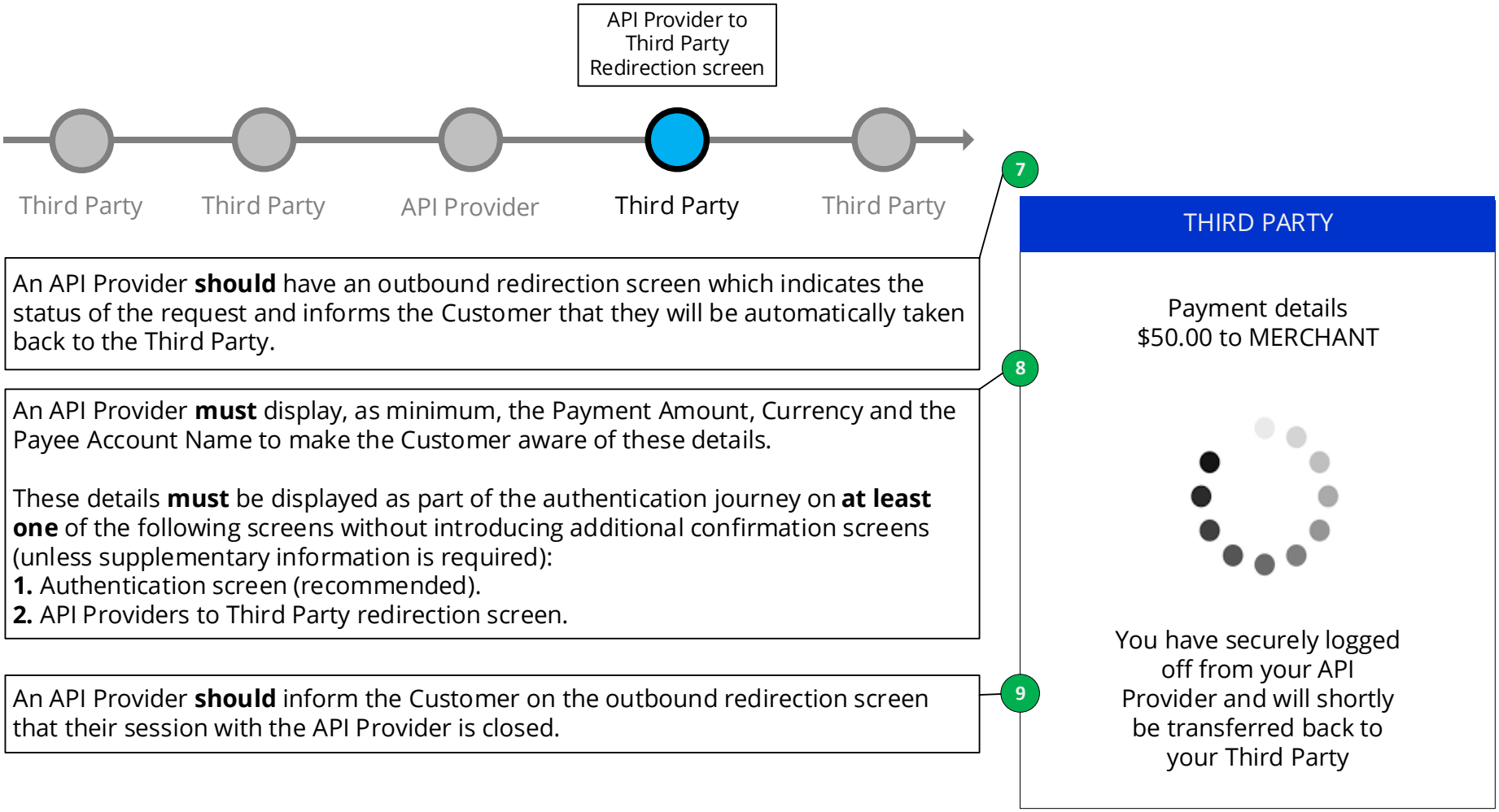
The API Provider **must** display, as minimum, the Payment Amount, Currency and the Payee Account Name to make the Customer aware of these details.

These details **must** be displayed as part of the authentication journey on **at least one** of the following screens without introducing additional confirmation screens (unless supplementary information is required:
1. Authentication screen (recommended).
2. API Provider to Third Party redirection screen.

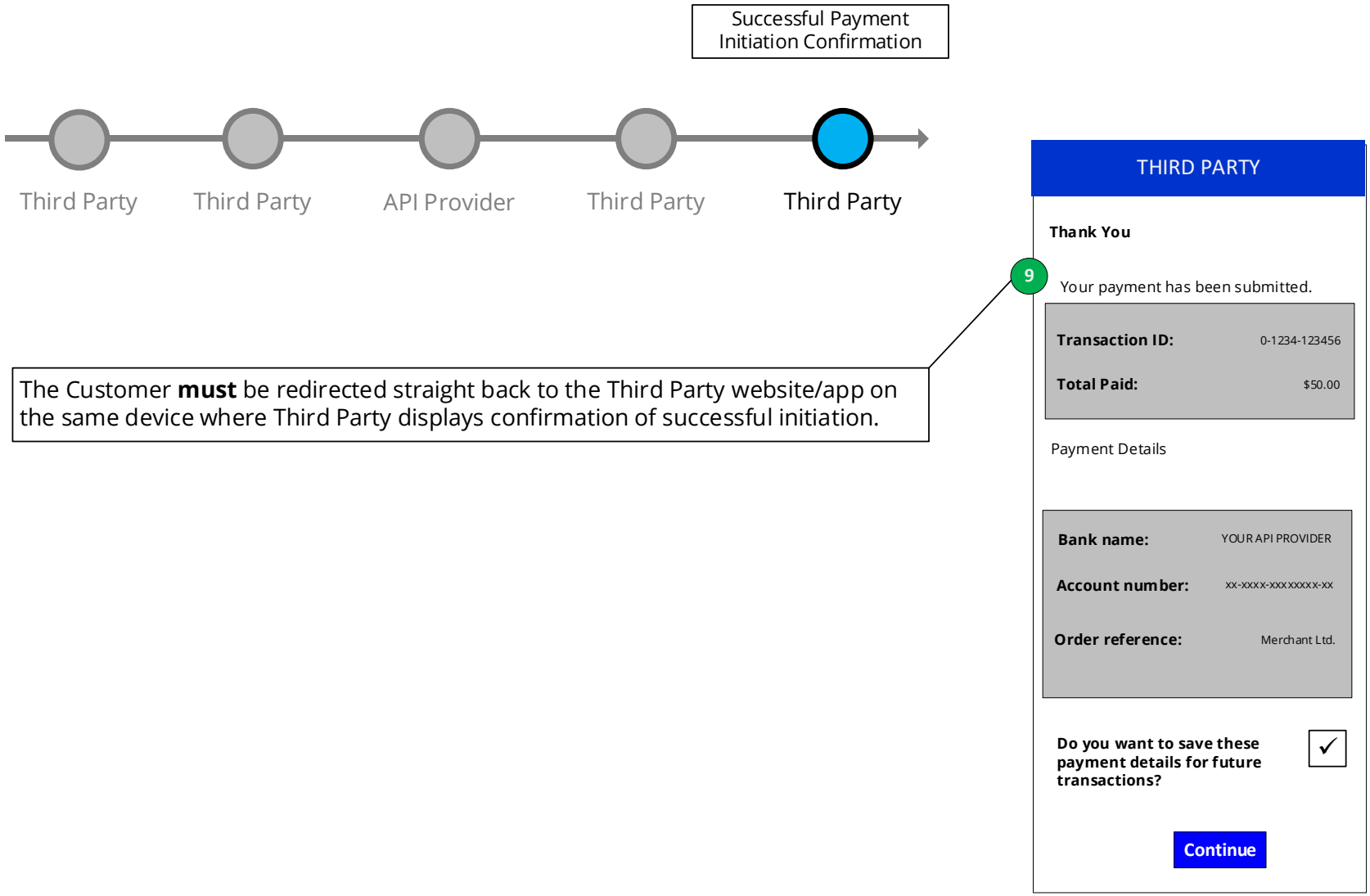
The API Provider web based authentication **should** have no more than the number of steps that the Customer would experience when making a payment directly through the API Provider web based channel (desktop/mobile).



3.2.2.4.4 API Provider redirection



3.2.2.4.5 Confirmation



3.2.3 App based redirection – Account Information Services

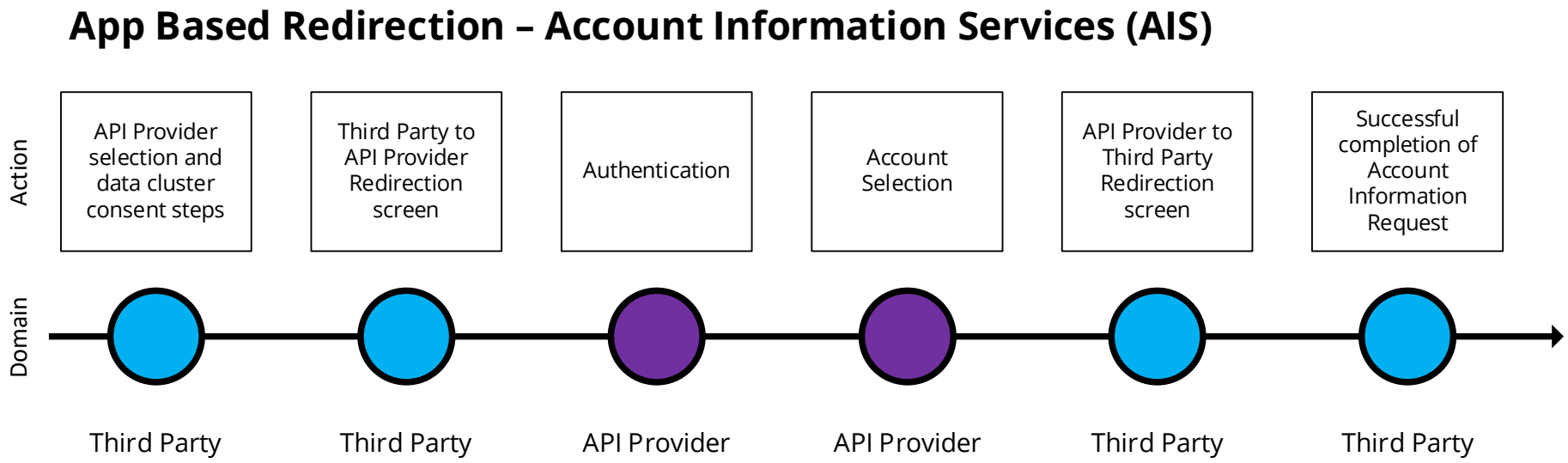
3.2.3.1 Journey description

Customer authentication with the API Provider using the API Provider mobile app installed on the same device on which the Customer is consuming the Third Party service.

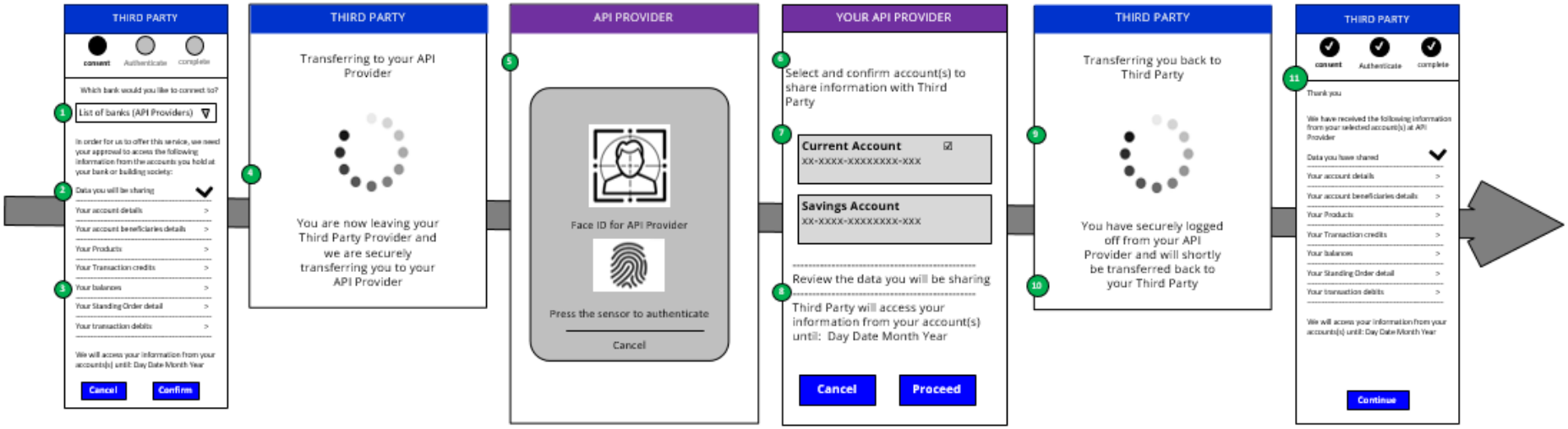
Enables the Customer to authenticate with the API Provider while using a Third Party for Account Information Services using the same API Provider app based authentication method which they use when accessing the API Provider mobile channel directly.

Third Party service could be web based or app based. The redirection should directly invoke the API Provider app to enable the Customer to authenticate and should not require the Customer to provide any Customer identifier or other credentials to the Third Party. Redirections can only be done on the same device.

3.2.3.2 Journey map

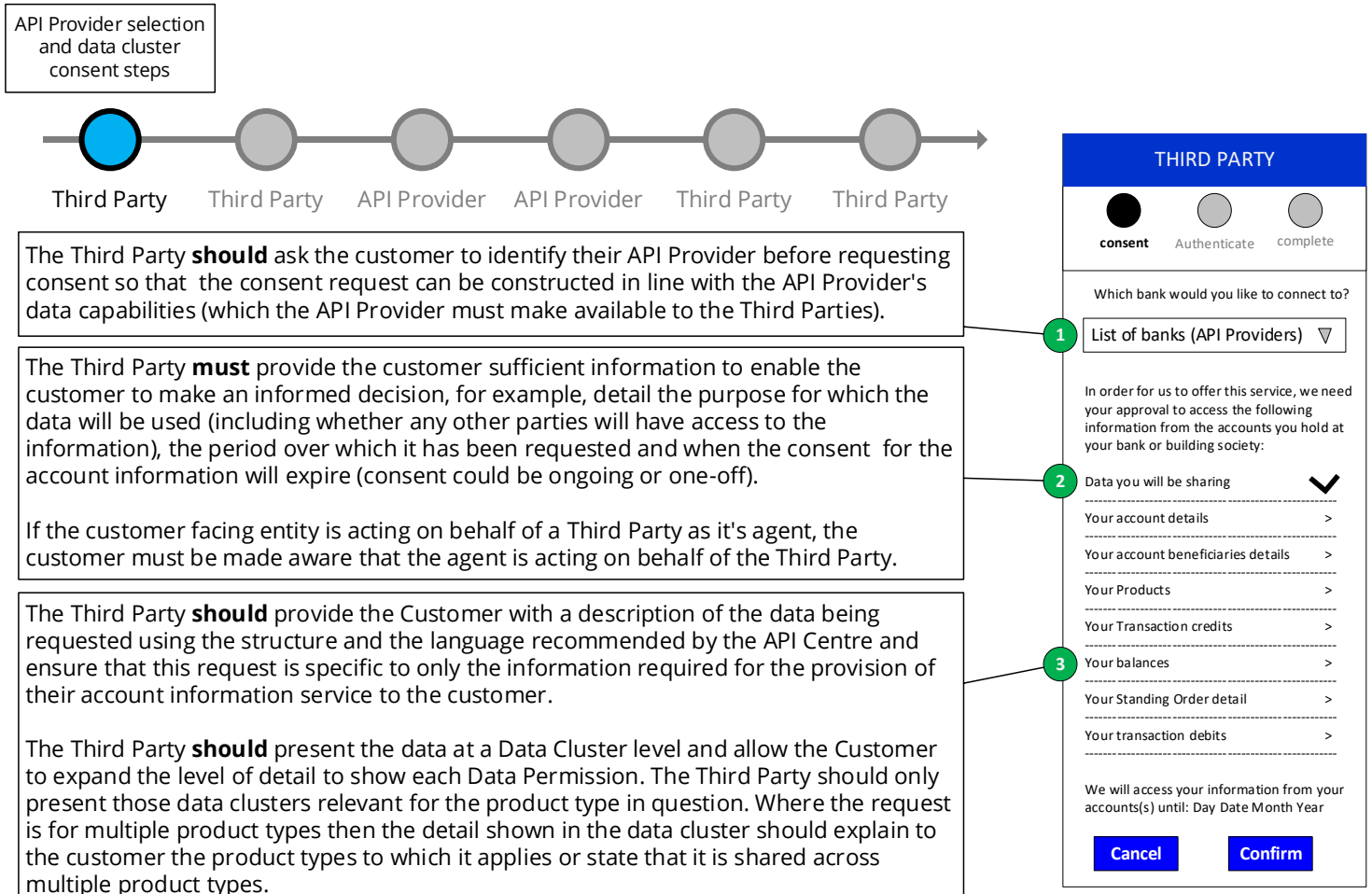


3.2.3.3 Wireframe journey



3.2.3.4 Wireframe annotations

3.2.3.4.1 API Provider selection



3.2.3.4.2 Third Party redirects to API Provider

Third Party to API Provider Redirection screen

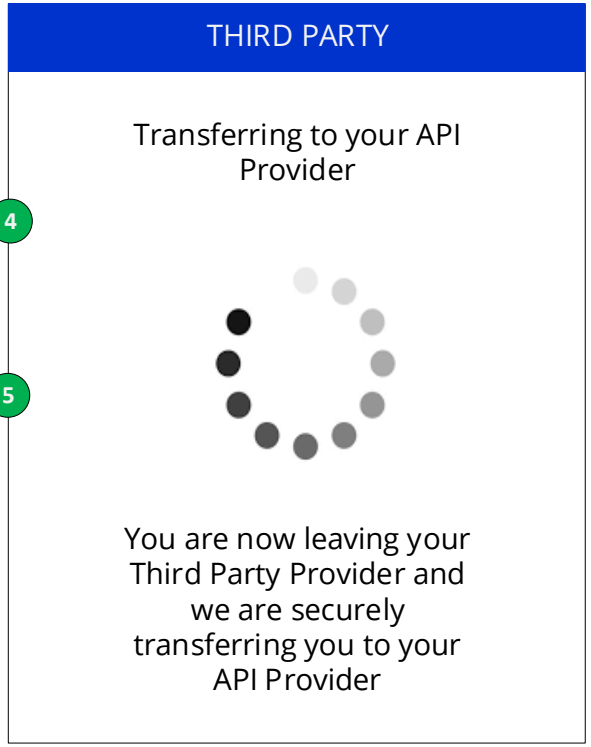
The Third Party **should** make the Customer aware on the inbound redirection screen that they will be taken to their API Provider for authentication for account access.

4

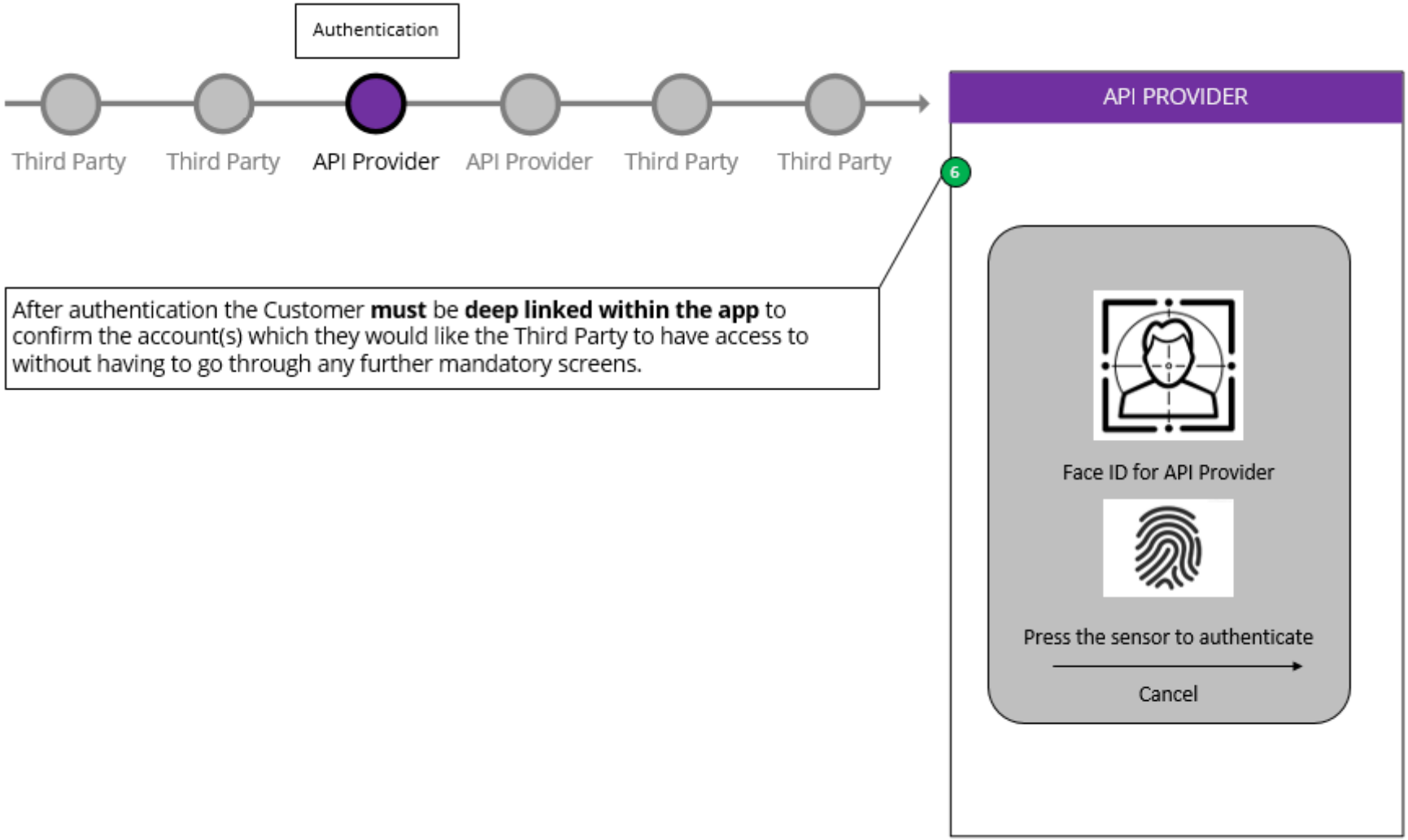
If the Customer has an API Provider app installed on the same device the redirection **should** invoke the API Provider app for authentication purposes only without introducing any additional screens.

The API Provider app based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the API Provider mobile app(biometric, passcode, credentials) and offer the same authentication method(s) available to the Customer when authenticating with the API Provider direct channels.

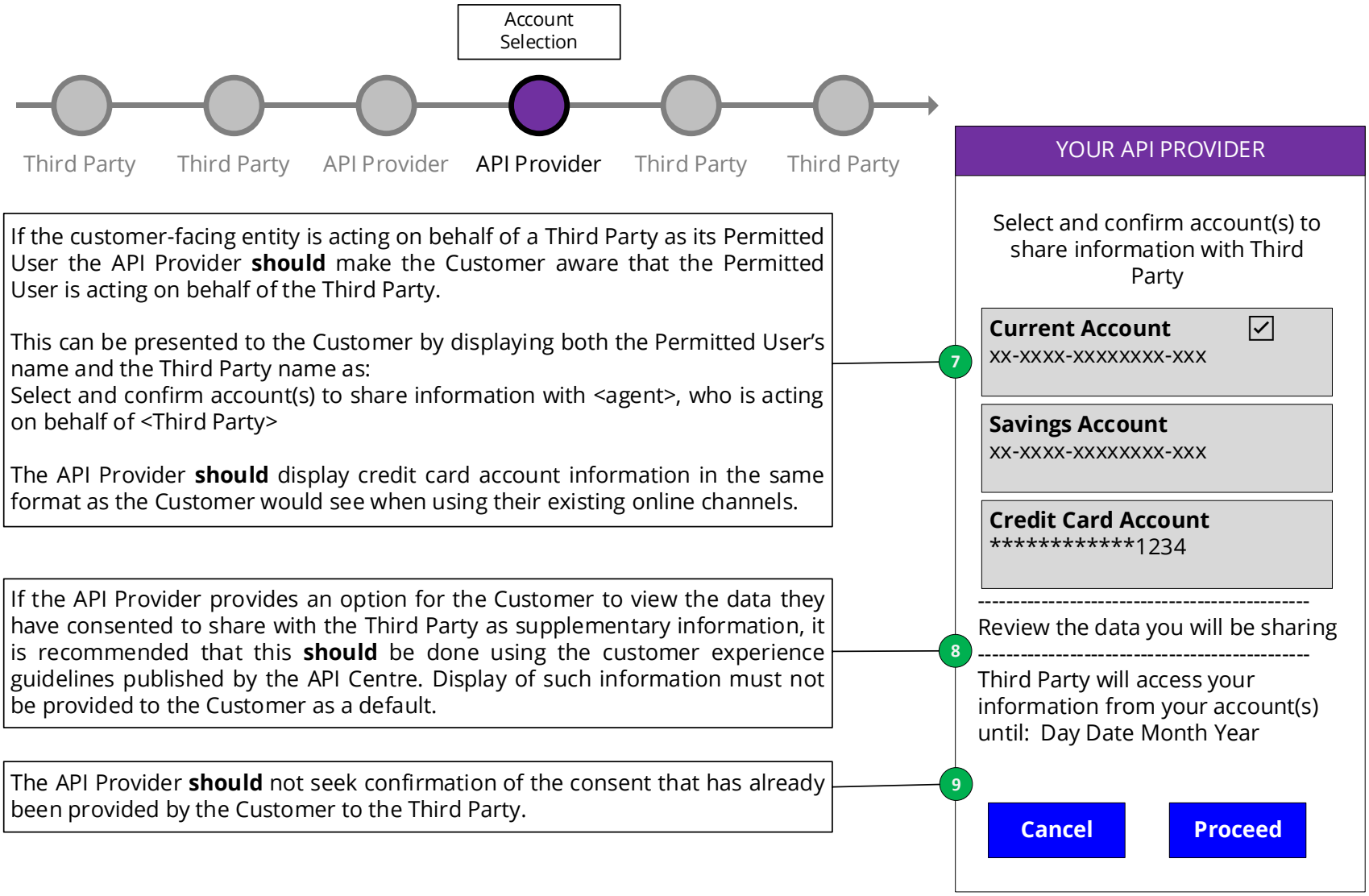
5



3.2.3.4.3 Authentication



3.2.3.4.4 Account selection



If the customer-facing entity is acting on behalf of a Third Party as its Permitted User the API Provider **should** make the Customer aware that the Permitted User is acting on behalf of the Third Party.

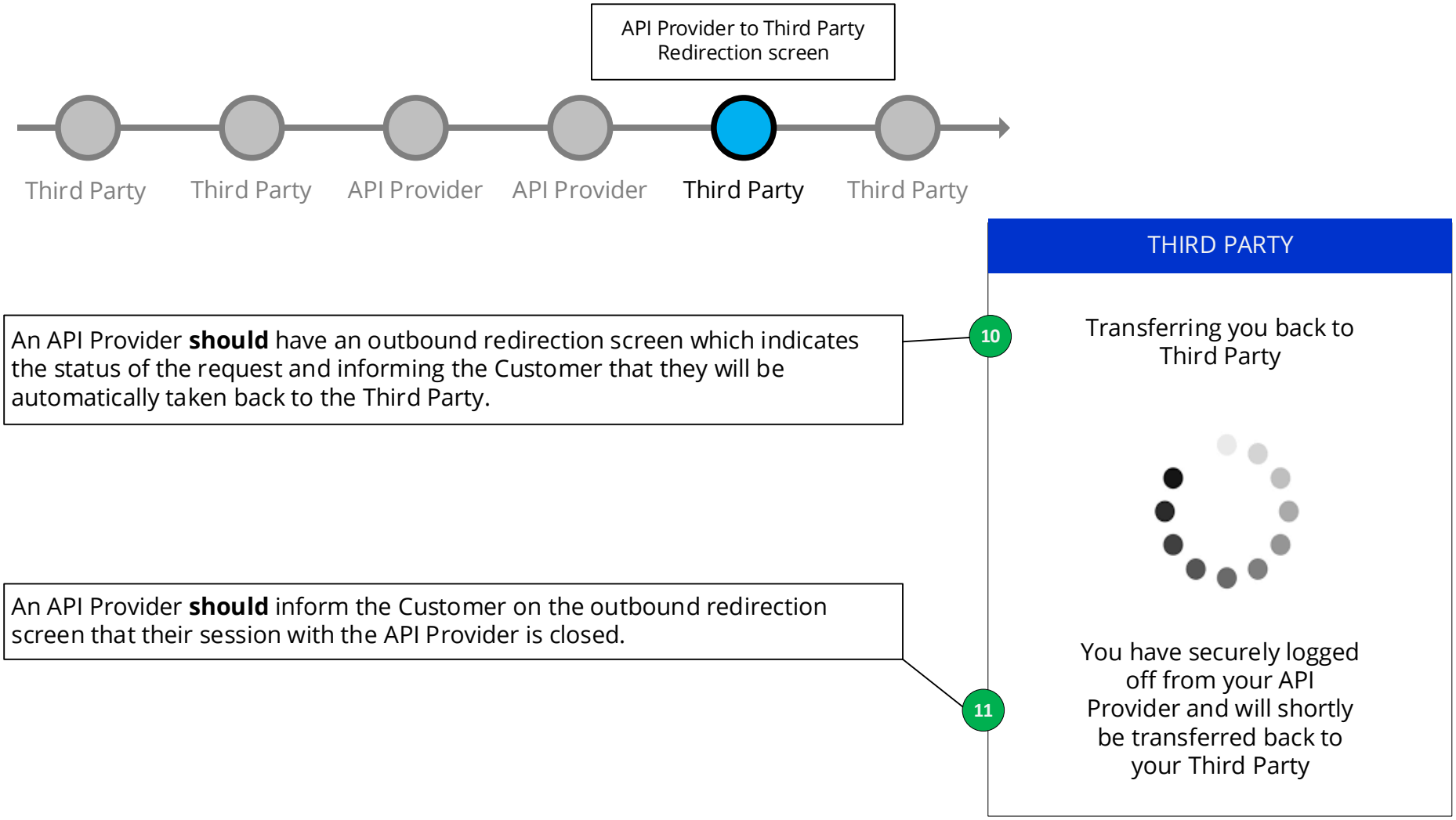
This can be presented to the Customer by displaying both the Permitted User's name and the Third Party name as:
Select and confirm account(s) to share information with <agent>, who is acting on behalf of <Third Party>

The API Provider **should** display credit card account information in the same format as the Customer would see when using their existing online channels.

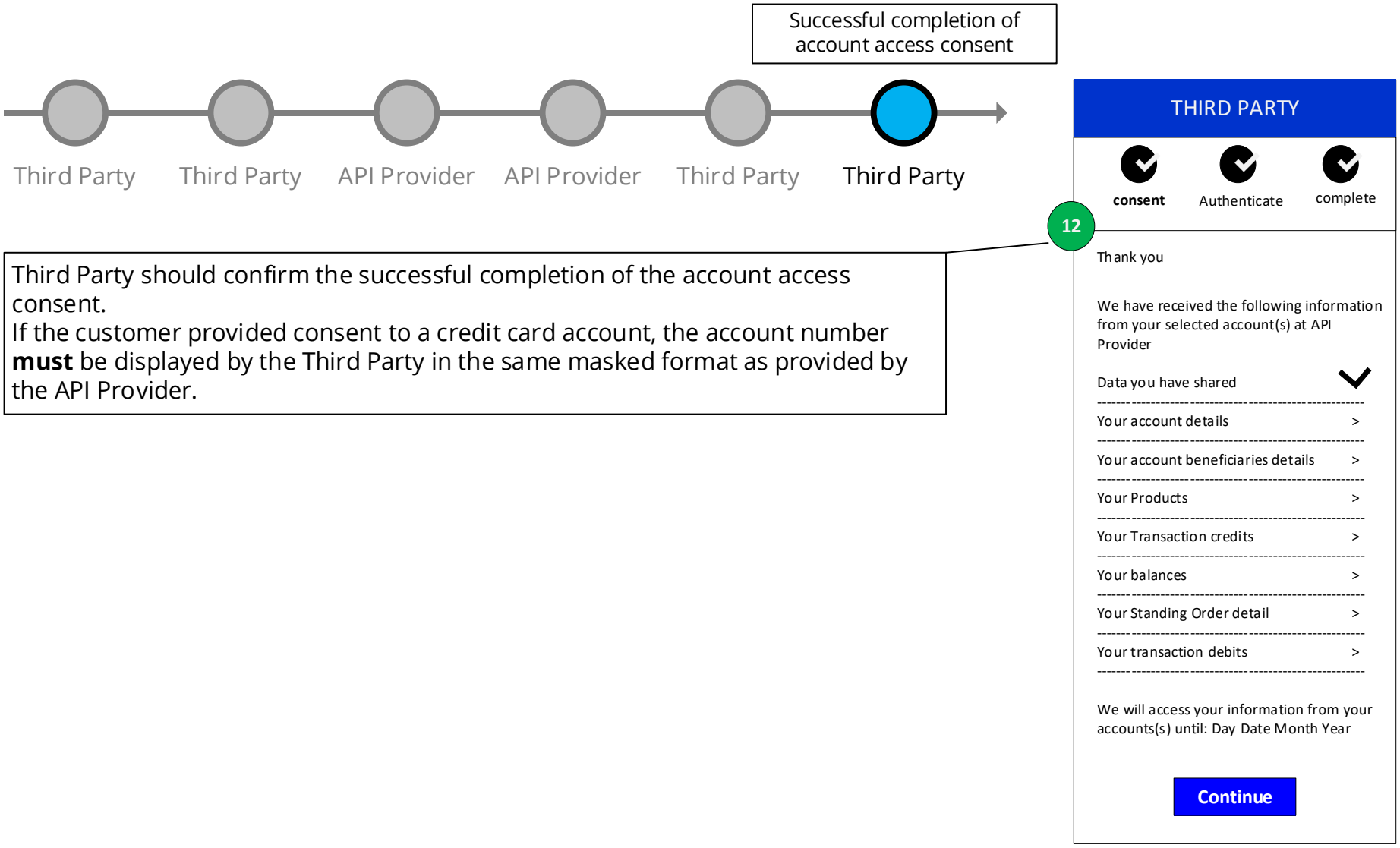
If the API Provider provides an option for the Customer to view the data they have consented to share with the Third Party as supplementary information, it is recommended that this **should** be done using the customer experience guidelines published by the API Centre. Display of such information must not be provided to the Customer as a default.

The API Provider **should** not seek confirmation of the consent that has already been provided by the Customer to the Third Party.

3.2.3.4.5 API Provider redirects to Third Party



3.2.3.4.6 Third Party confirmation



Third Party should confirm the successful completion of the account access consent.
If the customer provided consent to a credit card account, the account number **must** be displayed by the Third Party in the same masked format as provided by the API Provider.

3.2.4 App based redirection – Payment Initiation Services

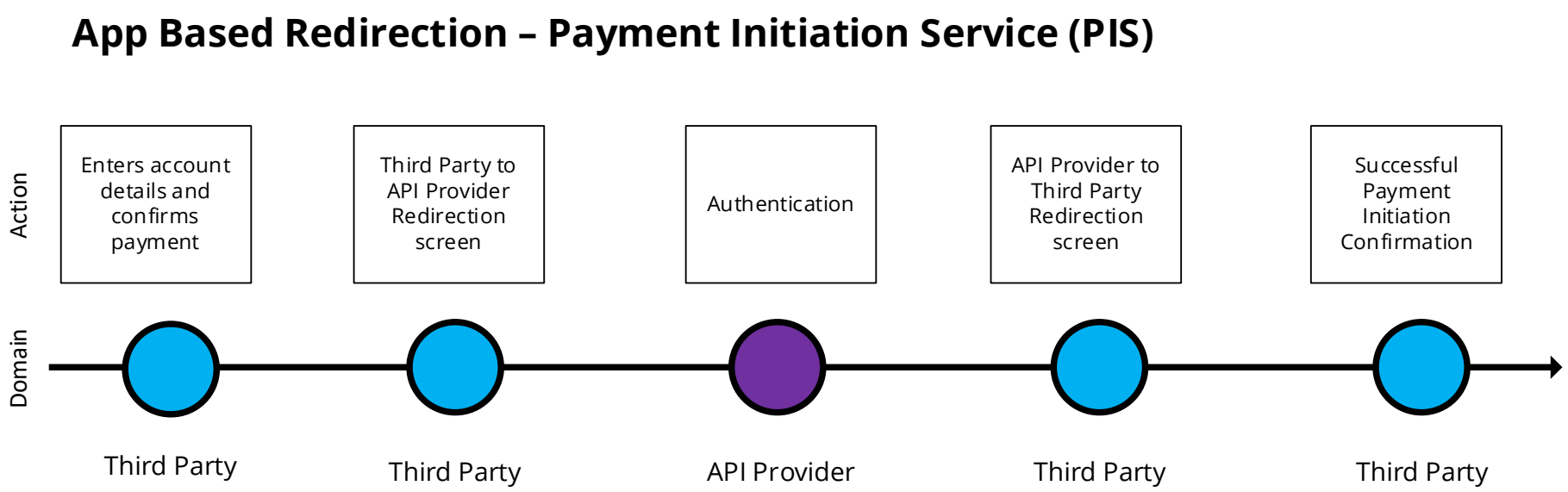
3.2.4.1 Journey description

Customer authentication, with the API Provider using the API Provider mobile app installed on the same device on which the Customer is consuming the Third Party service.

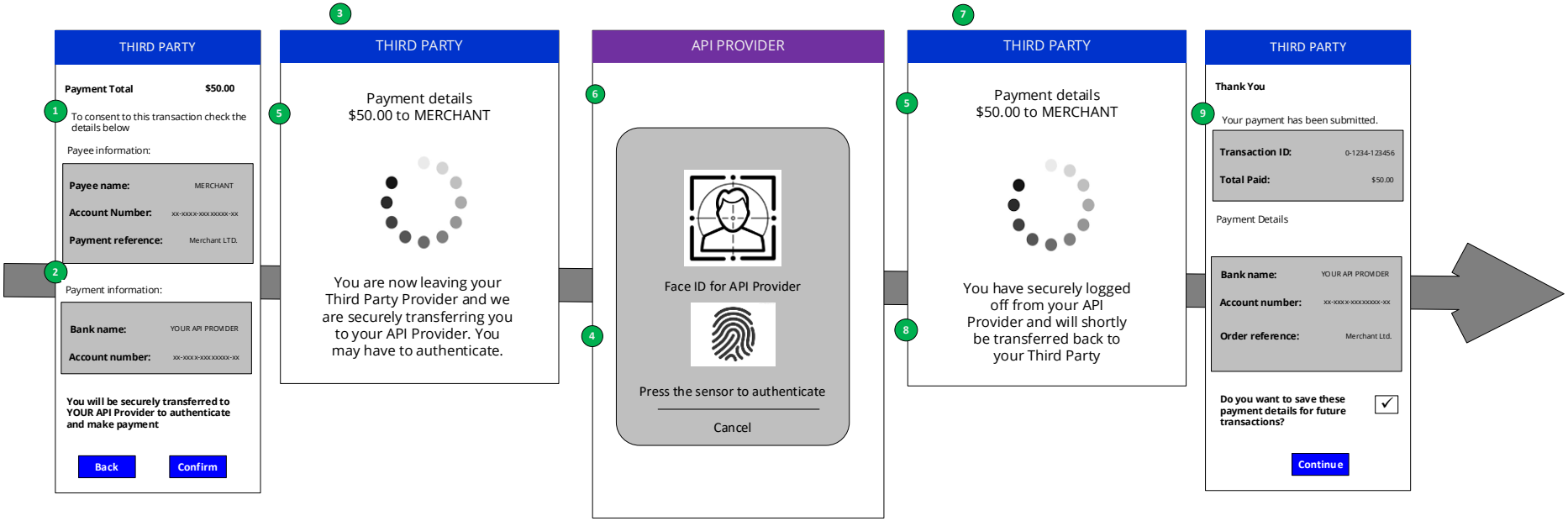
Enables the Customer to authenticate with the API Provider while using a Third Party for Payment Initiation Services, using the same API Provider app-based authentication method that they use when accessing the API Provider mobile channel directly and is appliable to both one time only payments initiation customer journeys as well as when establishing an Enduring Payment Consent.

The Third Party service could be web based or app based. The redirection should directly invoke the API Provider app to enable the Customer to authenticate and should not require the Customer to provide any Customer identifier or other credentials to the Third Party.

3.2.4.2 Journey map



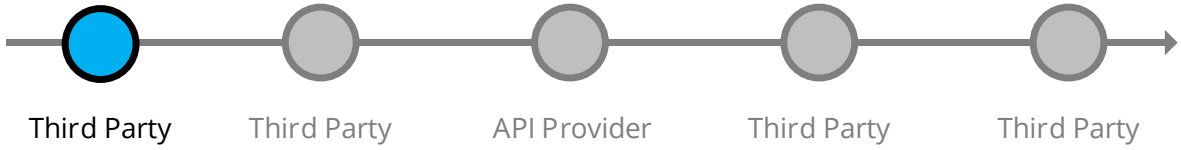
3.2.4.3 Wireframe journey



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

3.2.4.3.1 Customer payment account selection

Enters account details and confirms payment

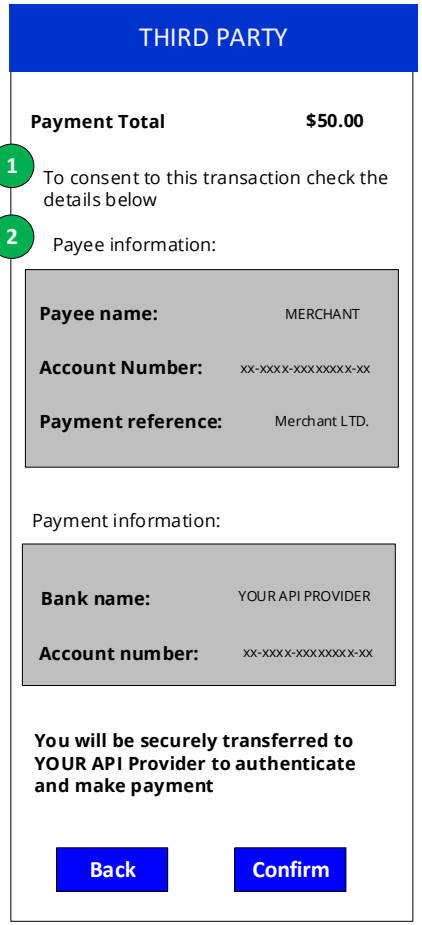


Customer Payment Account Selection

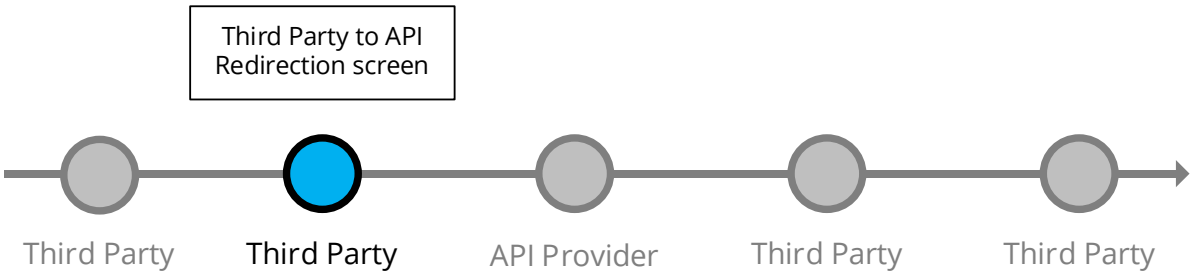
The Third Party **must** provide the Customer with at least one of the following options:

- Enter the Payer payment Account Identification details.
- Select their Account Identification details (this assumes they have been saved previously).

The Third Party **should** communicate information clearly to the Customer when obtaining consent in order to initiate the payment order.



3.2.4.3.2 Third Party redirects to API Provider

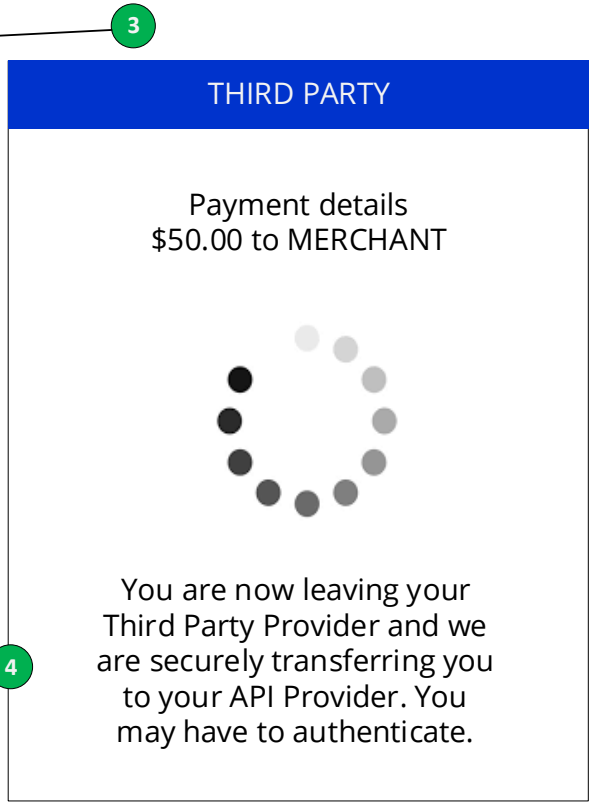


The Third Party **should** make the Customer aware through an inbound redirection screen that they are being taken to their API Provider for authentication to complete the payment.

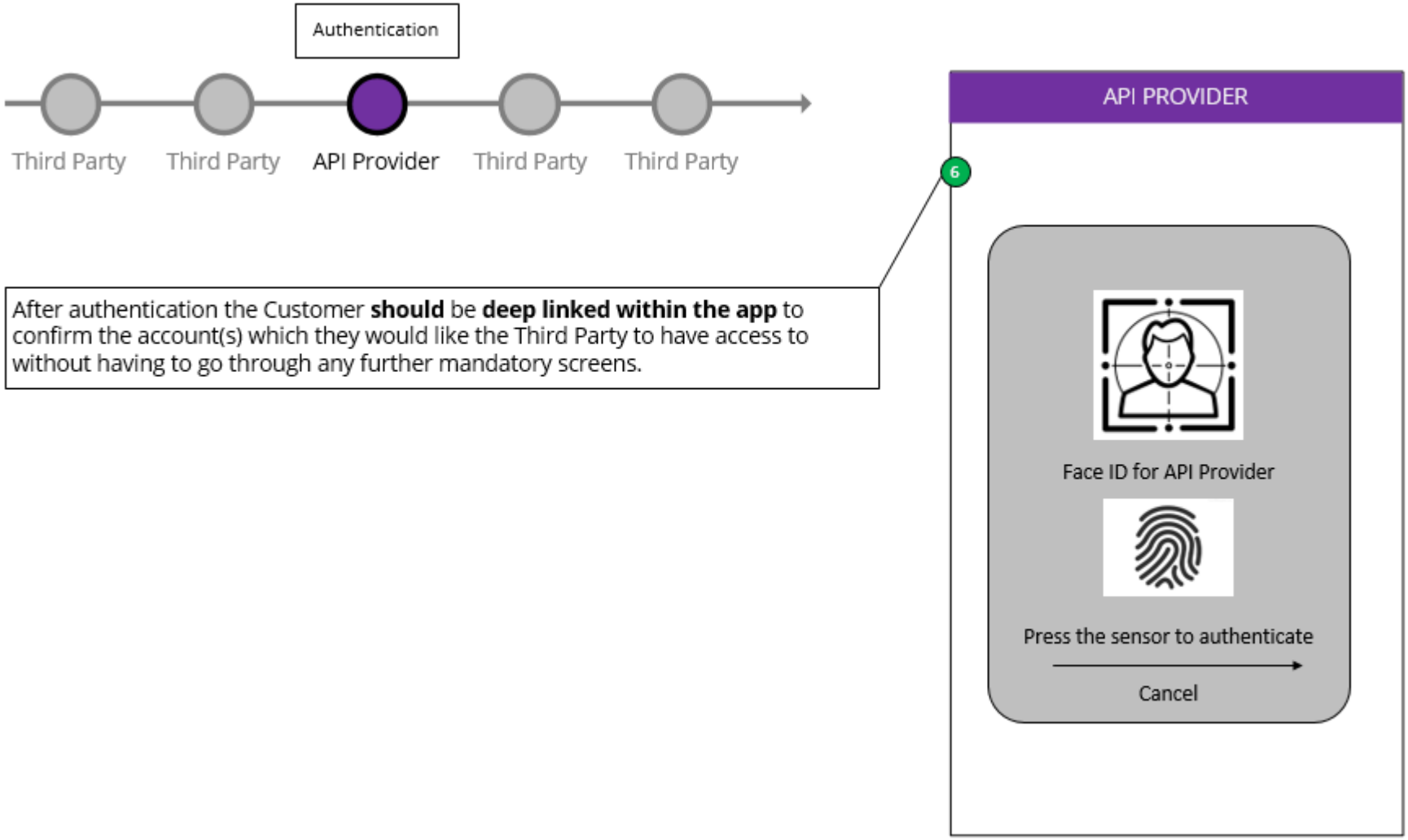
The Third Party **should** display in the Redirection screen the Payment Amount, Currency and the Payee Account Name to make the Customer aware of these details.

The redirection **should** take the Customer to an API Provider web page (desktop/ mobile) for authentication purposes only without introducing any additional screens.

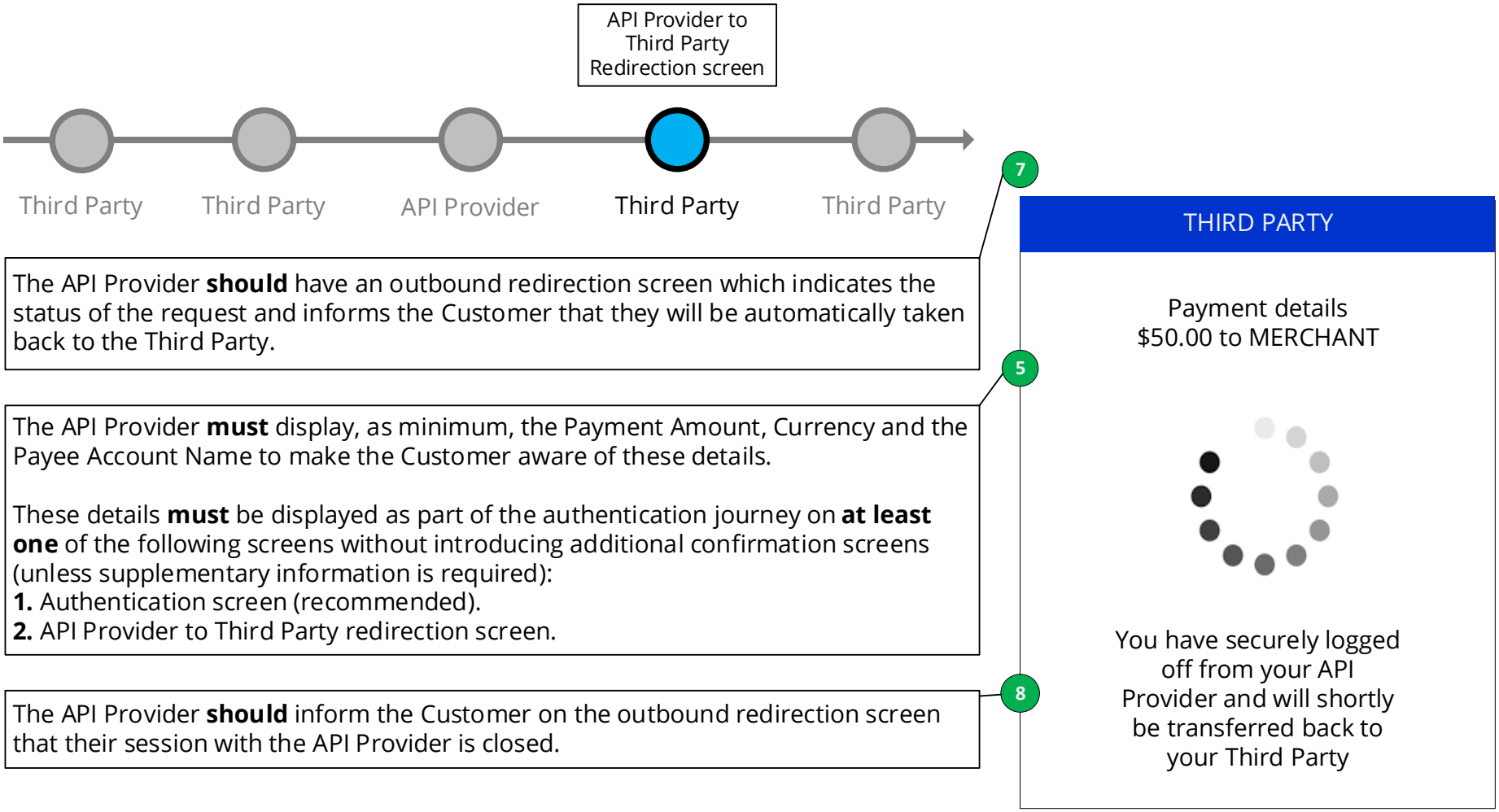
The web based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the web based API Provider channel (desktop/mobile).



3.2.4.3.3 Authentication



3.2.4.3.4 API Provider redirects to Third Party



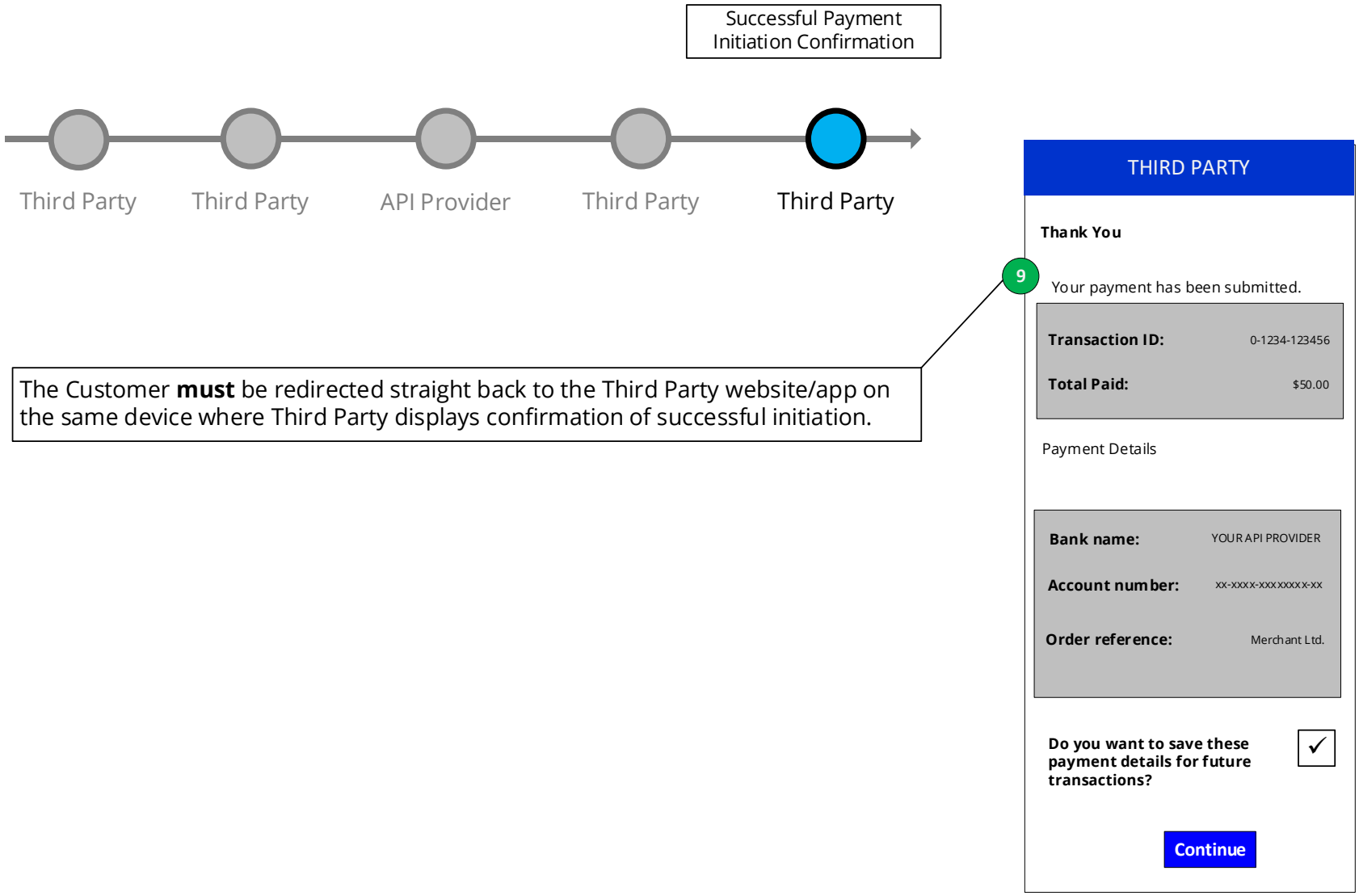
The API Provider **should** have an outbound redirection screen which indicates the status of the request and informs the Customer that they will be automatically taken back to the Third Party.

The API Provider **must** display, as minimum, the Payment Amount, Currency and the Payee Account Name to make the Customer aware of these details.

These details **must** be displayed as part of the authentication journey on **at least one** of the following screens without introducing additional confirmation screens (unless supplementary information is required):
1. Authentication screen (recommended).
2. API Provider to Third Party redirection screen.

The API Provider **should** inform the Customer on the outbound redirection screen that their session with the API Provider is closed.

3.2.4.3.5 Payment confirmation



3.3 App-to-browser redirection – Account Information Services

It is possible that a Customer using a mobile device does not have their API Provider mobile app installed, or their API Provider does not provide an app at all. In these instances, the Third Party app will need to launch the native mobile browser to present the Customer with their API Provider's web channel to authenticate.

3.4 Browser-to-app redirection

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

If a Customer is using a desktop to access the Third Party, then under the redirection model the journey will have to be completed on the API Provider browser channel. Only with “Decoupled authentication” (see 3.6) can the Customer use their app to authenticate in this situation.

3.5 Effective use of redirection screens

Within a typical journey, a Customer is presented with two redirection screens, at the Third Party first then followed by the API Provider:

1. First message that informs the Customer they are moving from the Third Party domain to the API Provider domain.
    - Happens after the Customer has provided consent to the Third Party for the account information or payment initiation service.
2. Second message that informs the Customer they are moving back from the API Provider domain to the Third Party domain.
    - Happens after the API Provider has authenticated the Customer and completed the authorisation of the action with the Customer.

Research carried out by OBIE has suggested that the redirection screens are an important part of the process, providing the Customer with trust in the process. The following reasons are noted:

1. Helps the Customer navigate their online journey by informing them of what is going to happen next.
2. Creates a clear sense of separation between the Third Party domain and the API Provider domain.
3. Reassures the Customer that they are in control and helps engender trust.

3.6 Decoupled authentication

A major addition to the API Standards for v2.0.0, known as “Decoupled” authentication, allows for the flow to be completed with a Customer using a separate secondary device to authenticate with the API Provider.

To enable the flow the Customer uses a separate secondary device to authenticate with the API Provider. This model allows for a number of innovative solutions and has the added benefit of being able to take advantage of biometrics for Strong Customer Authentication (SCA), where they may be engaging with a Third Party through a separate device, such as a Point of Sale (POS) device.

We have used examples for a Payment Initiation Service journey, but the same principles apply for all Account Information Service journeys.

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

3.6.1 Model A: Static Customer identifier

3.6.1.1 Journey description

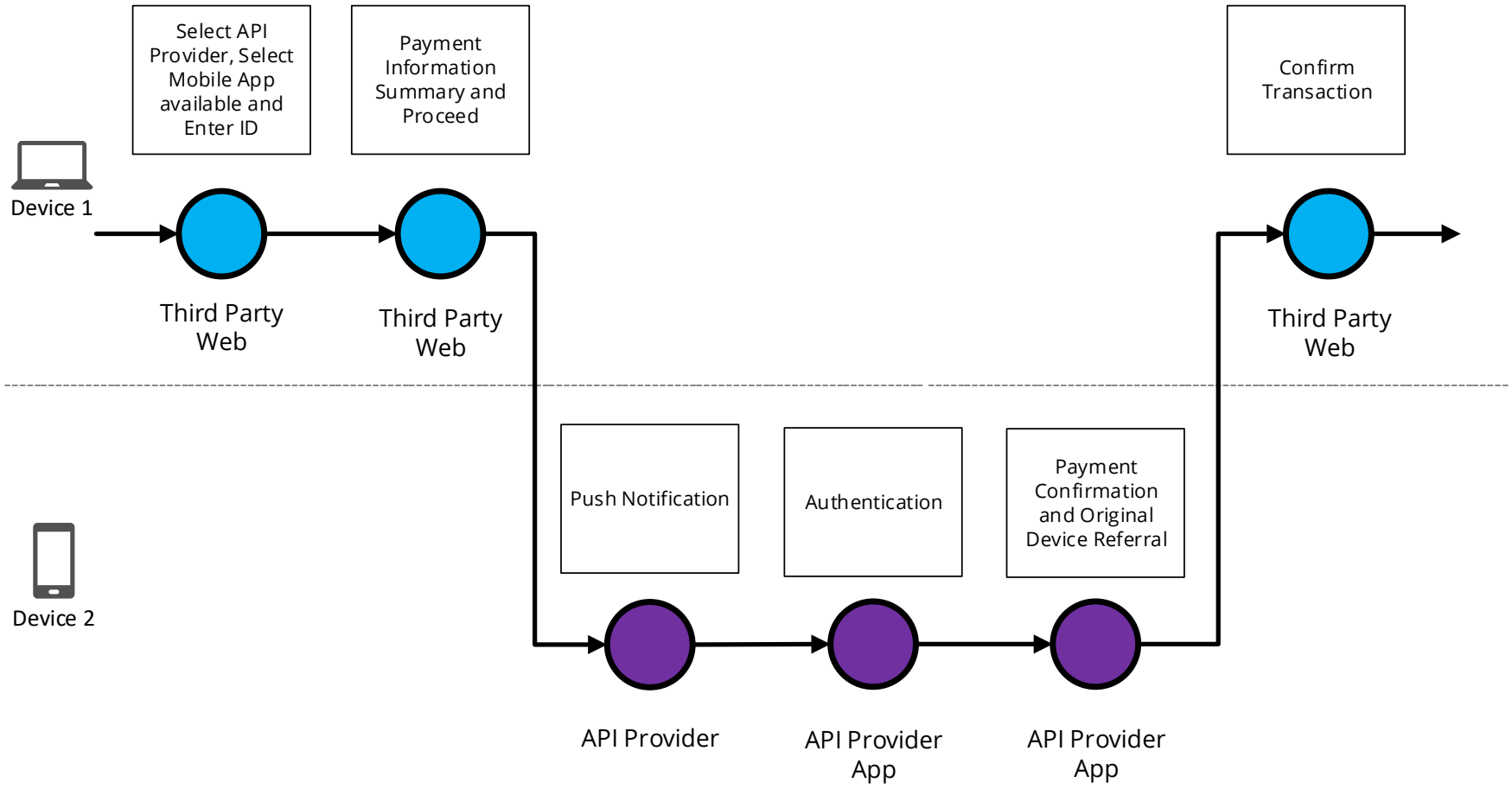
A Decoupled authentication flow, where the Customer provides a static identifier to the Third Party which is used by the API Provider to notify the Customer, such that the Customer can authenticate using the API Provider app on a separate device or mobile application.

This enables the Customer to use the same app-based authentication method with the API Provider they use when accessing the API Provider mobile app directly.

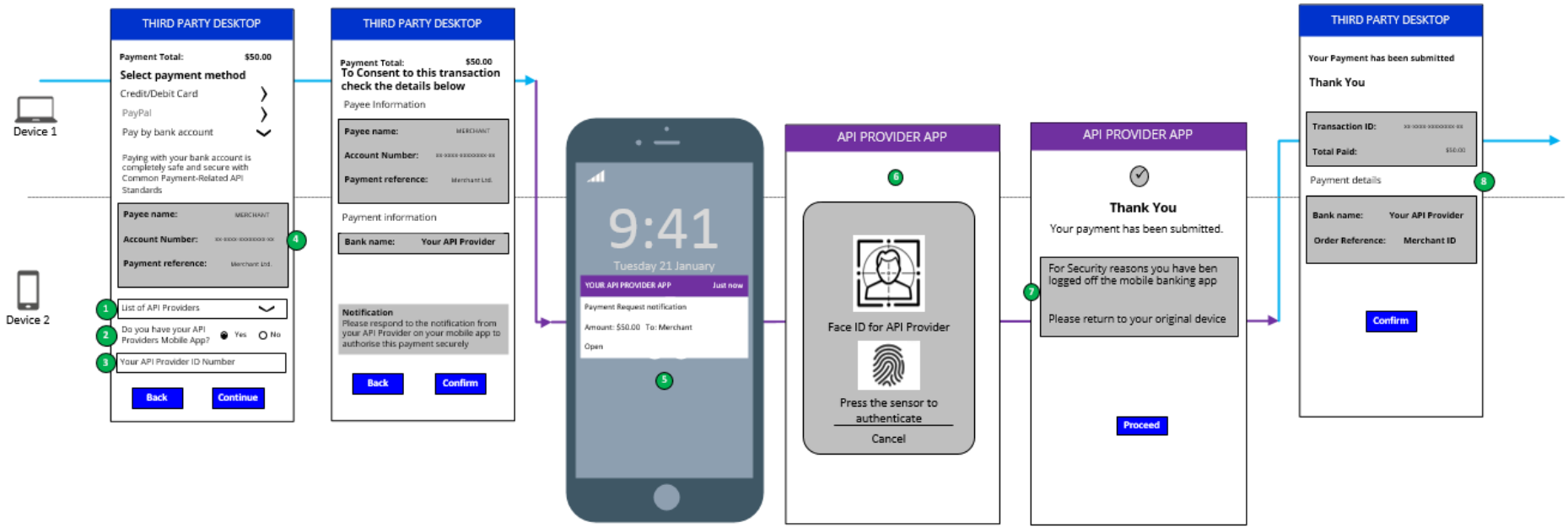
This model is best suited to Third Party apps with good user input options (e.g., website on PC/laptop), using a supported identifier, for example Customer phone number, email address, debit card number. The exact type of identifier supported by the API Provider should be published by the API Provider.

3.6.1.2 Journey map

Model A: Static Customer Identifier

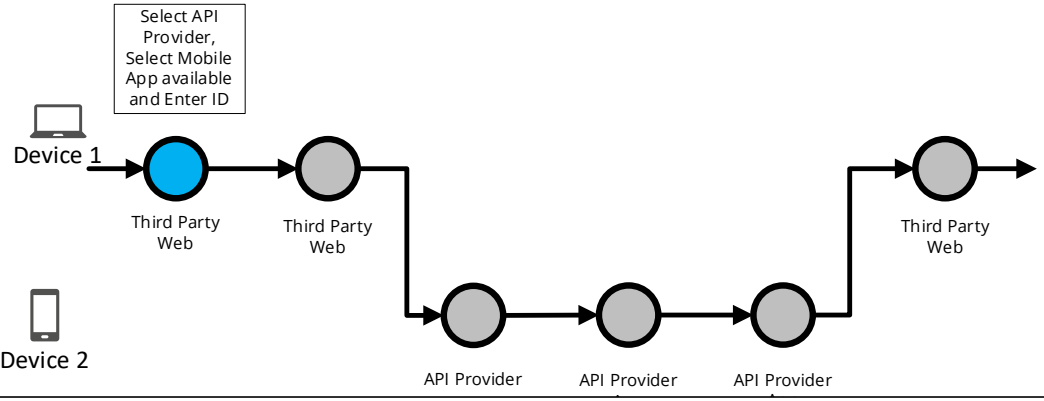


3.6.1.3 Wireframe journey



3.6.1.4 Wireframe annotations

3.6.1.4.1 Select API Provider



Customer payment Account Selection

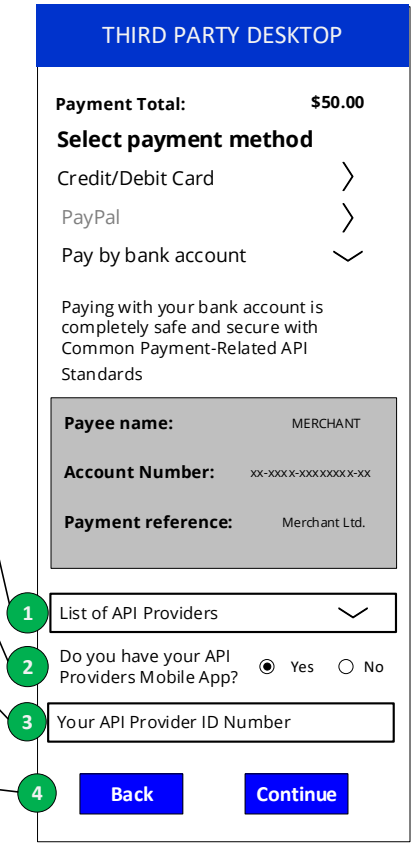
The Third Party **must** provide the Customer at least one of the following options:

- Enter their Payer payment Account Identification details.
- Select their Account Identification details (this assumes they have been saved previously).

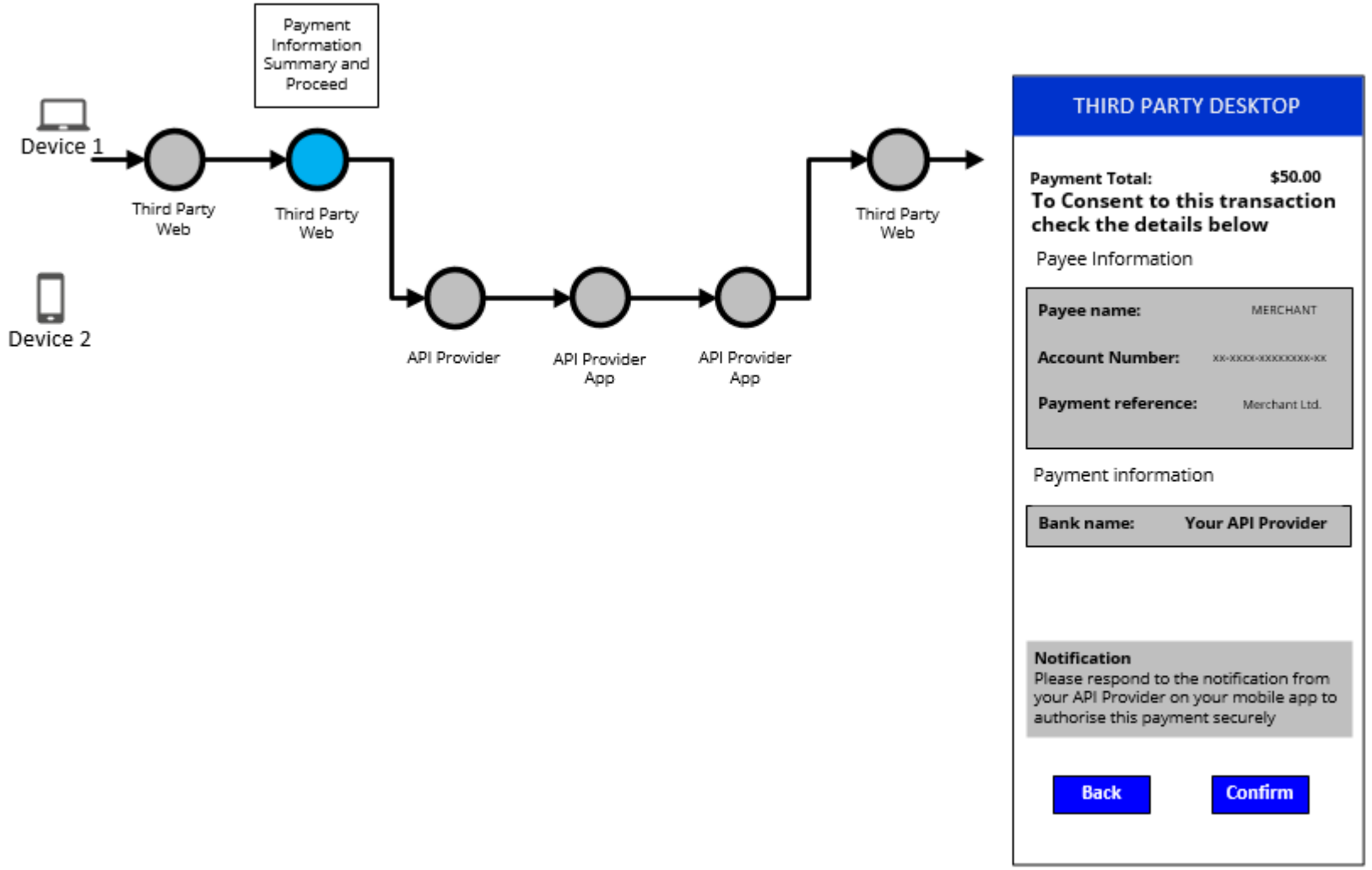
The Third Party **should** present the Customer with the authentication options supported by the API Provider which in turn can be supported by the Third Party device/channel (for e.g. a Third Party kiosk that can only support authentication by API Provider mobile app).

If a Third Party and API Provider support Model A, then the Third Party **should** request from the Customer the identifier which is supported by their API Provider.

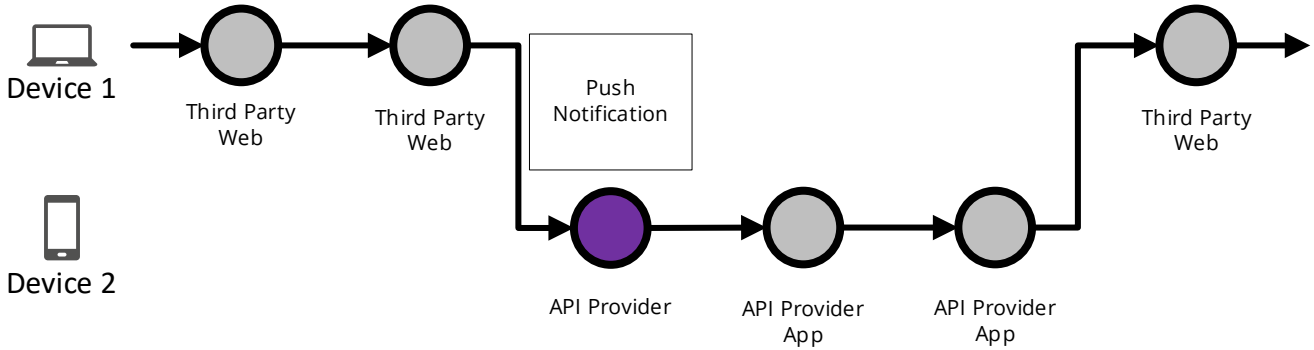
The Third Party **should** make the Customer aware about how this identifier will be used.



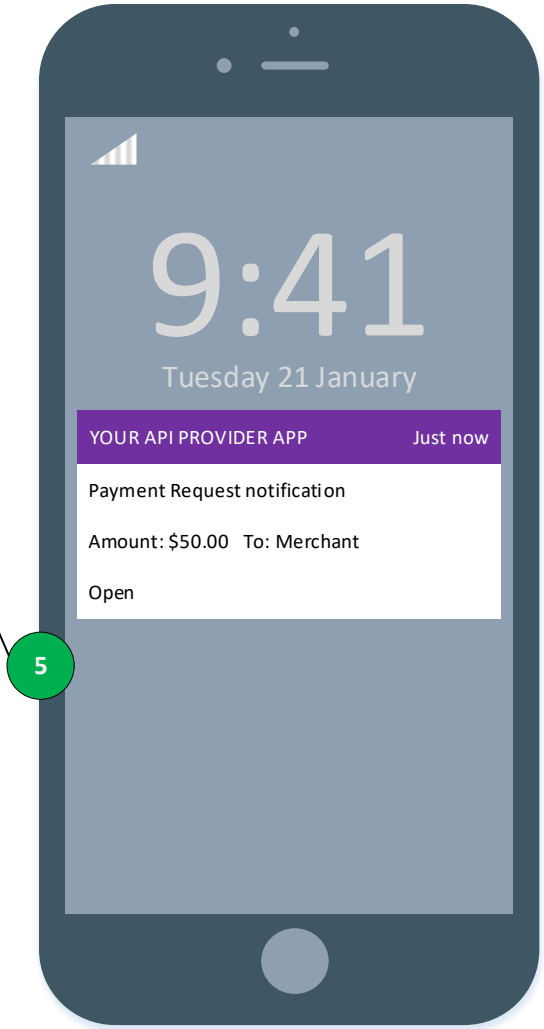
3.6.1.4.2 Payment information summary and proceed



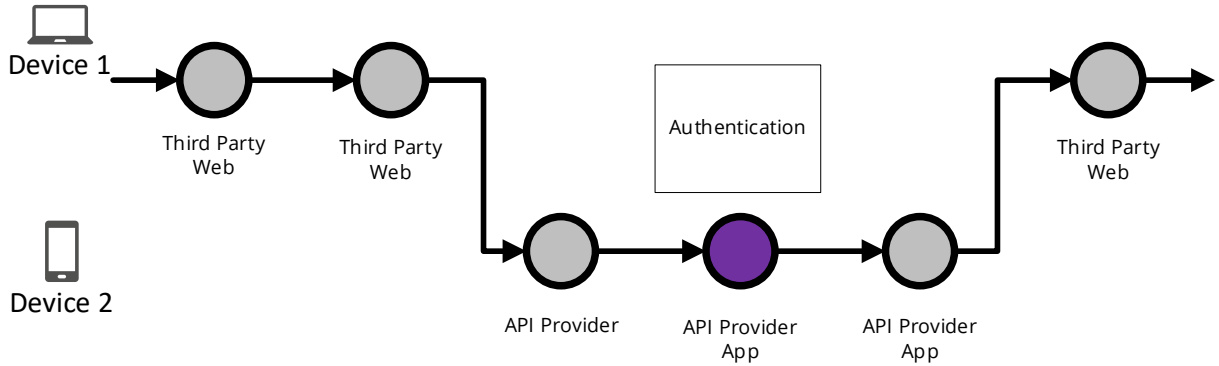
3.6.1.4.3 Push notifications



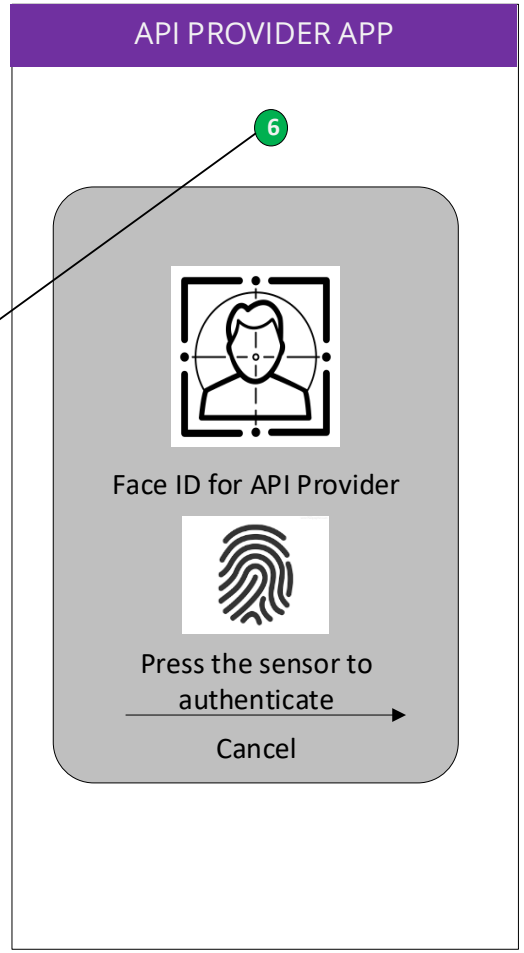
After the Customer enters the specified identifier, if the Customer has an API Provider app then the API Provider **must** notify the customer through the API provider app for authentication purposes, without introducing any additional screens. The notification **must** clearly mention the payment request with the amount and the payee



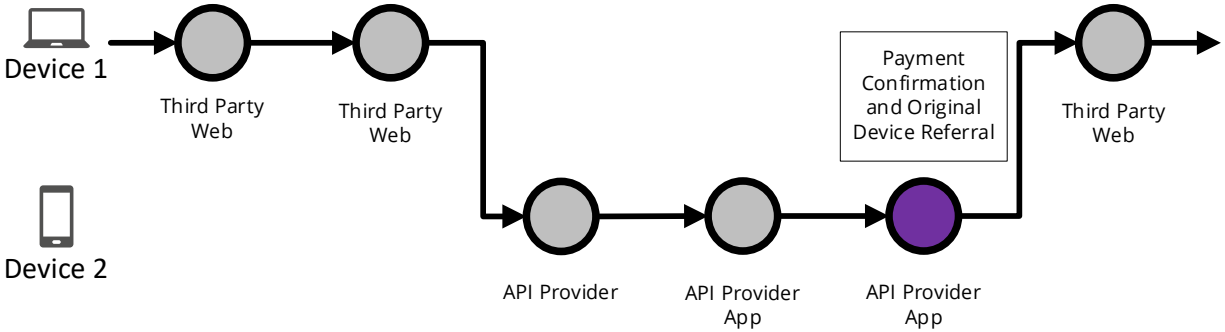
3.6.1.4.4 Authentication



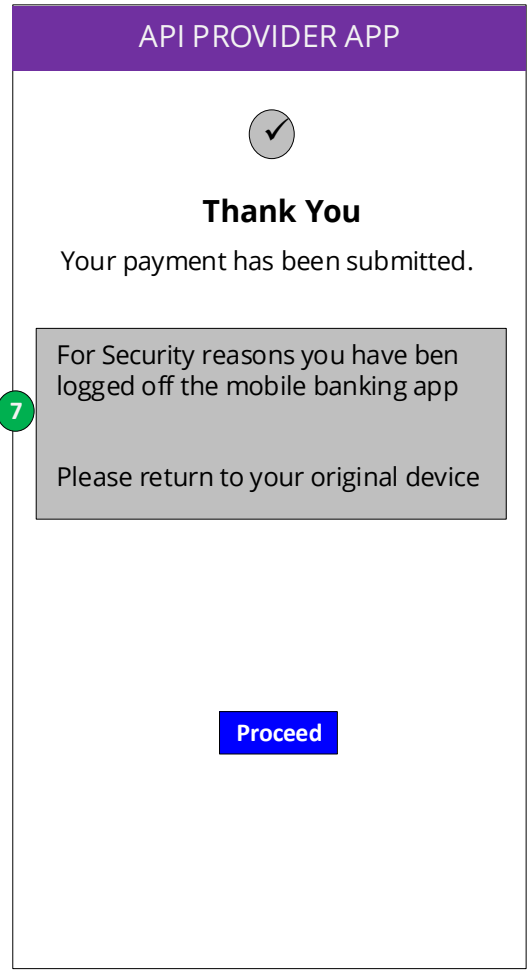
The API Provider app based authentication **should** have no more than the number of steps the Customer would experience when directly accessing the API Provider mobile app (biometric, passcode, credentials) and these screens **should** be the same steps where possible to do so.



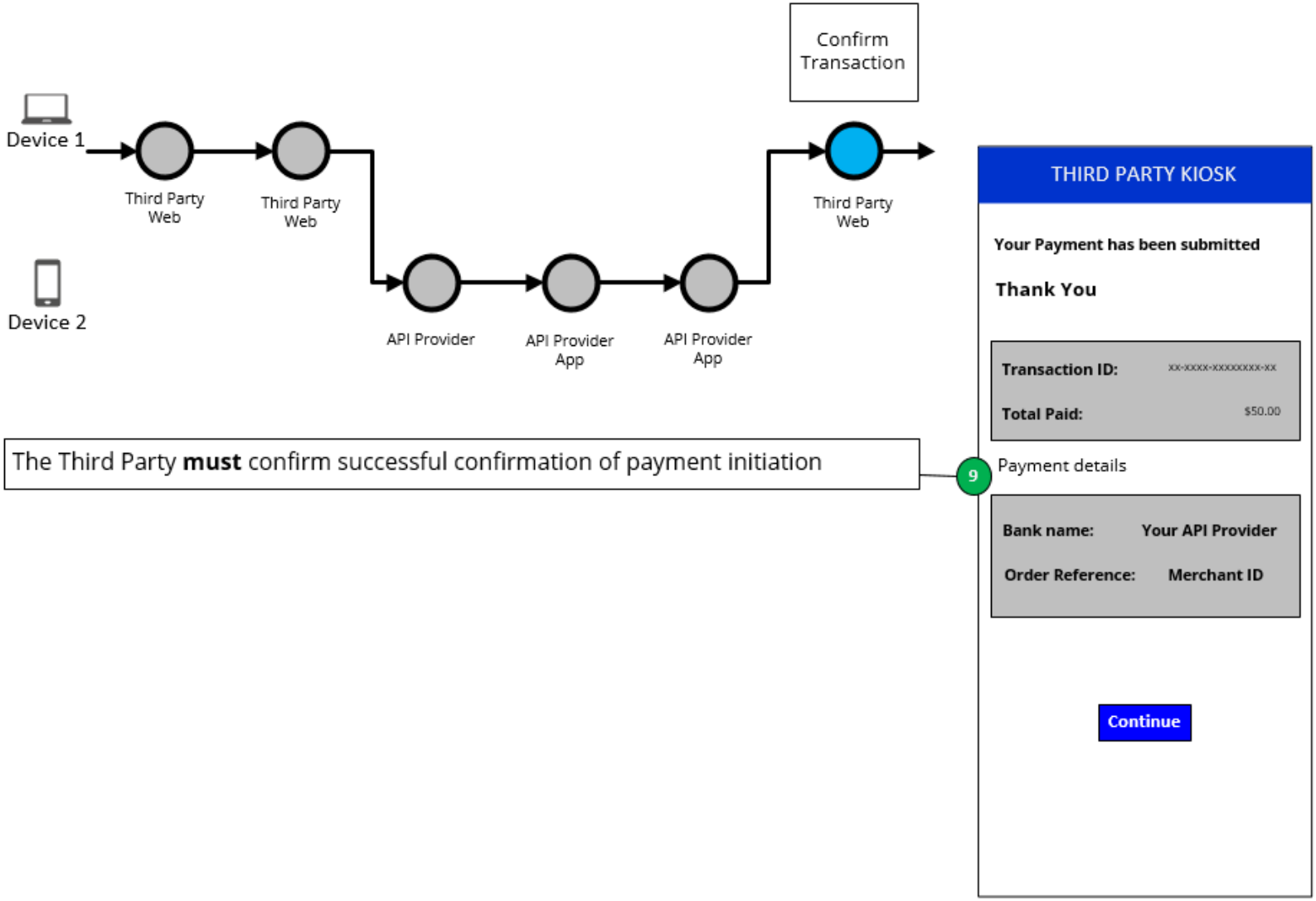
3.6.1.4.5 Payment confirmation



If the Customer is logged off from the API Provider app, the API Provider **should** make the Customer aware that they have been logged off and notify them to check back on the originating Third Party app.



3.6.1.4.6 Confirm transaction



3.6.2 Model B: API Provider generated identifier

3.6.2.1 Journey description

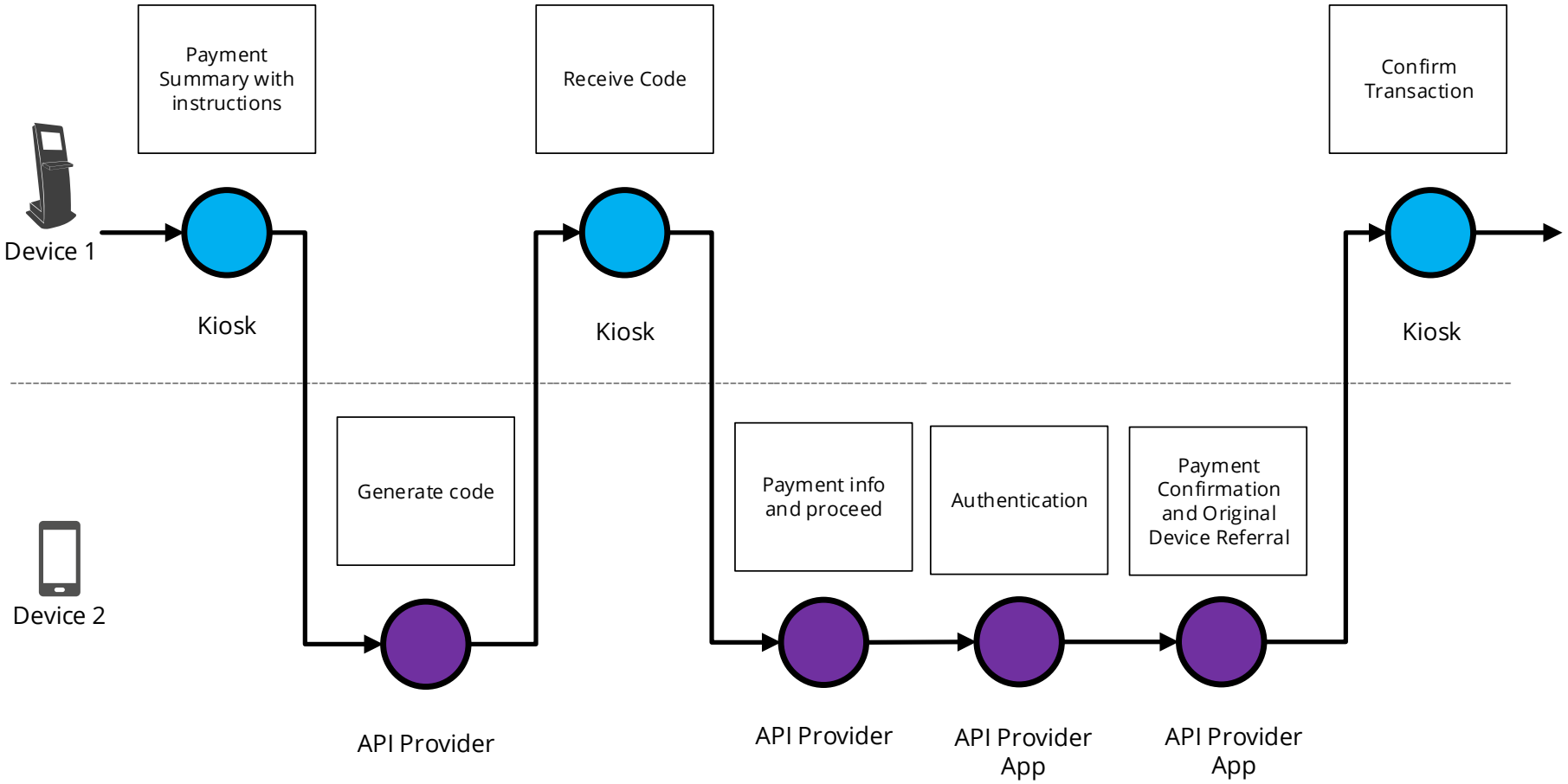
A Decoupled authentication flow where the Customer provides a dynamic identifier generated with their API Provider to the Third Party which is then used by the API Provider to identify the Customer through the API Provider app to authenticate and action the Third Party request.

This model is best suited to a Third Party app that can "capture" the code from the API Provider app (e.g., by scanning a QR code).

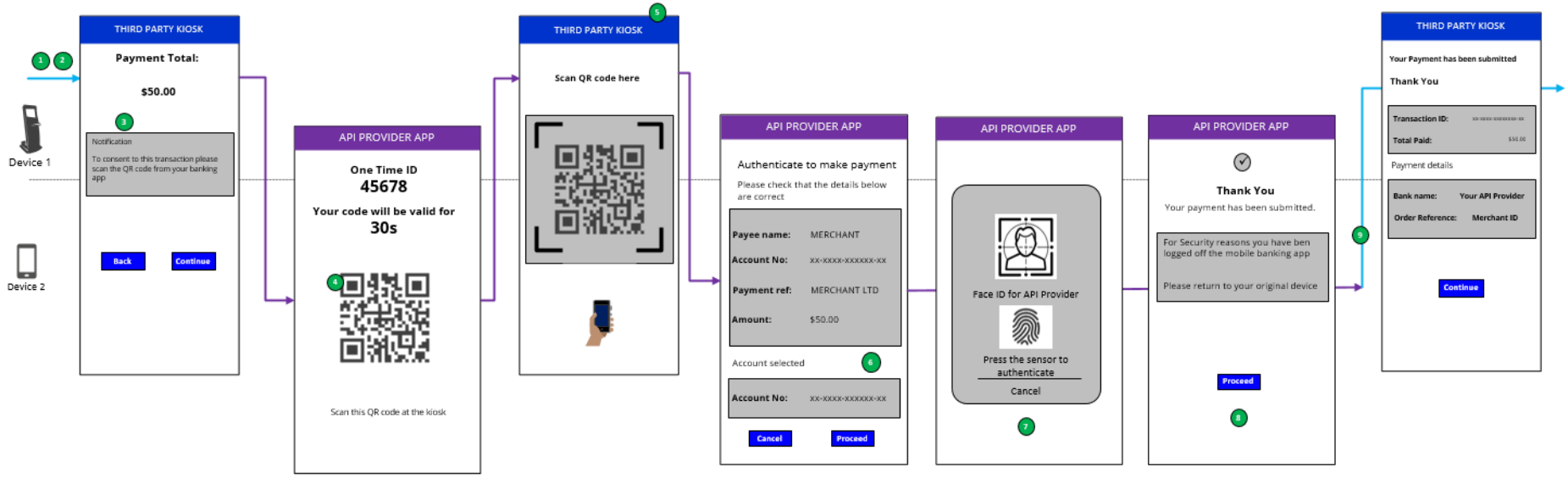
Alternatively, the Customer can be prompted to type in an identifier in the Third Party App. This may however be a long series of characters and may result in a sub-optimal Customer experience.

3.6.2.2 Journey map

Model B: API Provider Generated Identifier

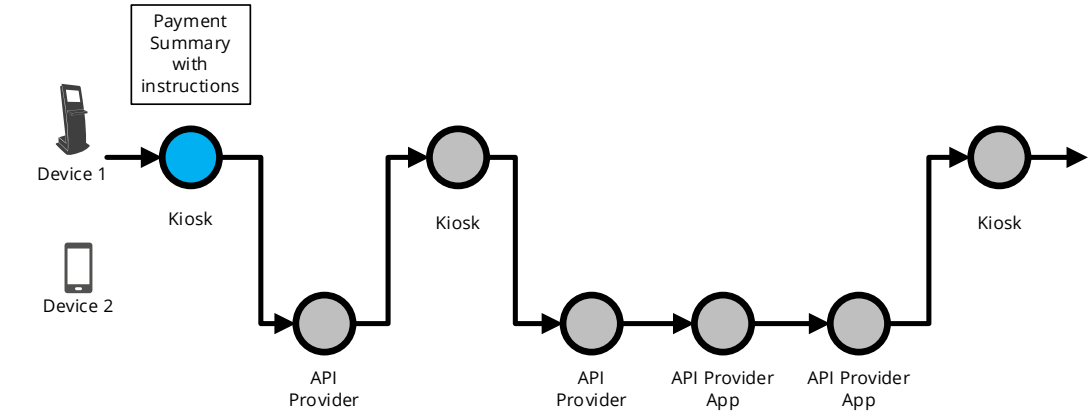


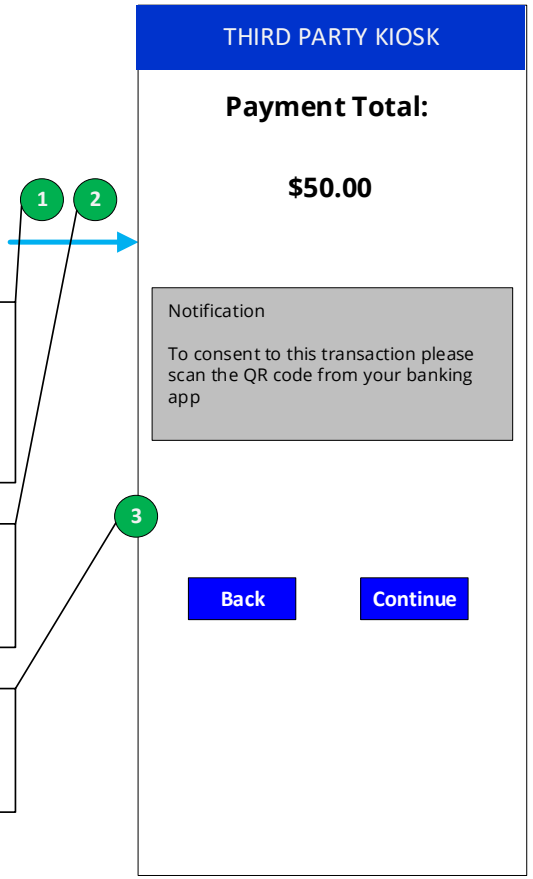
3.6.2.3 Wireframe journey



3.6.2.4 Wireframe annotations

3.6.2.4.1 Payment summary





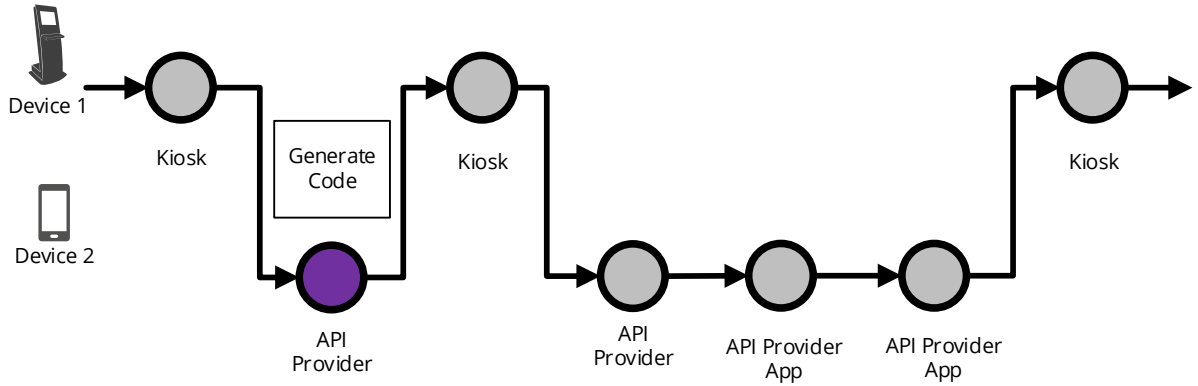
<u>Customer payment Account Selection</u>
A Third Party **should** provide the Customer with either / both of the following options:

- Enter their Payer payment account identification details.
- Select their Account Identification details (this assumes they have been saved previously).

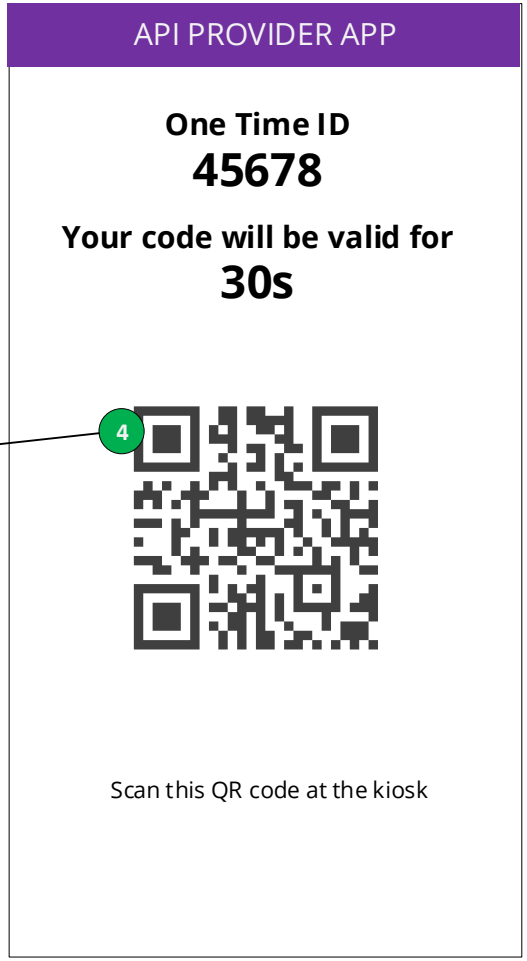
A Third Party **should** present the Customer with the authentication options supported by the API Provider which in turn can be supported by the Third Party device/channel (for e.g. A Third Party kiosk that can only support authentication by API Provider mobile app).

If a Third Party and API Provider support Model B then the Third Party **should** provide the Customer information on how the identifier can be generated with their API Provider and make the Customer aware about how this identifier will be used

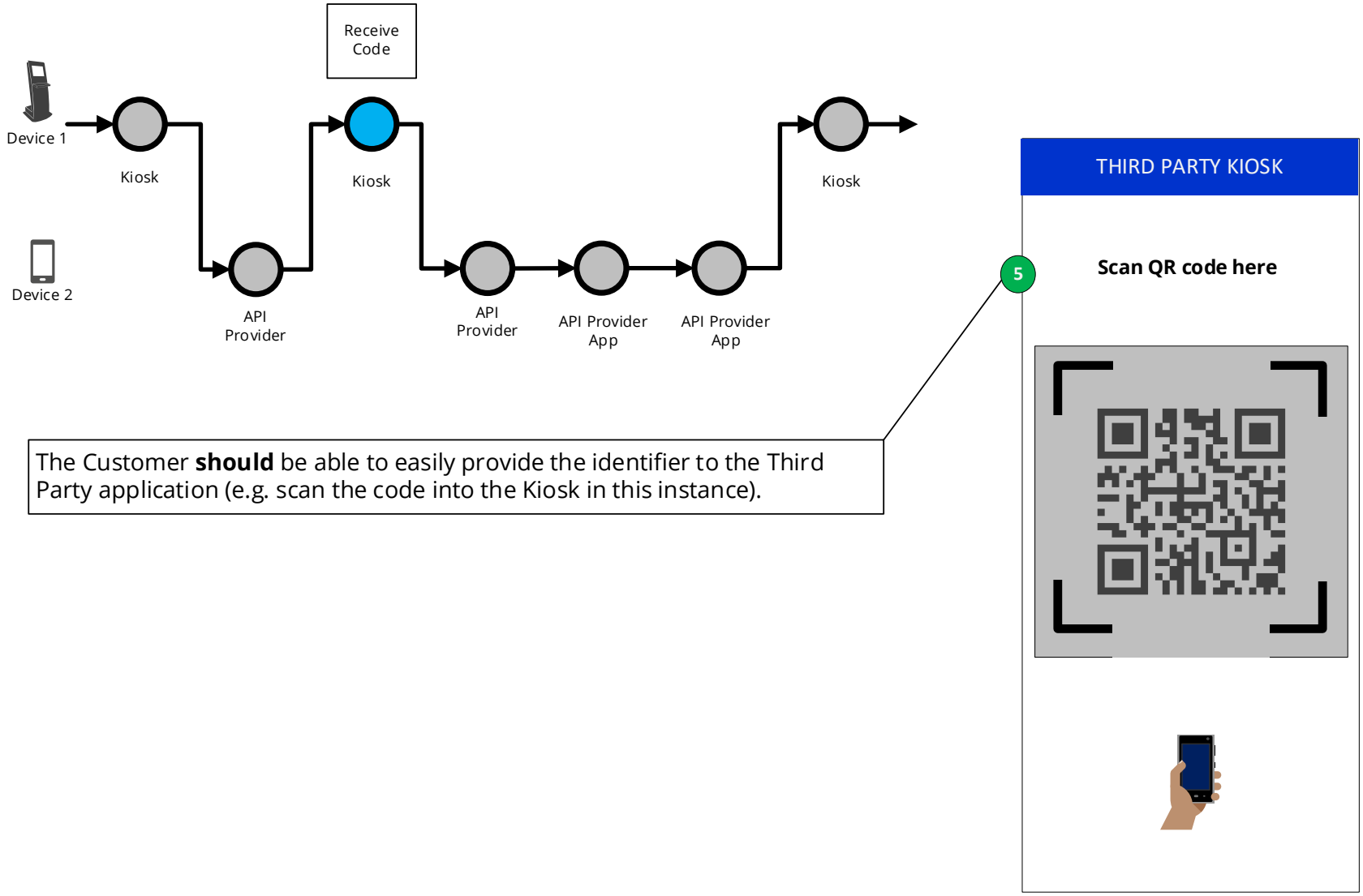
3.6.2.4.2 Generate code



The Third Party **should** make the Customer aware about how this identifier will be used.

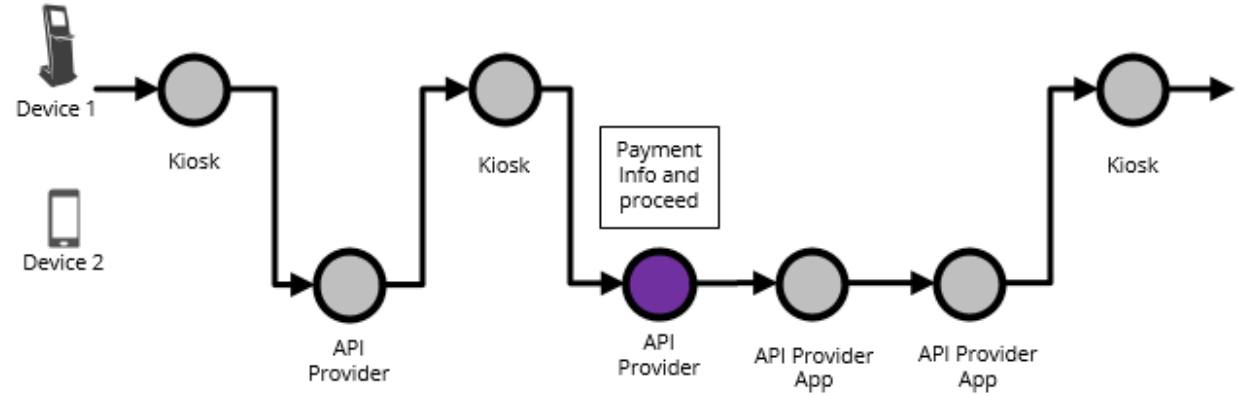


3.6.2.4.3 Receive code

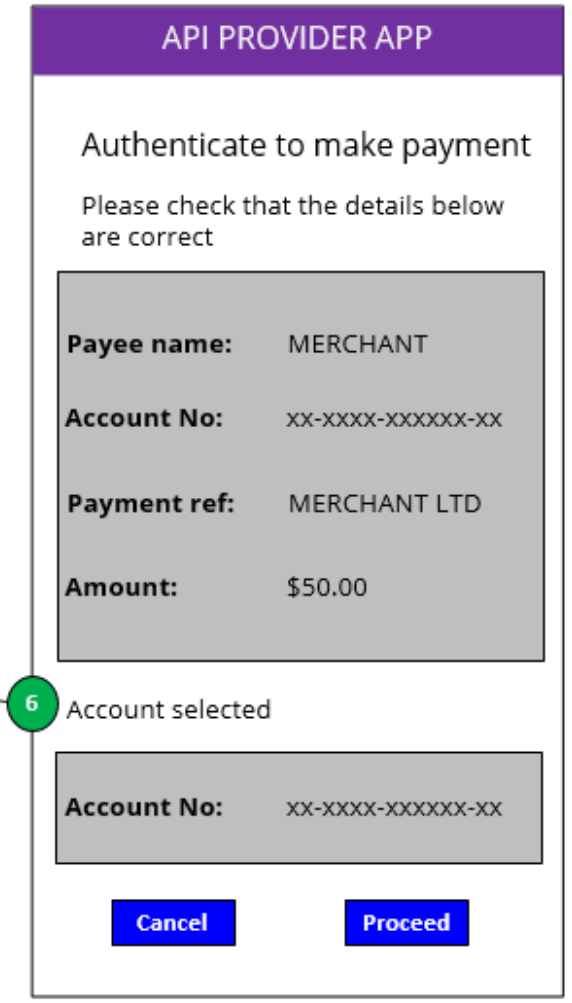


The Customer **should** be able to easily provide the identifier to the Third Party application (e.g. scan the code into the Kiosk in this instance).

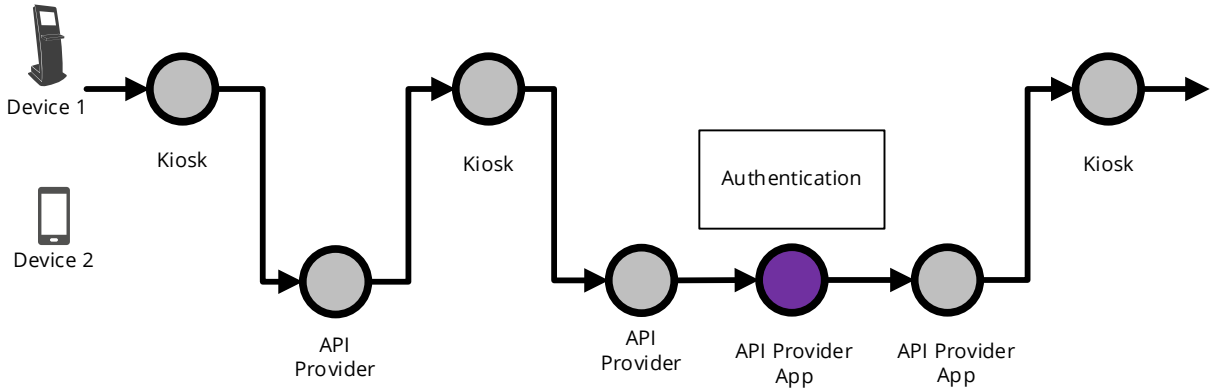
3.6.2.4.4 Payment information and proceed



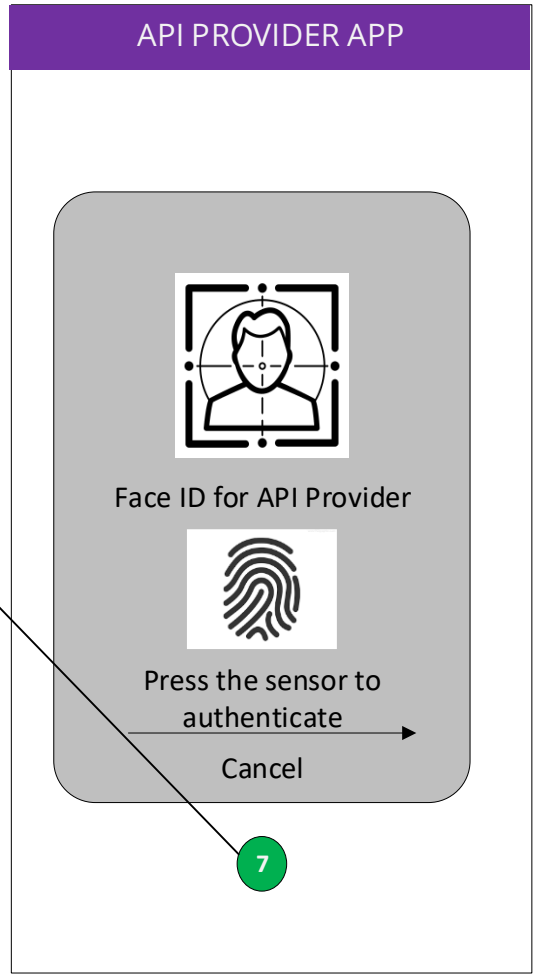
After the Customer provides the API Provider app generated identifier to the Third Party, then the API Provider **must** display the payment request within the same session of the API Provider app and clearly mention the amount and the payee.



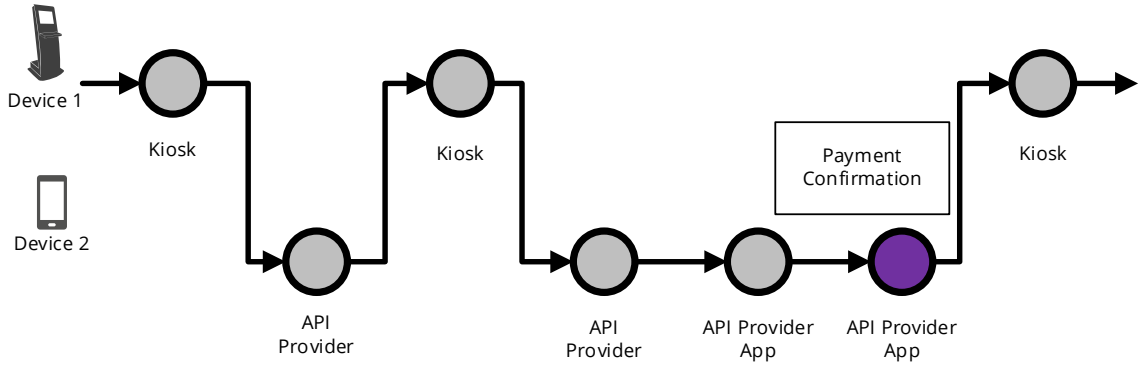
3.6.2.4.5 Authentication



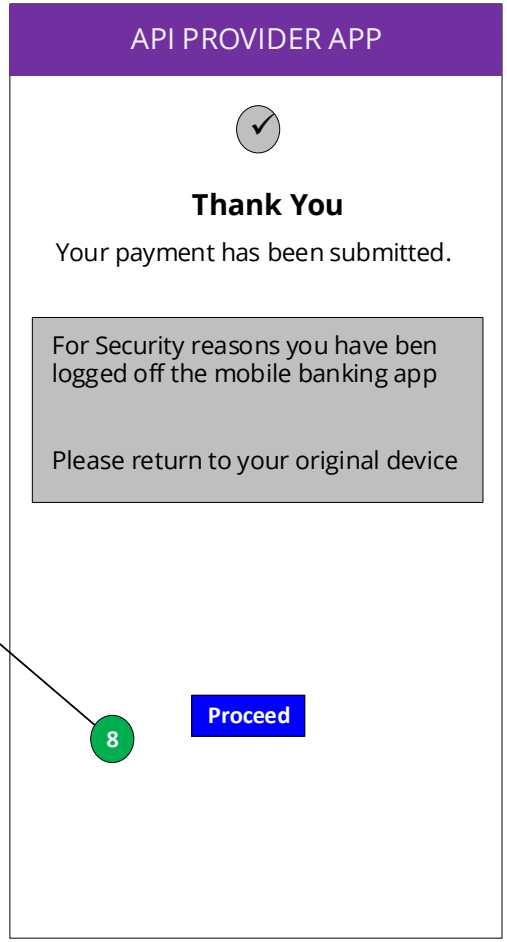
The API Provider **should** apply SCA which **should** have no more than the number of steps that the Customer would experience when directly accessing the API Providers mobile app (biometric, passcode, credentials).



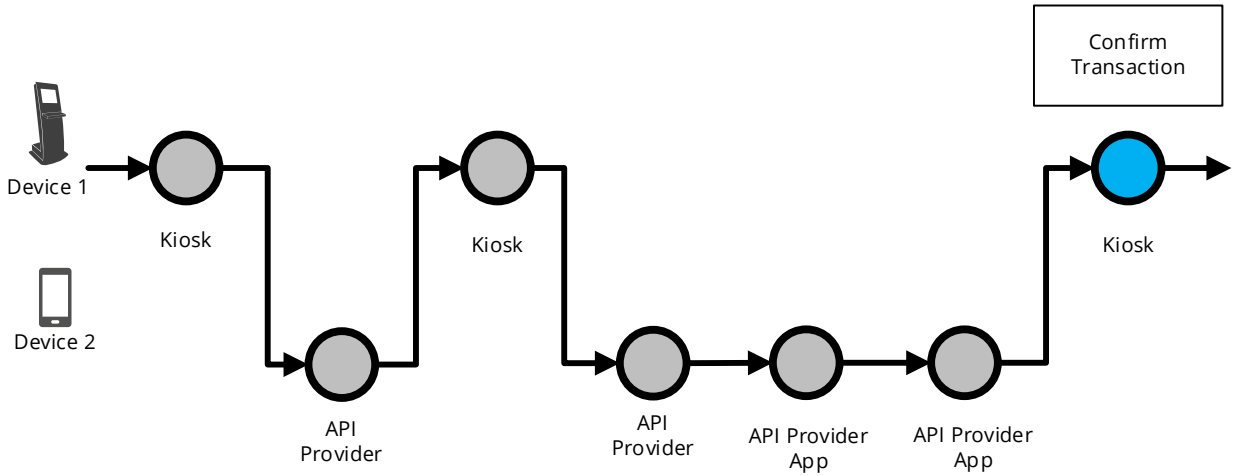
3.6.2.4.6 Payment confirmation



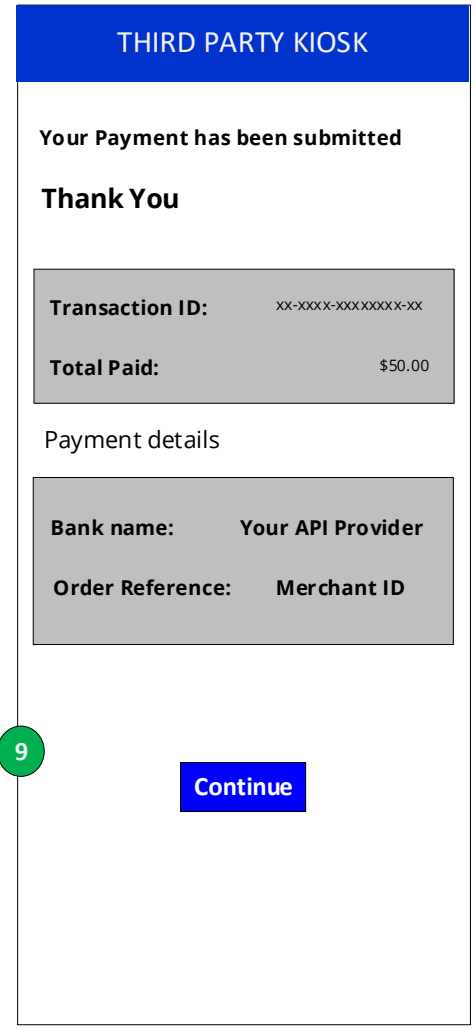
An API Provider **must** make the customer aware that they have been logged off from the API Provider app and notify them to check back on the originating Third Party app.



3.6.2.4.7 Confirm transaction



The Third Party **must** confirm successful confirmation of payment initiation.



3.6.3 Model C: Third Party generated identifier

3.6.3.1 Journey description

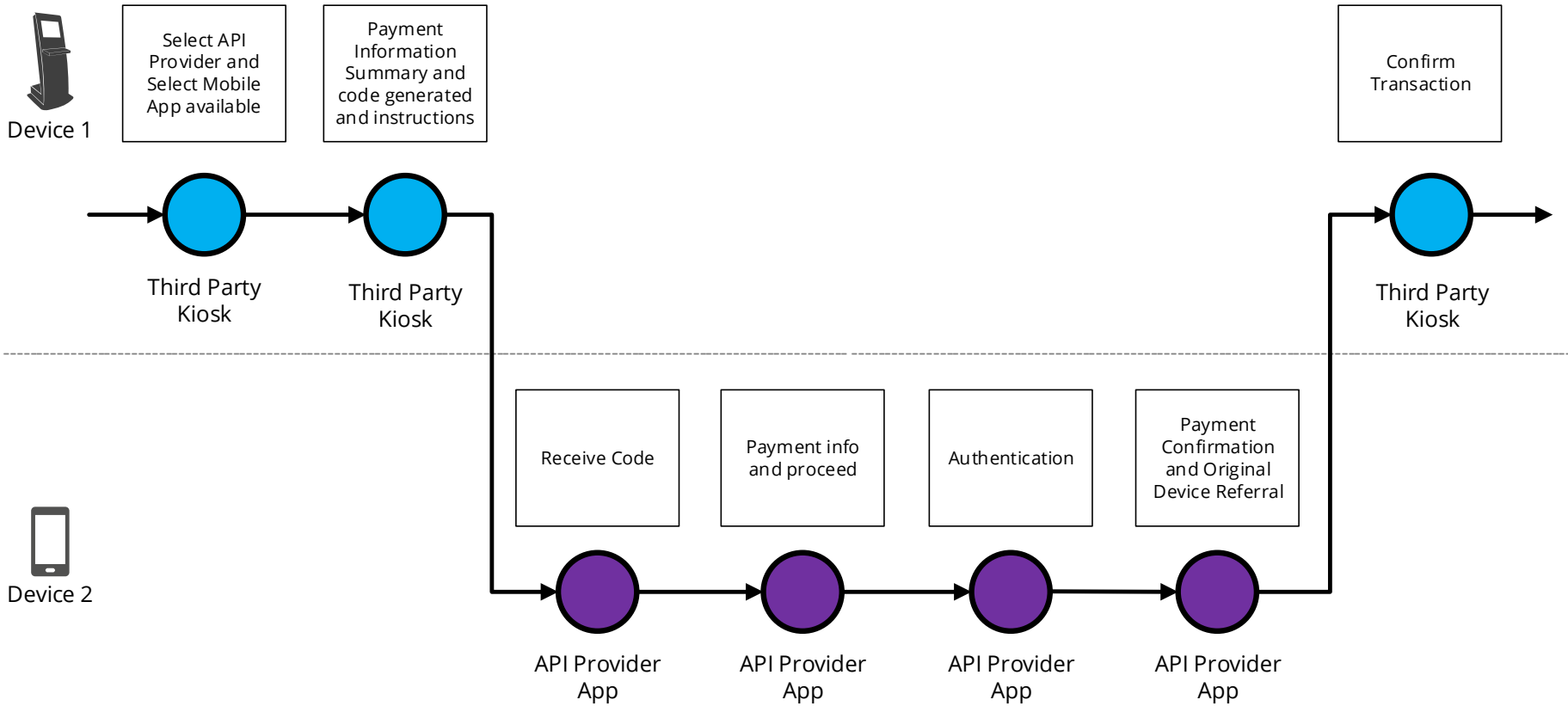
A Decoupled authentication flow where the Customer is provided with an identifier generated by the Third Party, which is then used by the API Provider to identify the Customer through the API Provider app to authenticate and action the Third Party request.

This model is best suited to a Third Party app that provides a QR code to all API Providers to "capture" the code from the API Provider app (e.g., by scanning a QR code).

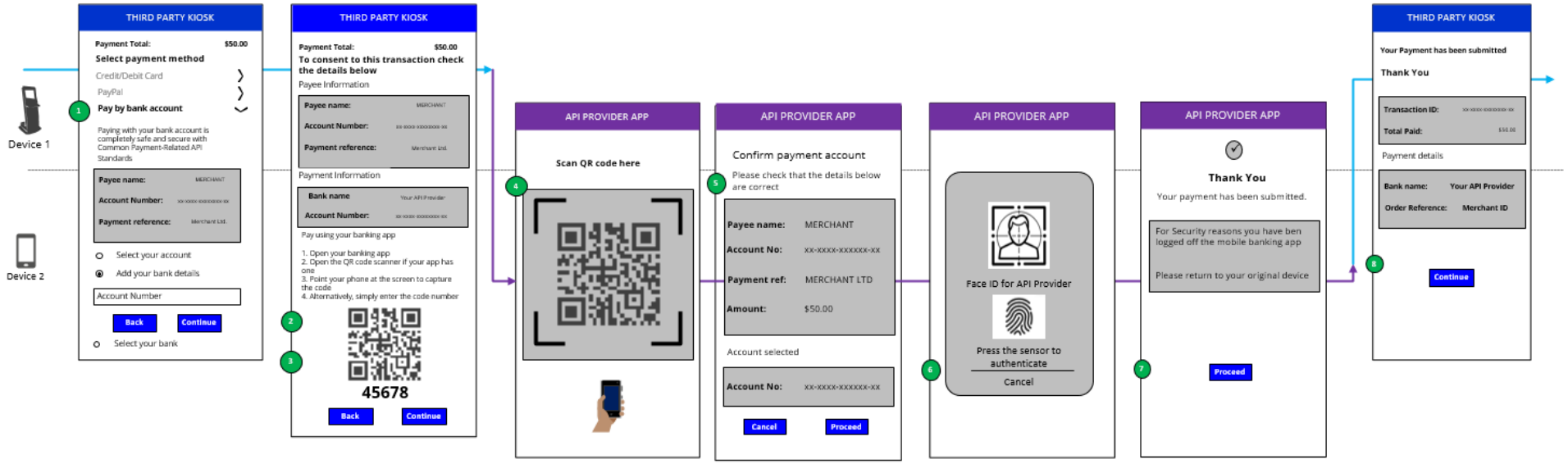
Alternatively, the Customer can be prompted to type in an identifier in the API Provider app. This may be a long series of characters and may result in a sub-optimal Customer experience.

3.6.3.2 Journey map

Model C: Third Party Generated Identifier

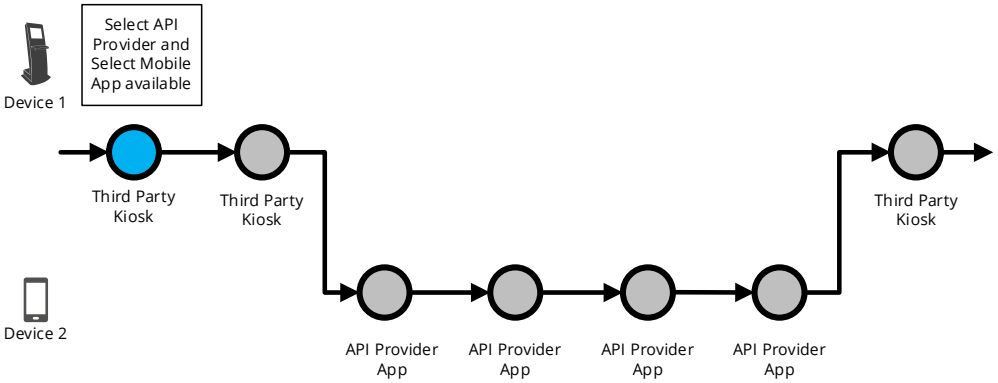


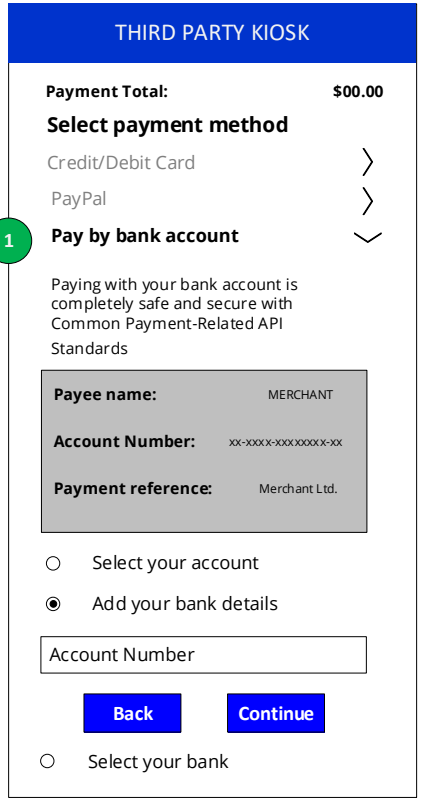
3.6.3.3 Wireframe journey



3.6.3.4 Wireframe annotations

3.6.3.4.1 Select API Provider





Minimum Set of Parameters

The Third Party **must** either allow the Customer to specify the below minimum set of parameters or pre-populate them for the Customer:

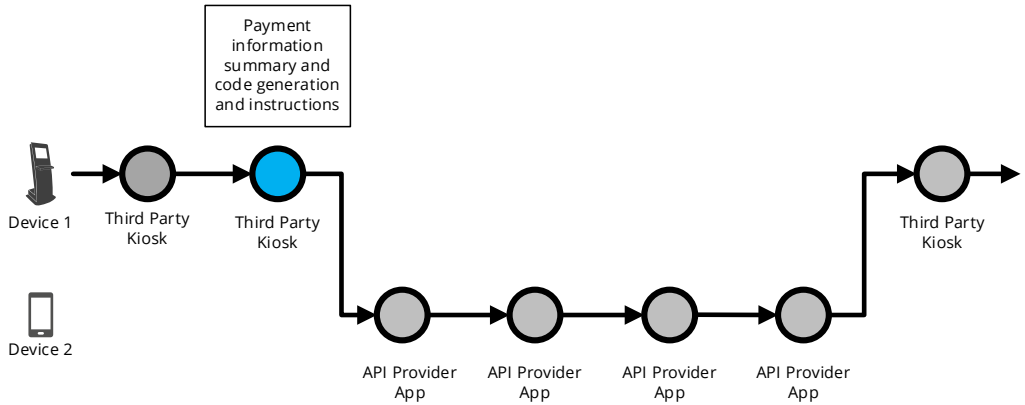
- Payment Amount and Currency.
- Payee Account Name.
- Payee Account Identification details (e.g. account number).
- Payment Reference - This is optional but it is good practice to be populated for a payment.
- Any supplementary information required which the API Provider has published as required and is specific to that API Provider

Customer Payment Account Selection

The Third Party **must** provide the Customer at least one of the following options:

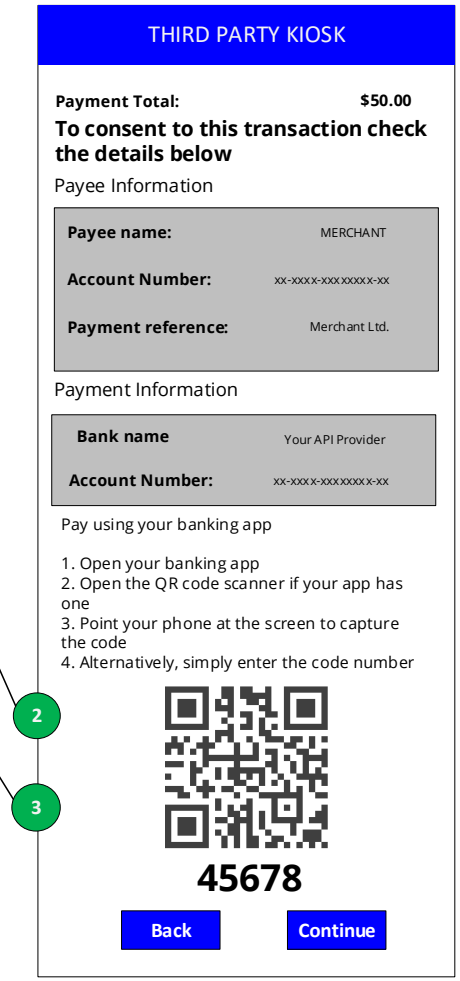
- Enter their Payer payment Account Identification details.
- The Third Party must allow the Customer to enter their payment Account Identification details in at least one of the ways specified in the API Centre API Specifications (e.g. account number).
- Select their Account Identification details (this assumes they have been saved previously).
- Select their API Provider in order to select their Customer payment Account from there later on in the journey.

3.6.3.4.2 Payment information summary

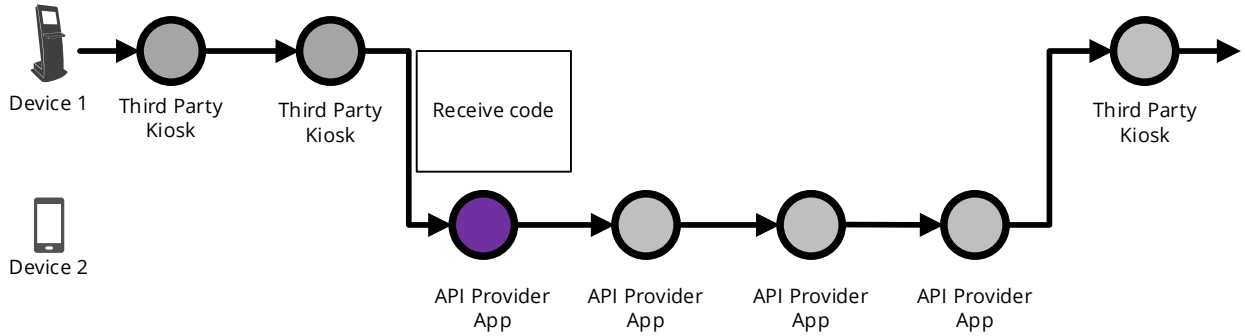


The Third Party **must** present the Customer with the authentication options supported by the API Provider which in turn can be supported by the Third Party device/channel (e.g. A Third Party kiosk that can only support authentication by an API Provider mobile app).

If a Third Party and API Provider support Model C then a Third Party **should** display an identifier generated from the API Provider to the Customer (e.g. QR code) and information on how the identifier should be used within the API Provider app (e.g. scan QR code with the API Provider app).

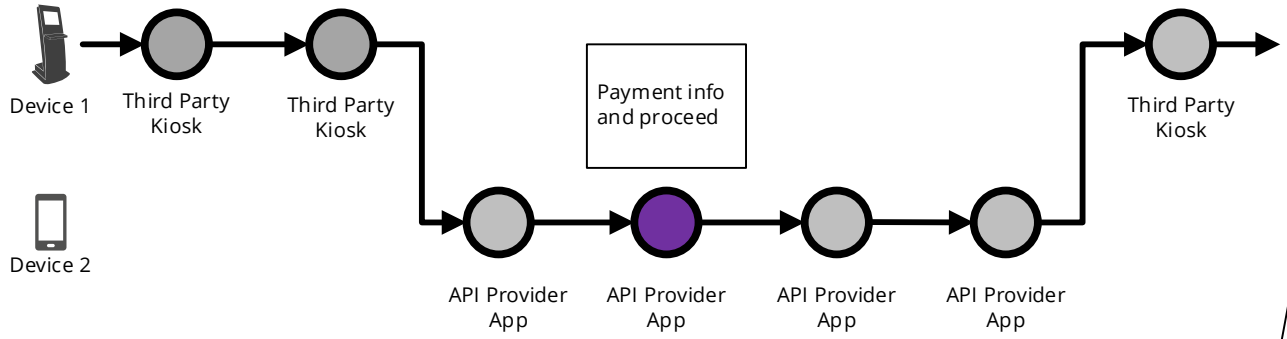


3.6.3.4.3 Receive code

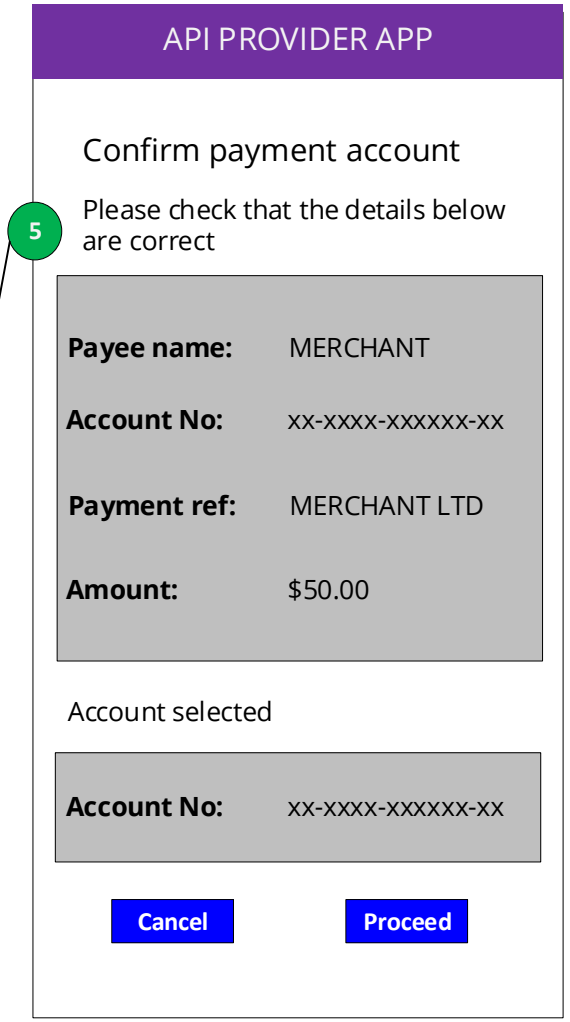


The Customer **should** be able to easily use the identifier presented by the Third Party application (e.g. scan the code from the Kiosk in this instance) without much friction (e.g of manually entering an alphanumeric code).

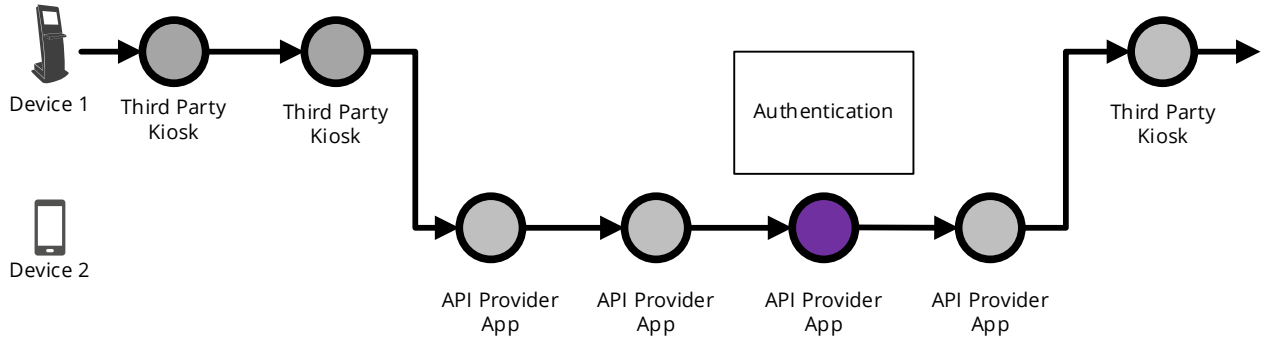
3.6.3.4.4 Payment information and proceed



After the Customer the scans identifier from the Third Party within the API Provider app, then the API Provider **must** display the payment request and clearly mention the amount and the payee and payment account.

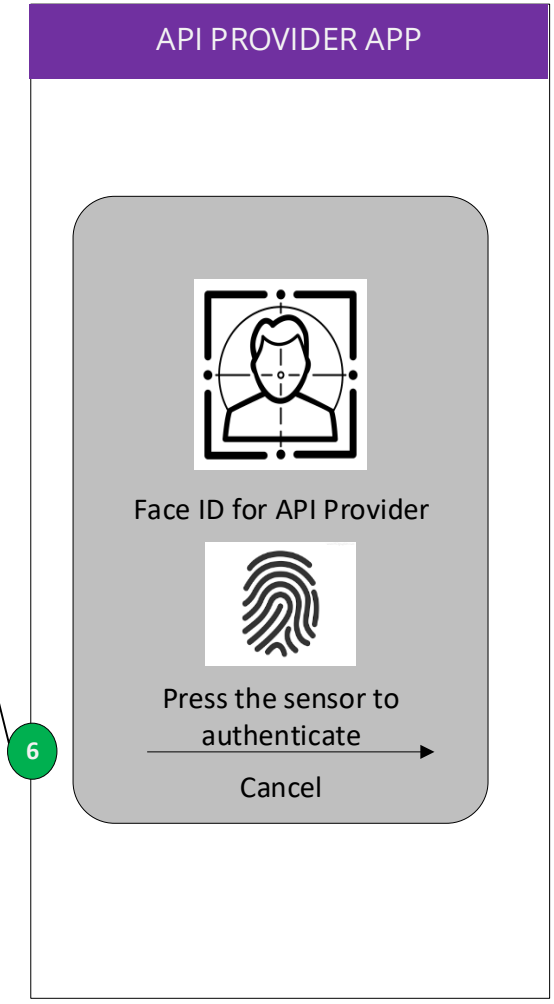


3.6.3.4.5 Authentication

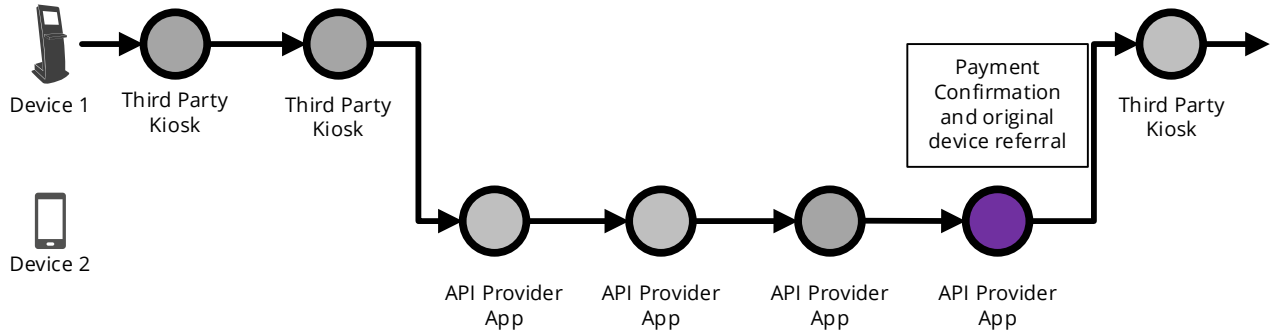


API Provider performs Secure Customer Authentication.

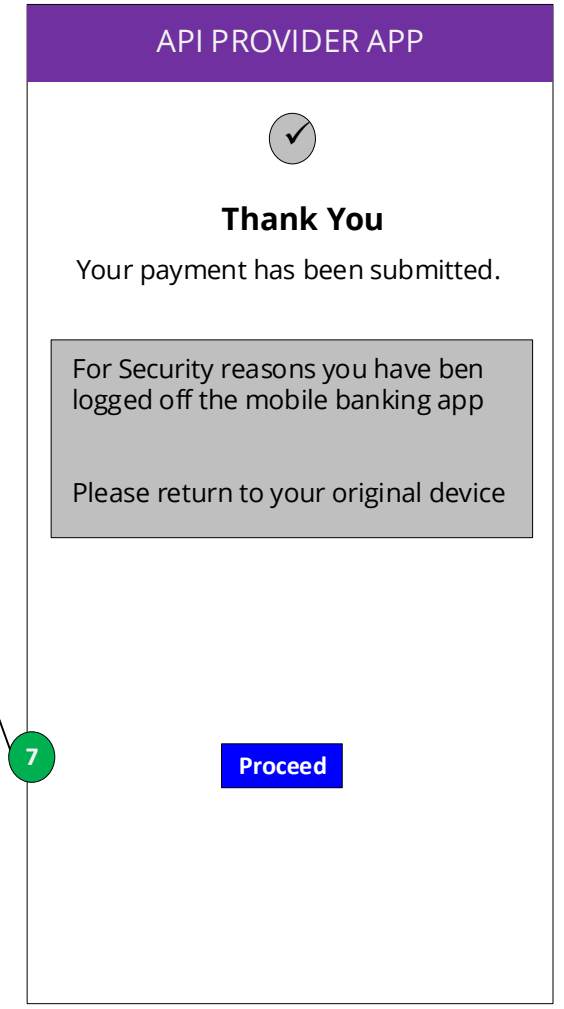
The API Provider app based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the API Provider mobile app (biometric, passcode, credentials)



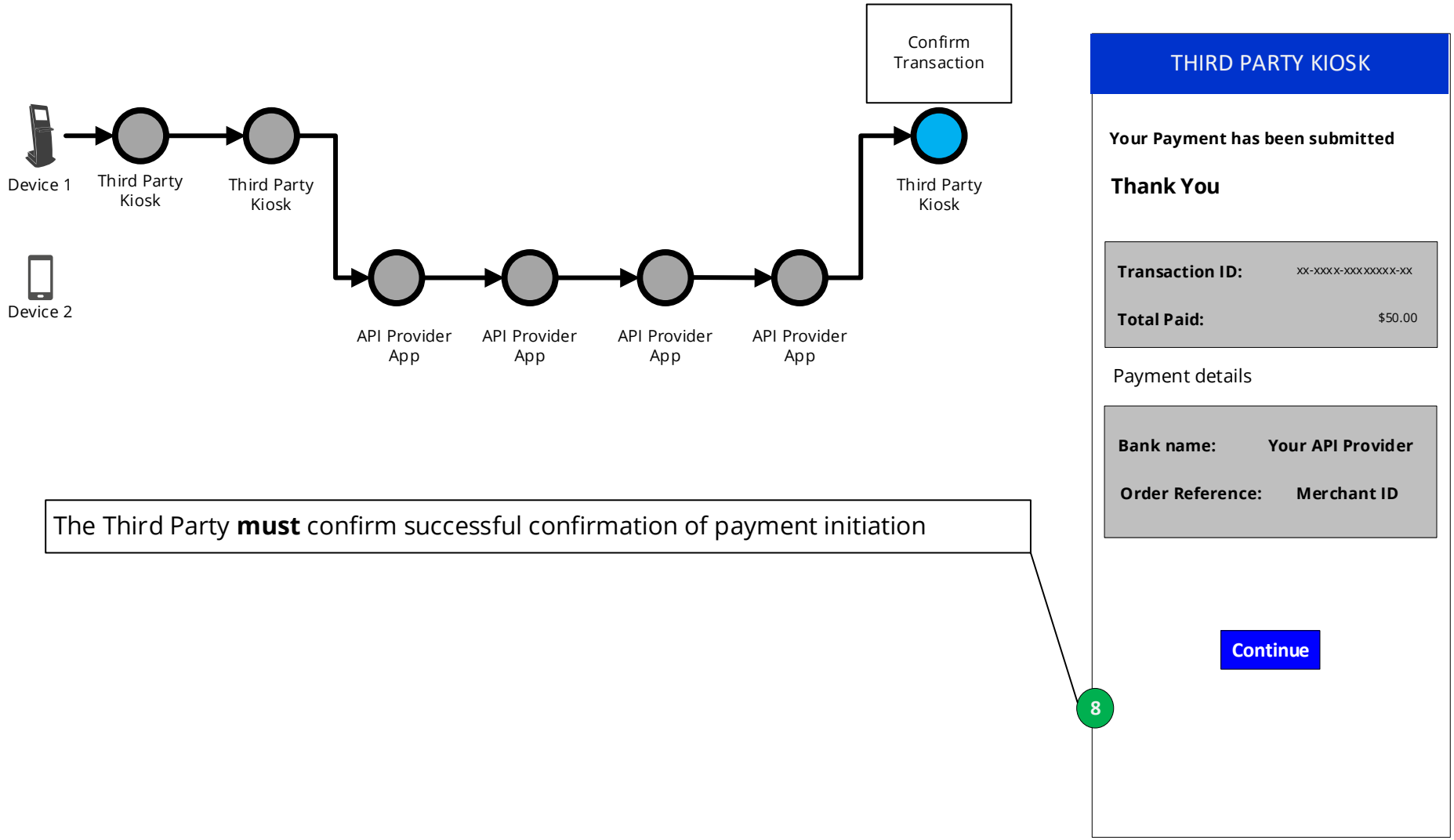
3.6.3.4.6 Payment confirmation



An API Provider **should** make the Customer aware that they have been logged off from the API Provider app and notify them to check back on the originating Third Party app



3.6.3.4.7 Confirm transaction



The Third Party **must** confirm successful confirmation of payment initiation

3.6.4 Model D: Customer with a previously generated ID token

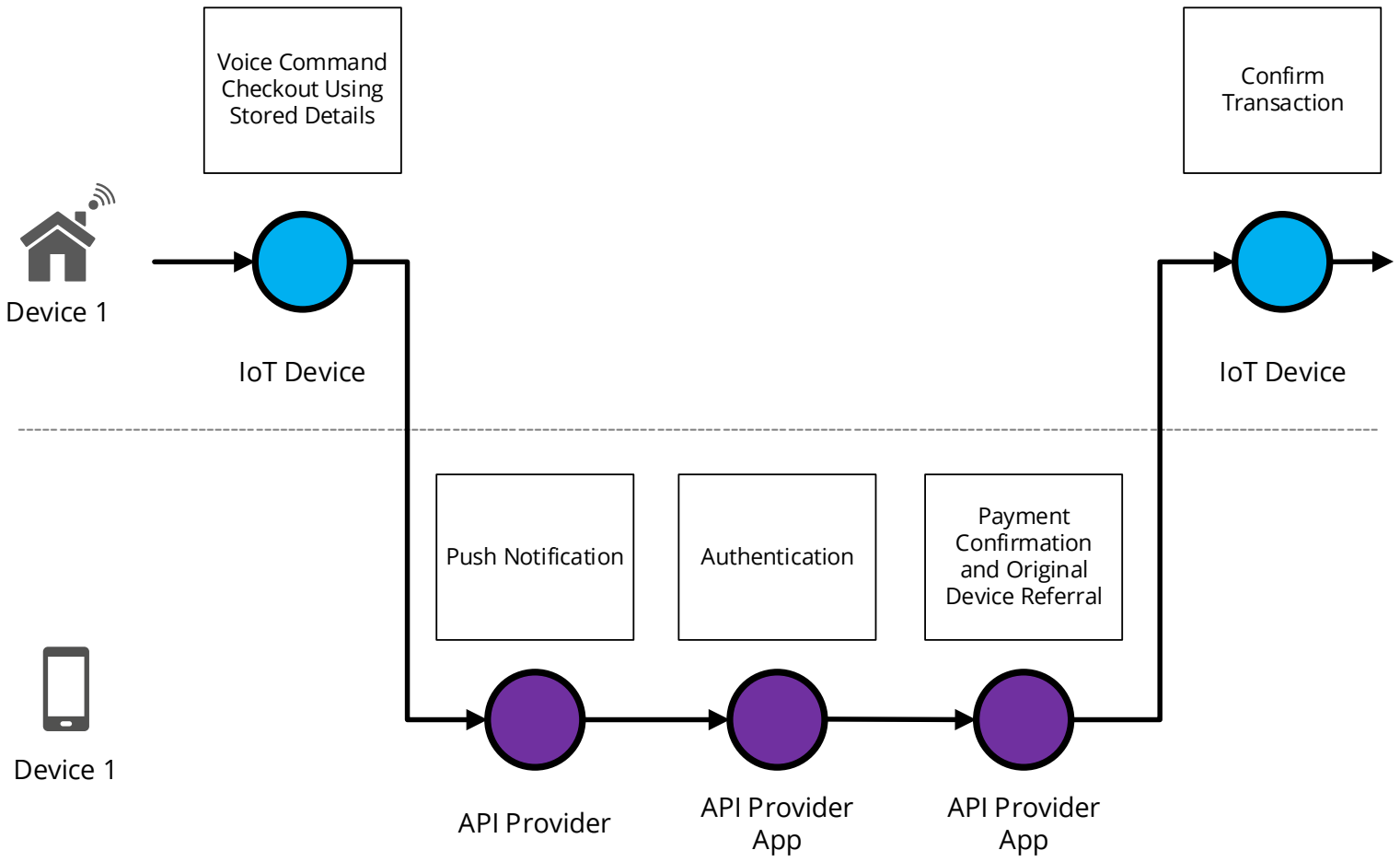
3.6.4.1 Journey description

A Decoupled authentication flow where the Third Party provides the API Provider with an ID Token, generated by the API Provider from a previous consent authentication event. This is used by the API Provider to re-identify the Customer for a new authentication and authorisation event**.**

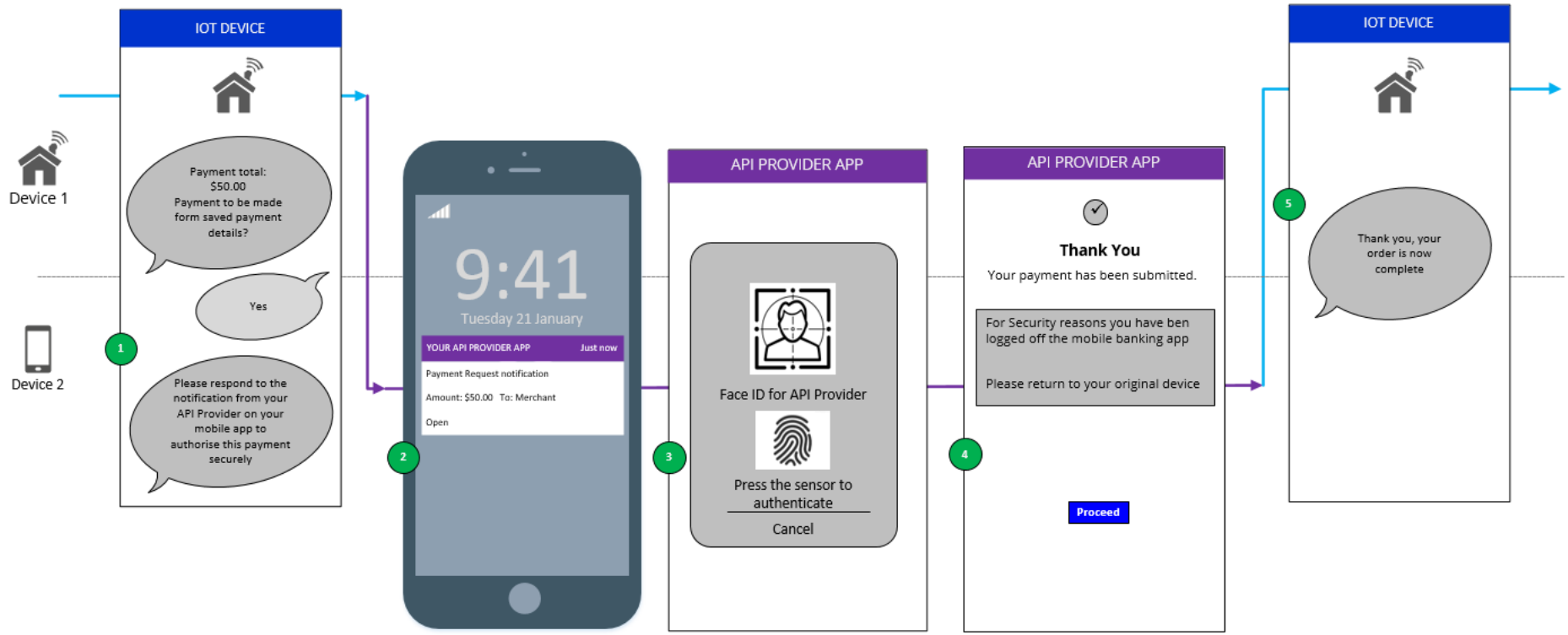
This model is ideally suited where the services offered by the Third Party involve POS, telephony, or where Customer interaction with the Third Party is not possible through a graphical interface (IoT devices), or even when the Customer may not be present within the Third Party channel.

3.6.4.2 Journey map

Model D: Customer with a Third Party account

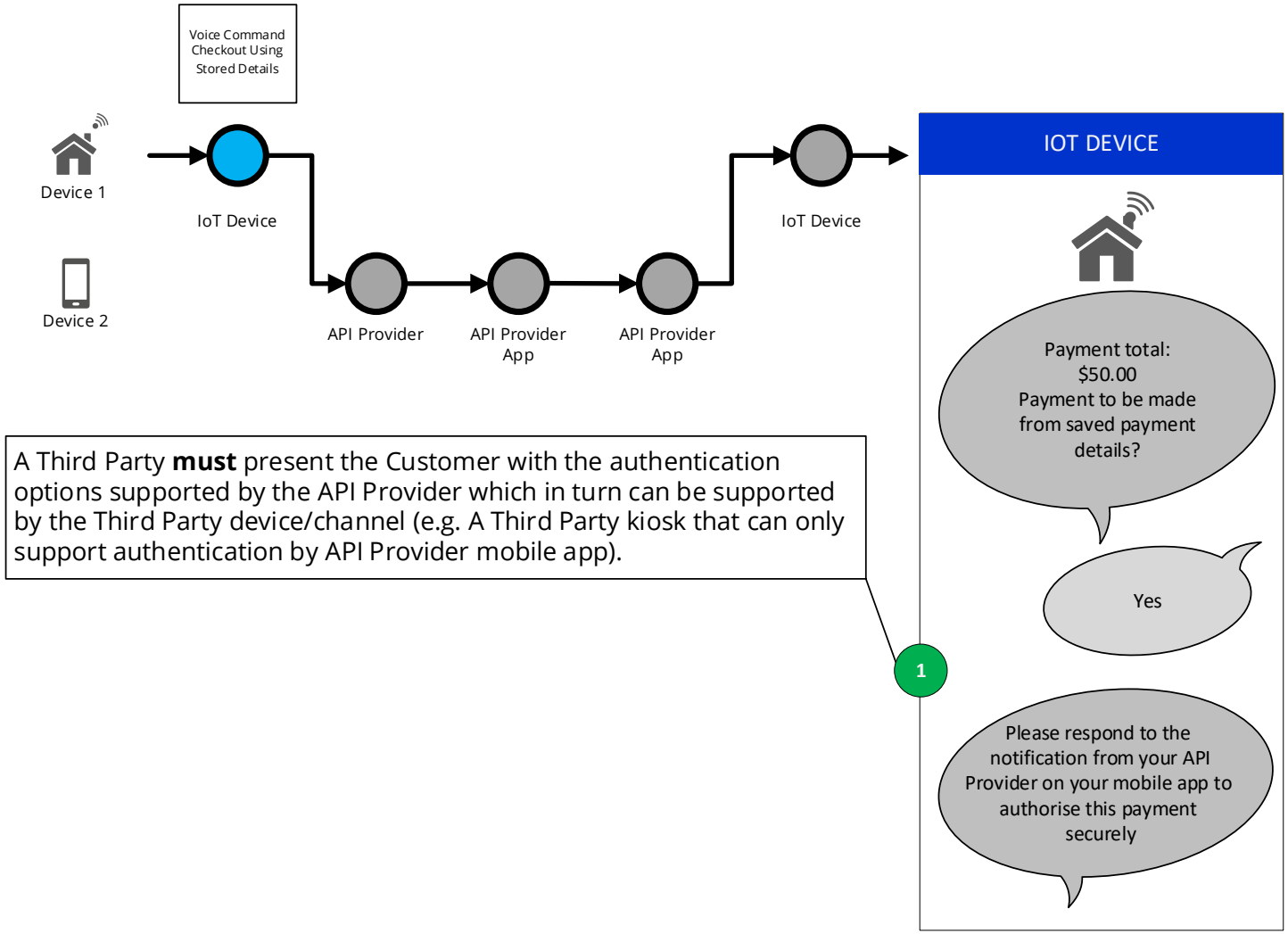


3.6.4.3 Wireframe journey

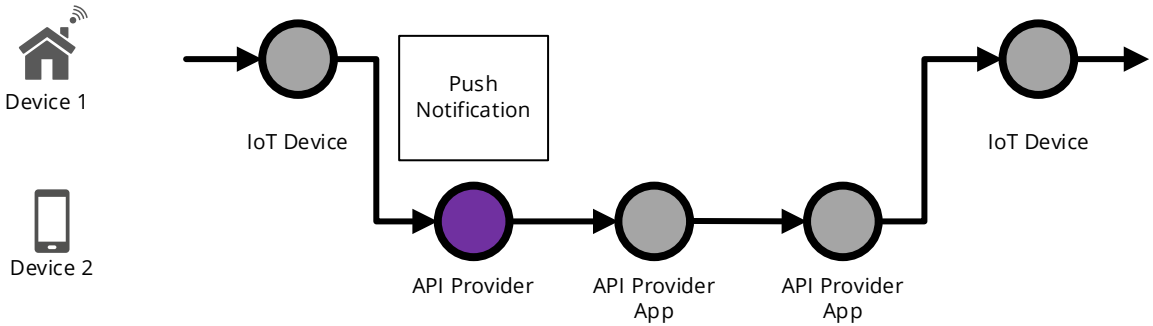


3.6.4.4 Wireframe annotations

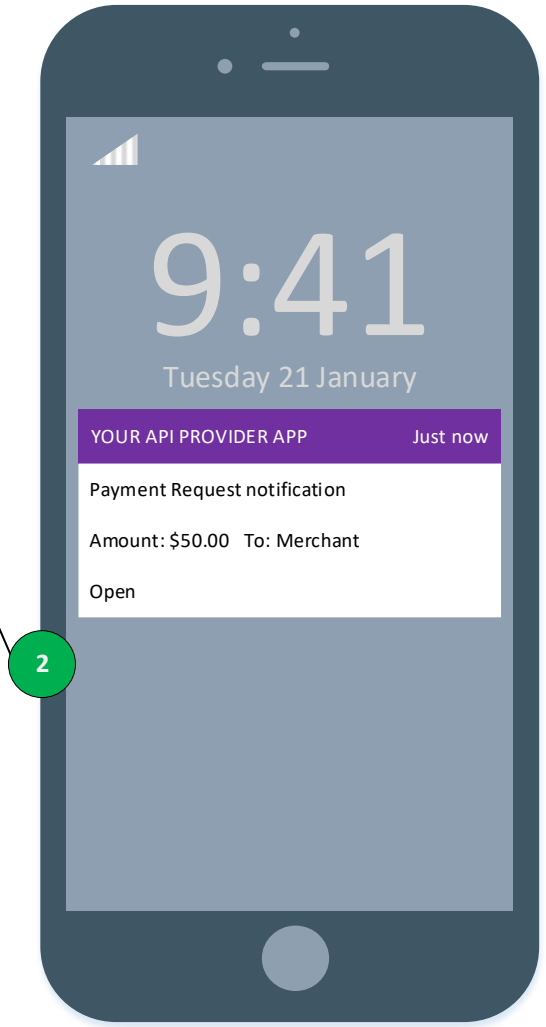
3.6.4.4.1 Voice command checkout



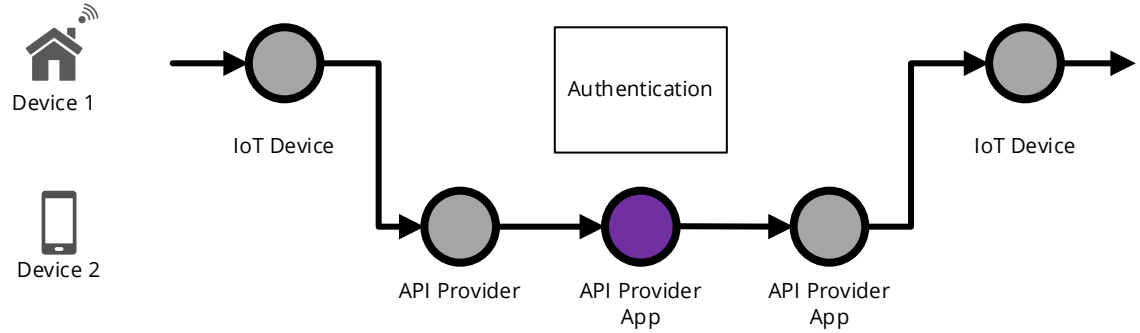
3.6.4.4.2 Push notification



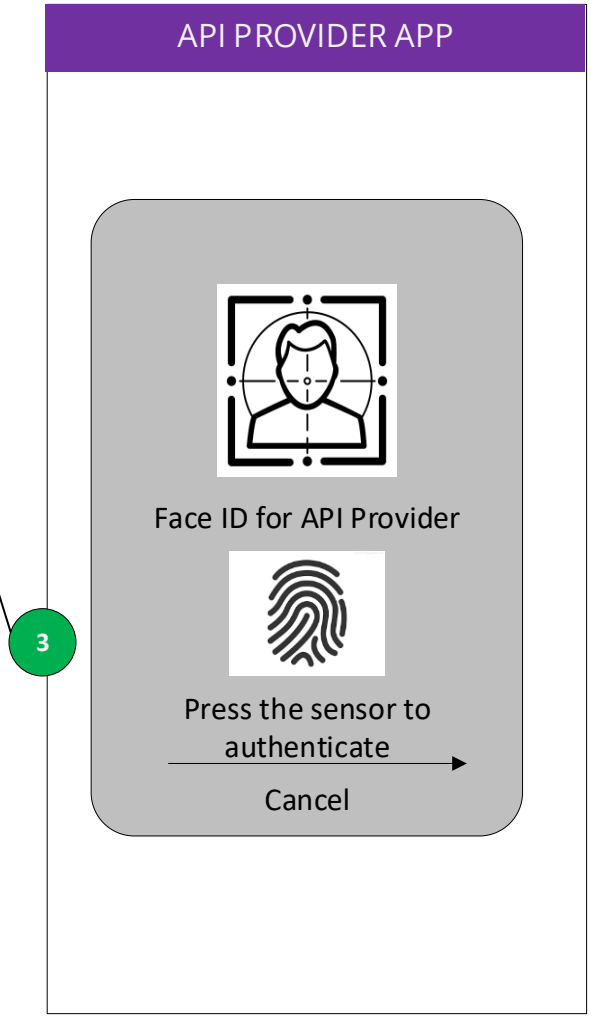
An API Provider **must** notify the Customer through the API Provider app for authentication purposes only without introducing any additional screens above what a Customer would experience through existing online channels. The notification **must** clearly mention the payment request with the amount and the payee.



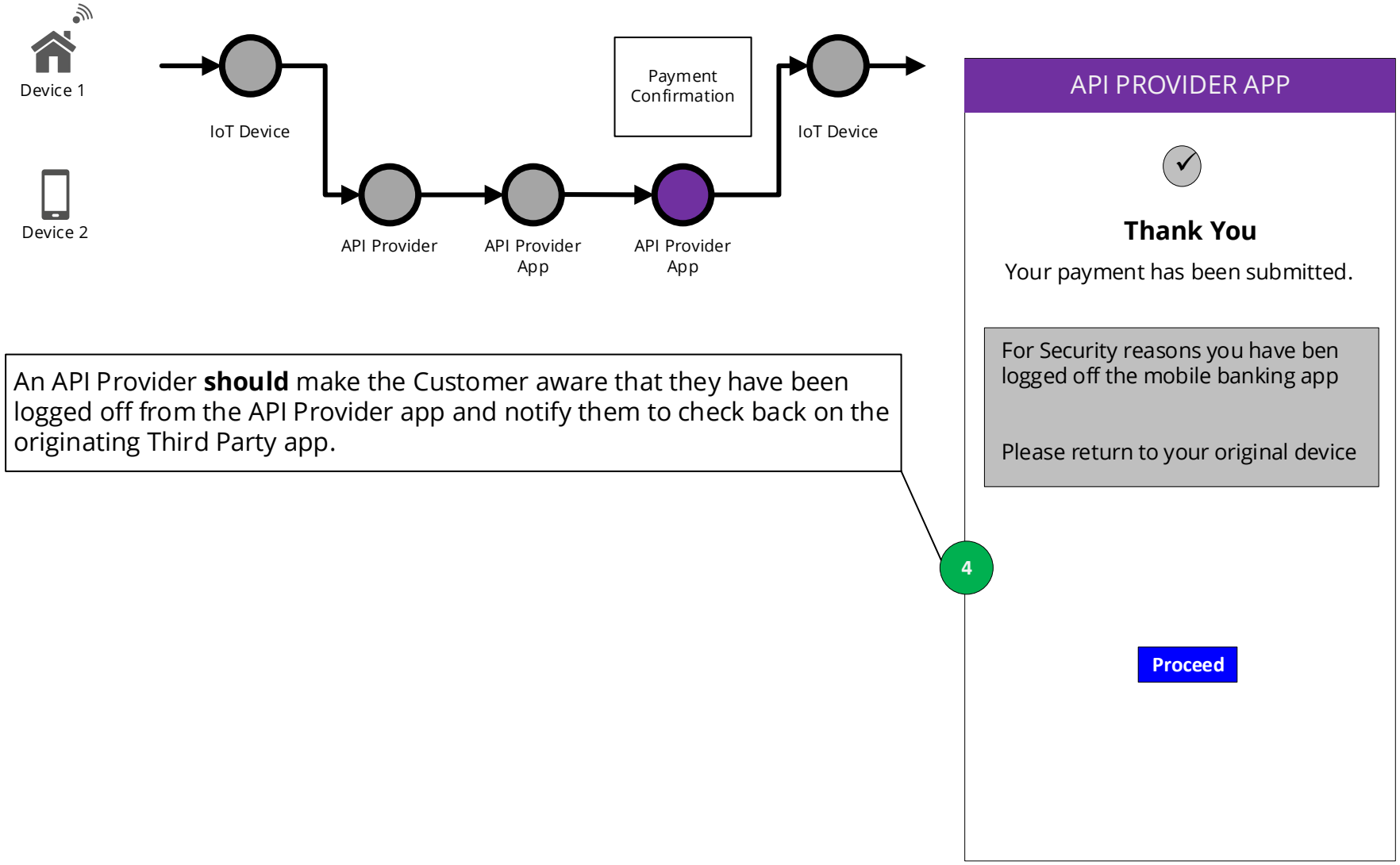
3.6.4.4.3 Authentication



An API Provider app based authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the API Provider mobile app (biometric, passcode, credentials).

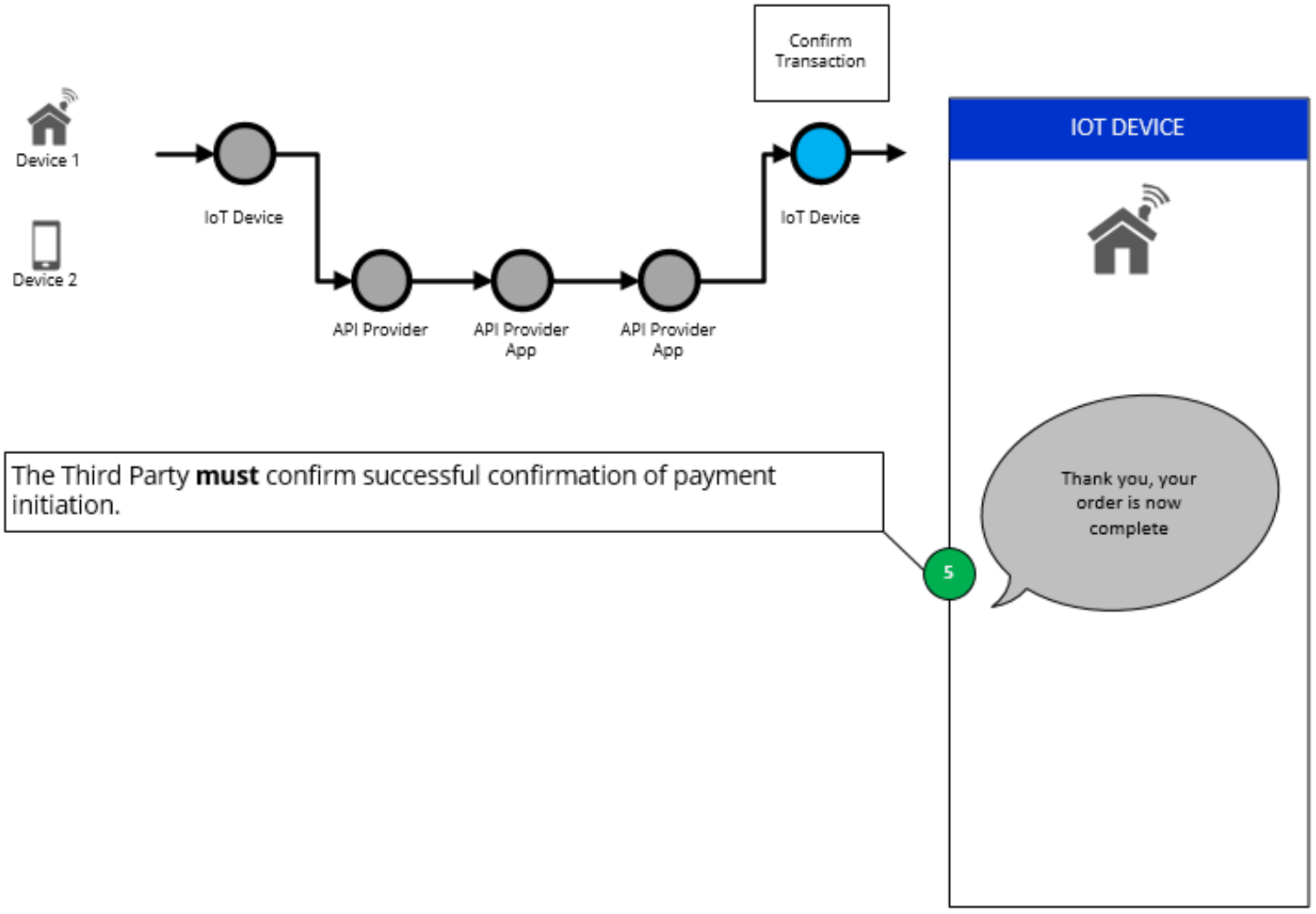


3.6.4.4.4 Payment confirmation



An API Provider **should** make the Customer aware that they have been logged off from the API Provider app and notify them to check back on the originating Third Party app.

3.6.4.4.5 Confirm transaction



The Third Party **must** confirm successful confirmation of payment initiation.

4 Account Information Services (AIS)

One of the primary aims of the Guidelines is to provide simplification and consistency throughout each stage of API Standards implementation. Therefore, we have defined a core set of Account Information Services journeys to illustrate the roles played by each party in the the API Standards ecosystem.

The API Standards support Account Information Services. They enable a Third Party to access account information from accounts held at API Providers and to provide account information services to a Customer, provided they have obtained the Customer's explicit consent.

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

- Account Information Consent – A Customer giving consent to a Third Party to request account information from their API Provider.
- Consent Dashboard and Revocation – Third Party facility to enable a Customer to view and cancel consents given to that Third Party.
- Access Dashboard and Revocation – API Provider facility to enable a Customer to view all Third Parties that have access to their account(s) and the ability to cancel that access. This should be available on those channels that the Customer uses to manage their accounts with the API Provider and be easy and intuitive for the Customer to find and use.
    - This facility should not include unnecessary steps, superfluous information or language which could discourage the use of Third Party services or divert the Customer from the access management process.
- Generic guidance around the effective use of re-direction screens (when the Customer is transferred to and from the API Provider's domain).

NOTE: *Limitations of Account Information Services Access for Customers acting with delegated user authority on behalf of Corporate Entities will only be able to use Third Party services, if this is permitted within the parameters of that delegated user authority*

4.1 Account Information Services core journeys

4.1.1 Account information consent

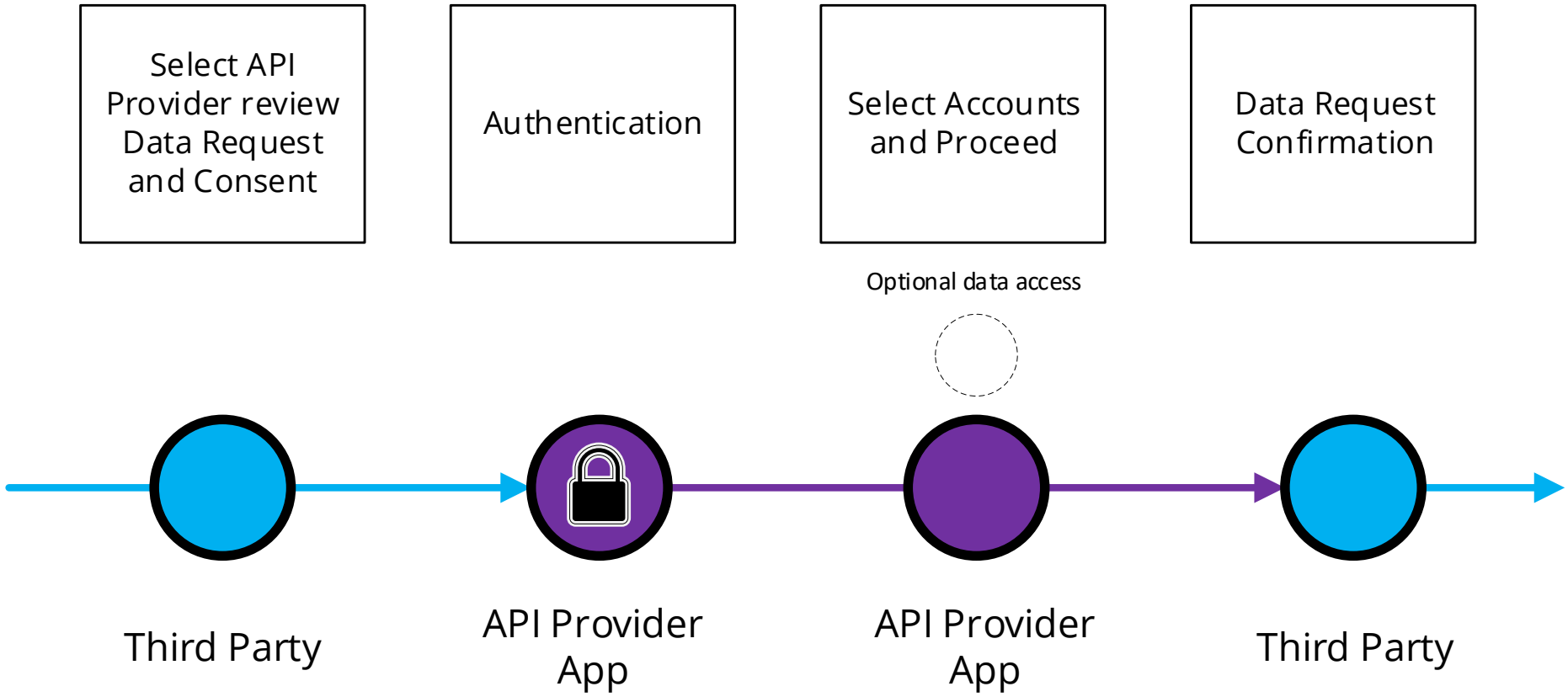
4.1.1.1 Journey description

In this journey:

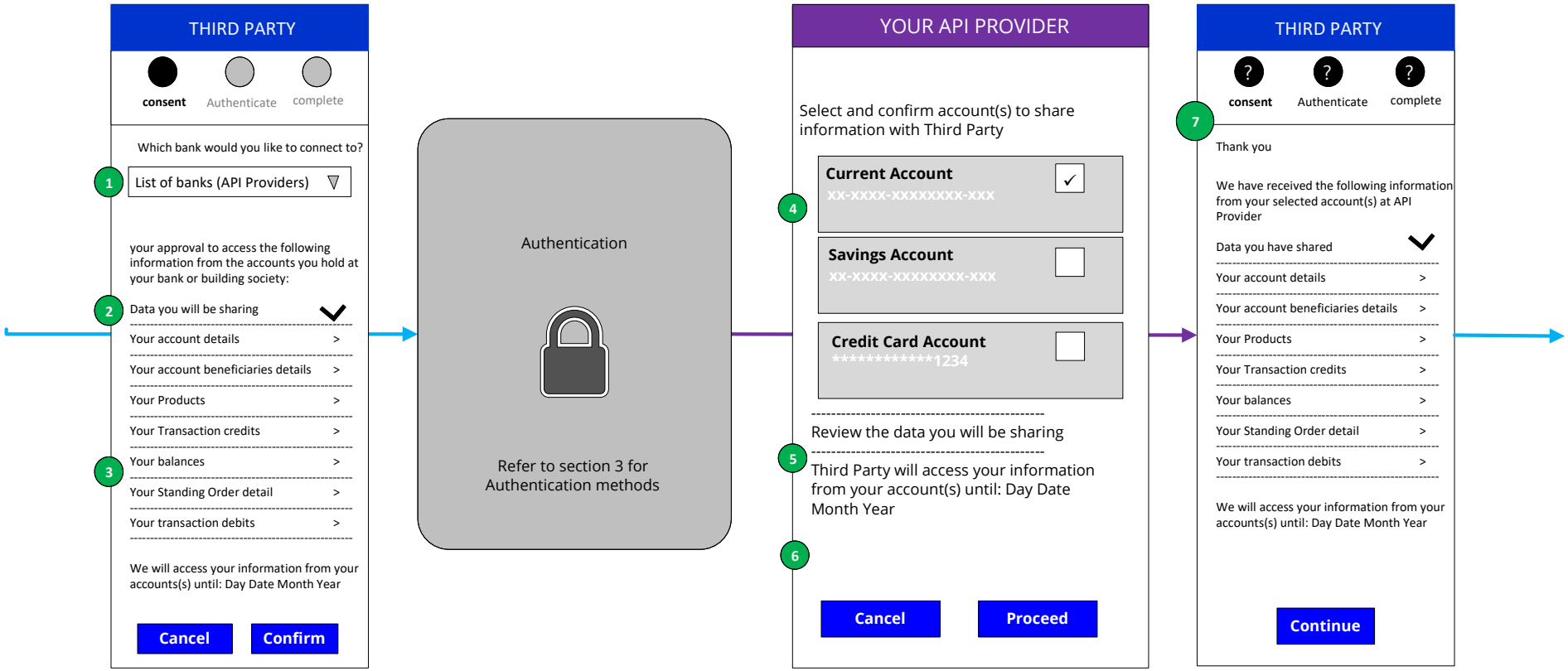
- The Third Party presents a description of the service that it is providing and the data that it requires in order to support its service proposition.
- The Customer selects the API Provider(s) where their payment account(s) is held.
- The Customer is then directed to the domain of their API Provider(s)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

NOTE: *When considering Third Party requests submitted by a Customer acting with delegated user authority on behalf of a corporate entity, the Customer may only be able to use Third Party services if this is permitted within the parameters of that delegated user authority.*

4.1.1.2 Journey map

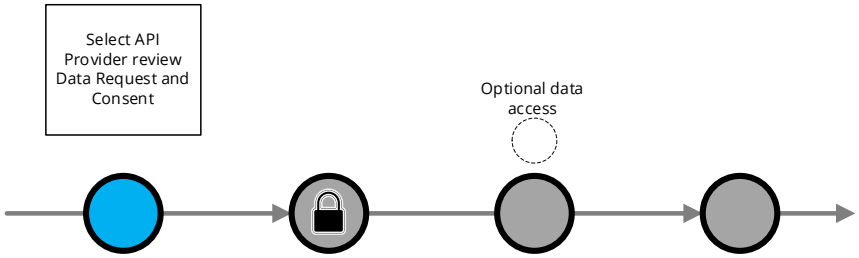


4.1.1.3 Wireframe journey



4.1.1.4 Wireframe annotations

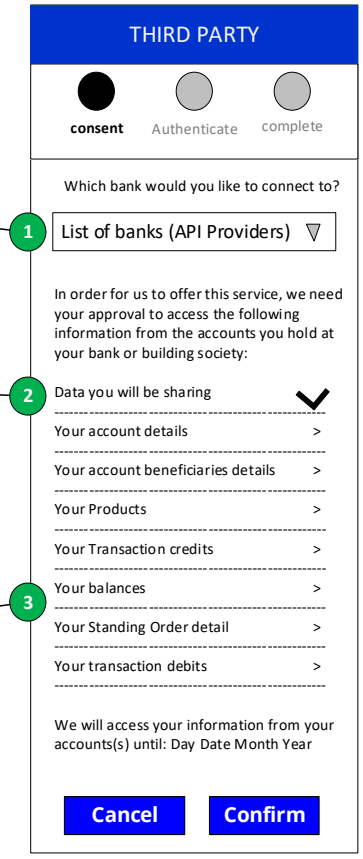
4.1.1.4.1 Select API Provider



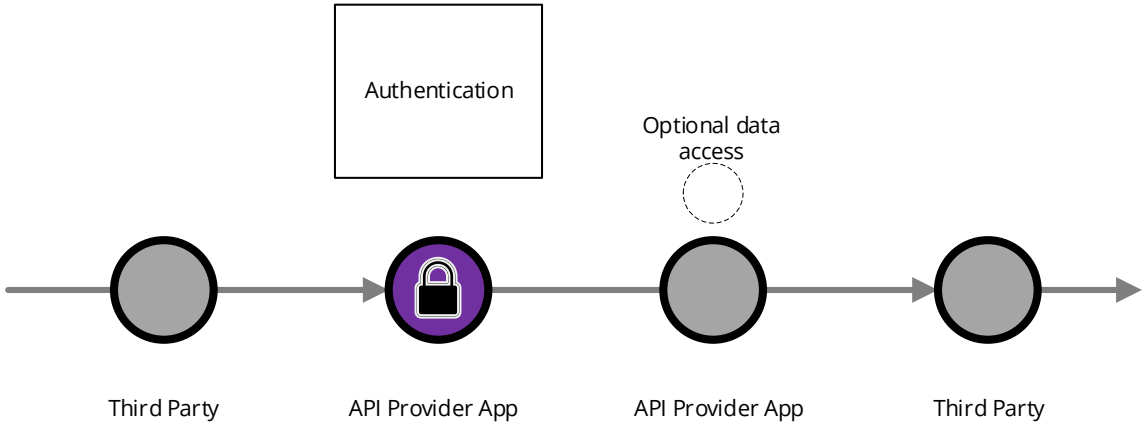
A Third Party **should** ask the Customer to identify their API Provider before requesting consent so that the consent request can be constructed in line with the API Provider data capabilities (which the API Provider must make available to the Third Party).

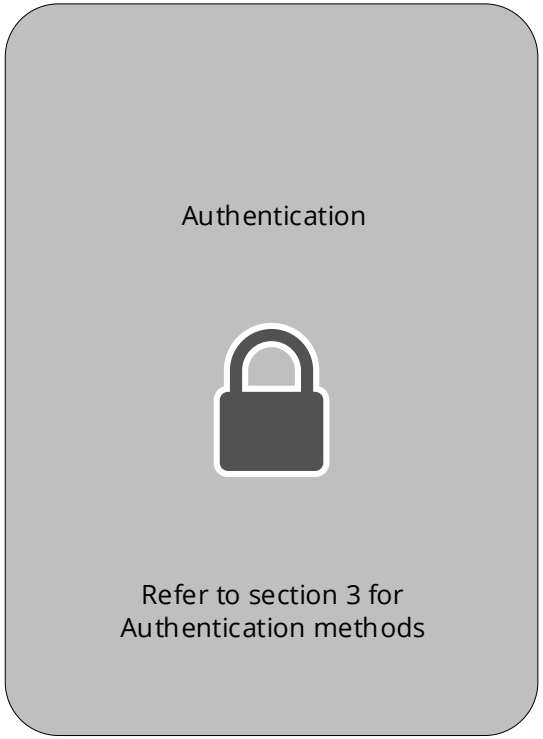
A Third Party **must** provide the Customer with sufficient information to enable the customer to make an informed decision, for example, detail the purpose for which the data will be used (including whether any other parties will have access to the information) the period over which it has been requested and when the consent for the account information will expire (consent could be on-going or one-off).
If the customer-facing entity is acting on behalf of a Third Party as its Permitted User, the Customer **must** be made aware that the Permitted User is acting on behalf of the Third Party.

The Third Party **should** provide the Customer with a description of the data being requested using the structure and language recommended and ensure that this request is specific to only the information required for the provision of their account information service to the Customer.
The Third Party **should** present the data at a Data Cluster level and allow the Customer to expand the level of detail to show each Data Permission. The Third Party should only present those data clusters relevant for the product type in question. Where the request is for multiple product types then the detail shown in the data cluster should explain to the Customer the product types to which it applies or state that it is shared across multiple product types.
Once the Customer has consented, the Customer will be directed to their API Provider.

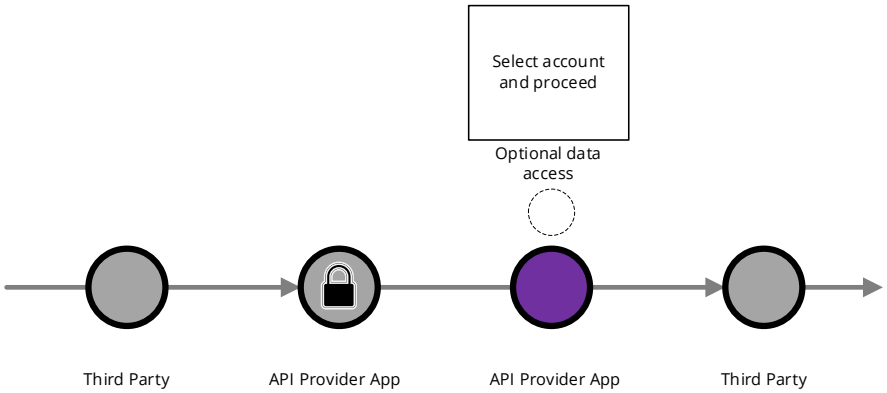


4.1.1.4.2 Authentication





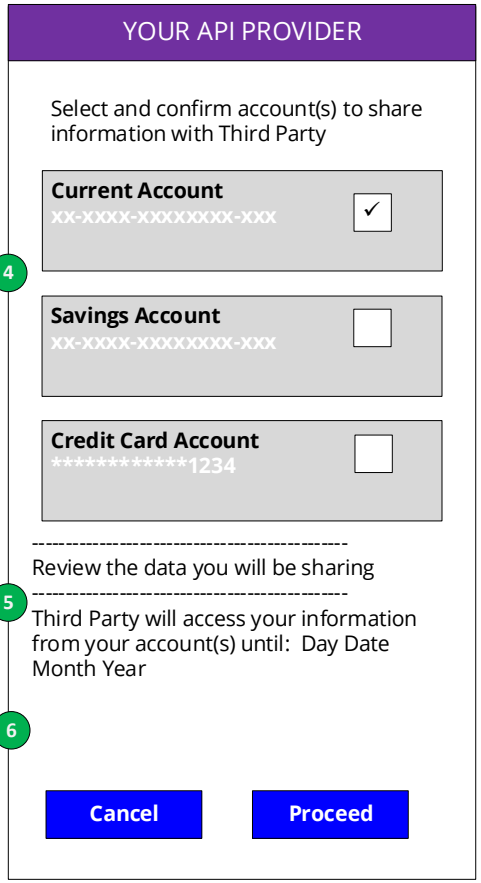
4.1.1.4.3 Select accounts and proceed



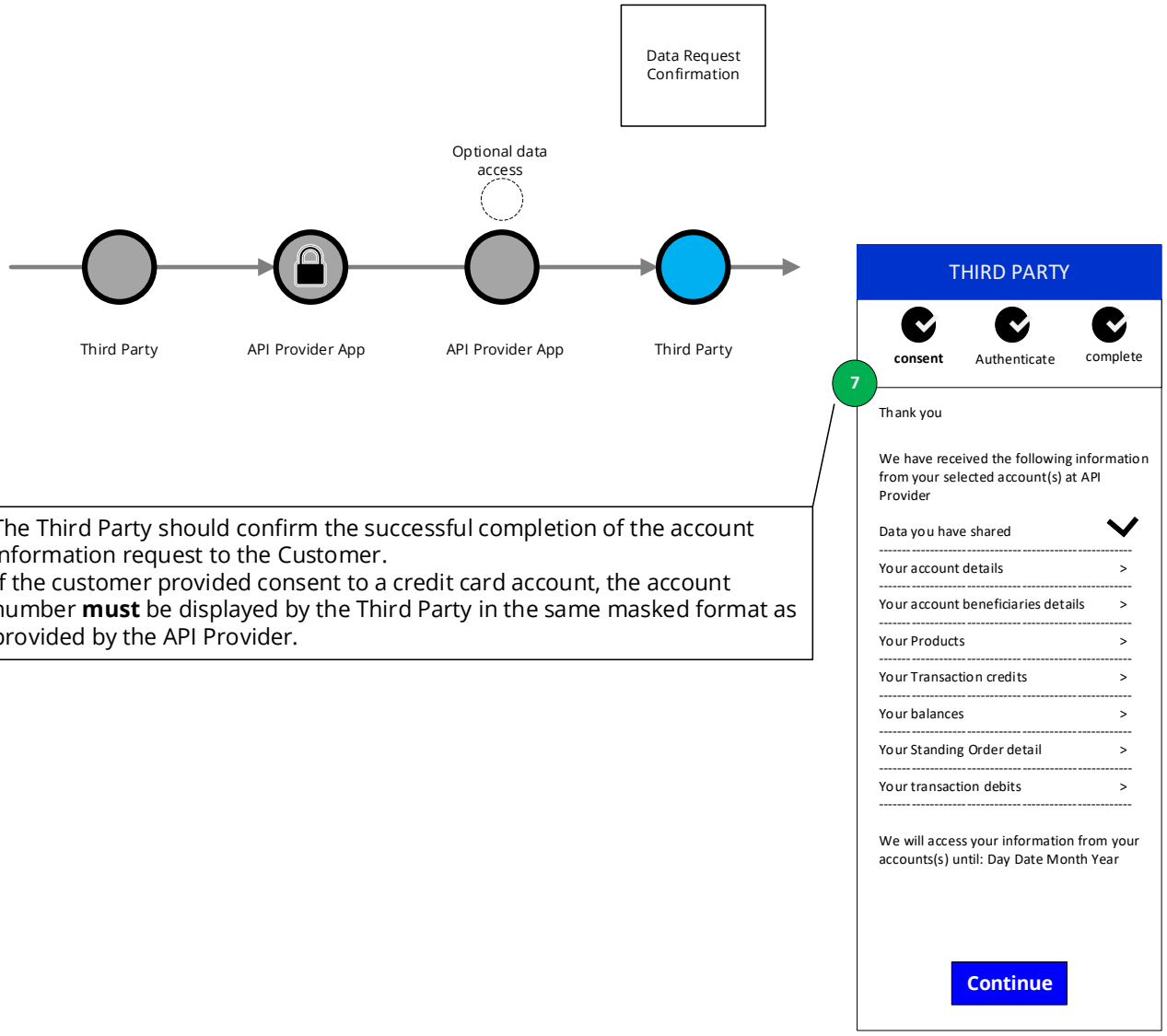
If the customer-facing entity is acting on behalf of a Third Party as its Permitted User the API Provider **should** make the Customer aware that the Permitted User is acting on behalf of the Third Party.
This can be presented to the Customer by displaying both the Permitted User name and the Third Party name as:
Select and confirm account(s) to share information with <Permitted User>, who is acting on behalf of <Third Party>
The API Provider **should** display credit card account information in the same format as the Customer would see when using their existing online channels.

If the API Provider provides an option for the Customer to view the data they have consented to share with the Third Party as supplementary information, this **should** be done using the structure and language recommended by API Centre. Display of such information **should not** be provided to the Customer as a default.

The API Provider **should** not seek confirmation of the consent that has already been provided by the Customer to the Third Party.



4.1.1.4.4 Data request confirmation

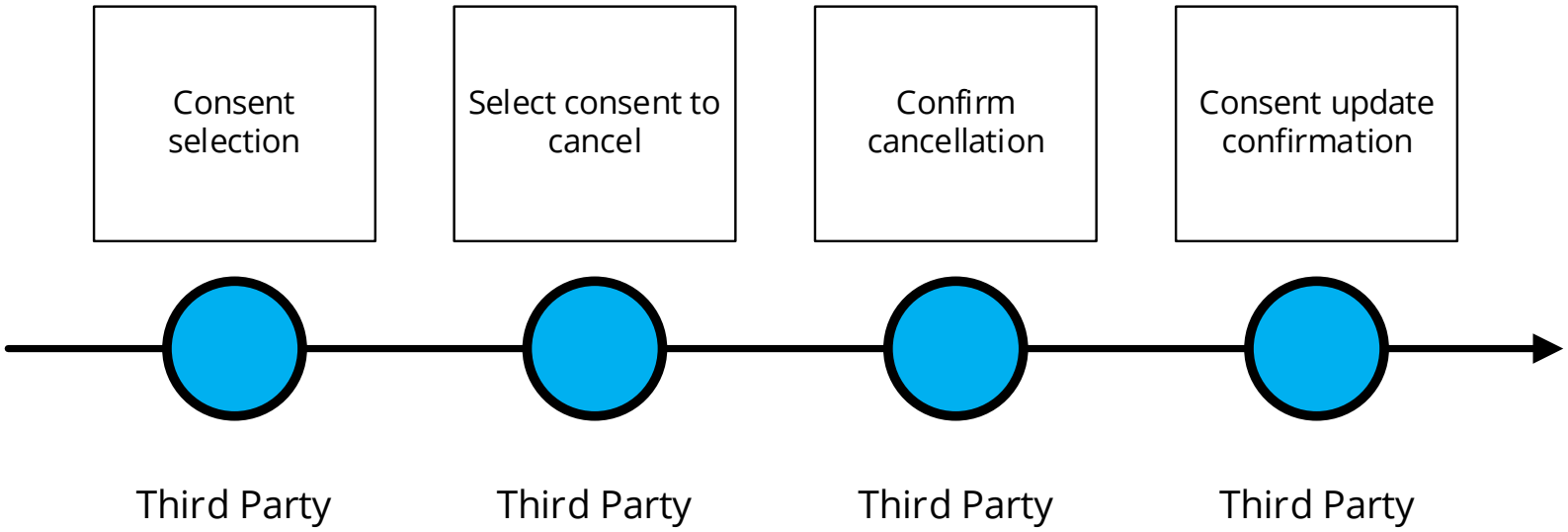


The Third Party should confirm the successful completion of the account information request to the Customer.
If the customer provided consent to a credit card account, the account number **must** be displayed by the Third Party in the same masked format as provided by the API Provider.

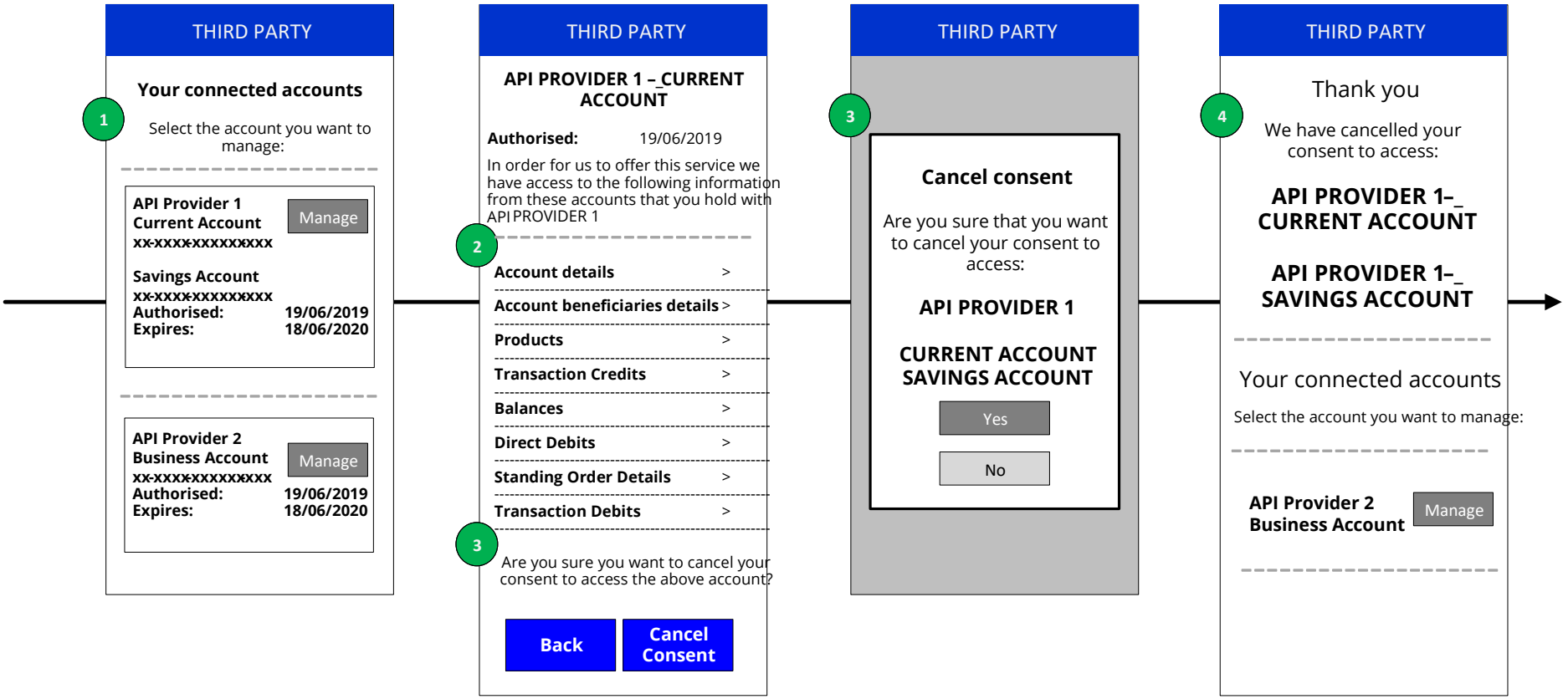
4.1.2 Consent dashboard and revocation

A Third Party should provide Customers with a facility to view and cancel on-going consents that they have given to that API Provider. Additionally, they may have consented to share data from several API Providers with a single Third Party. This section describes how these consents should be displayed and how the Customer journey to cancel them should be constructed.

4.1.2.1 Journey map

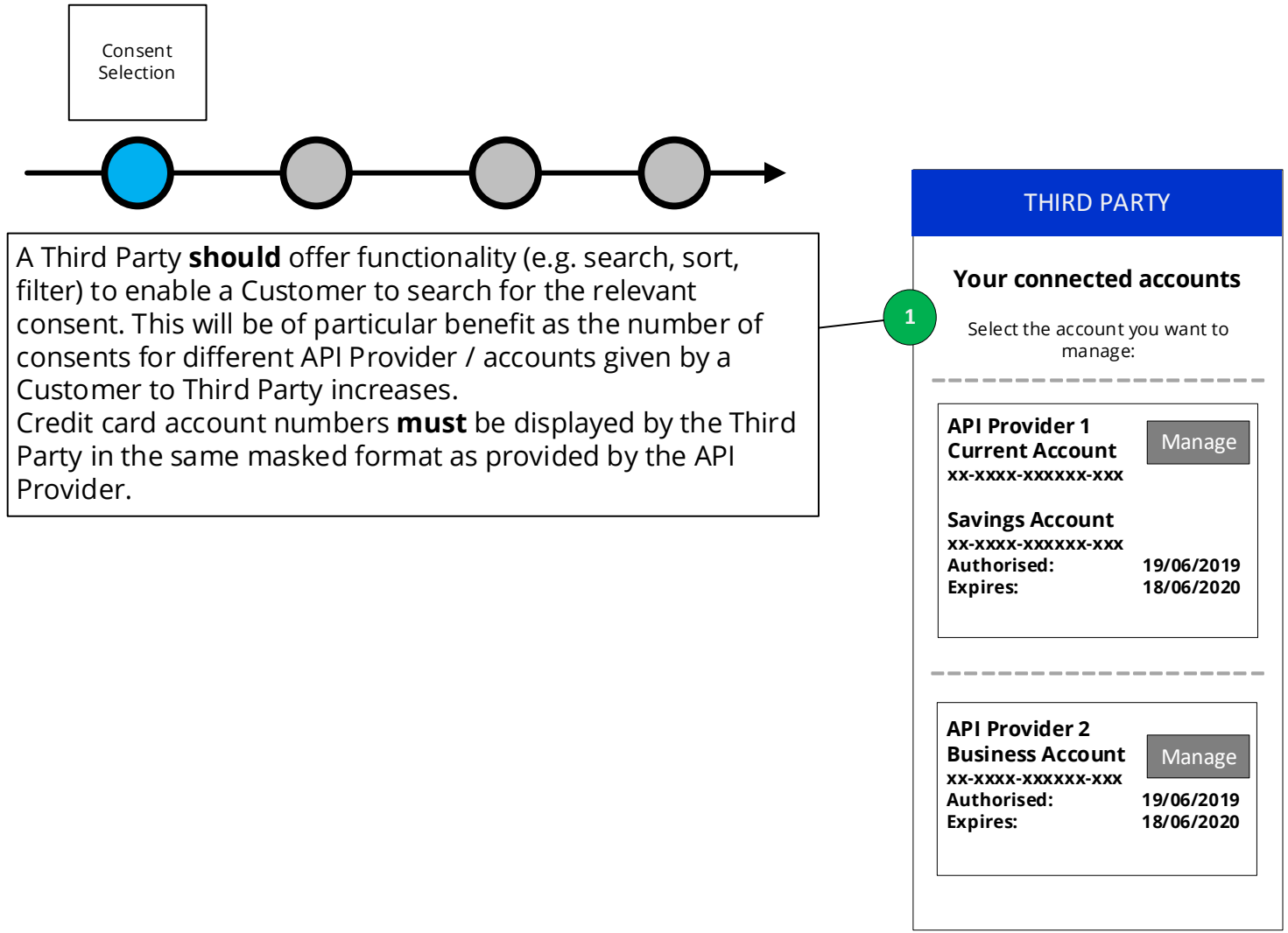


4.1.2.2 Wireframe journey

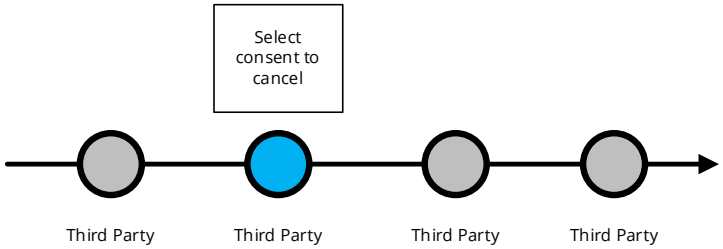


4.1.2.3 Wireframe annotations

4.1.2.3.1 Consent selection



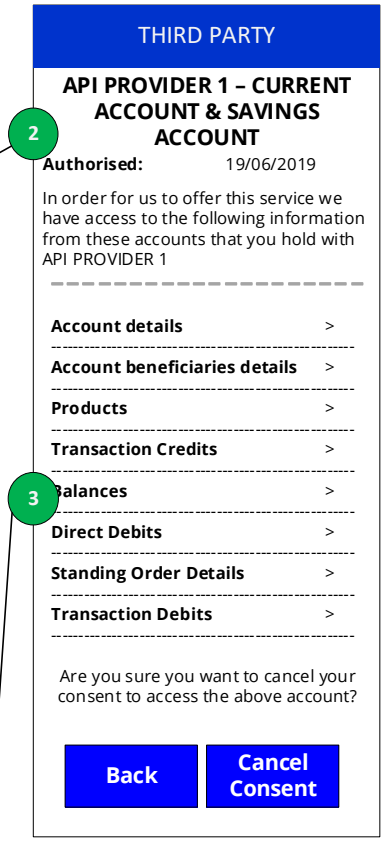
4.1.2.3.2 Select consent to cancel



A Third Party **should** describe the data being shared through each consent using the structure and language recommended by the API Centre and ensure this request is specific to only the information required for the provision of their account information service to the Customer.
Credit card account numbers **must** be displayed by the Third Party in the same masked format as provided by the API Provider.
A Third Party **should** present the data at a Data Cluster level and allow the Customer to expand the level of detail to show each Data Permission.
The Consent Dashboard **should** also describe:

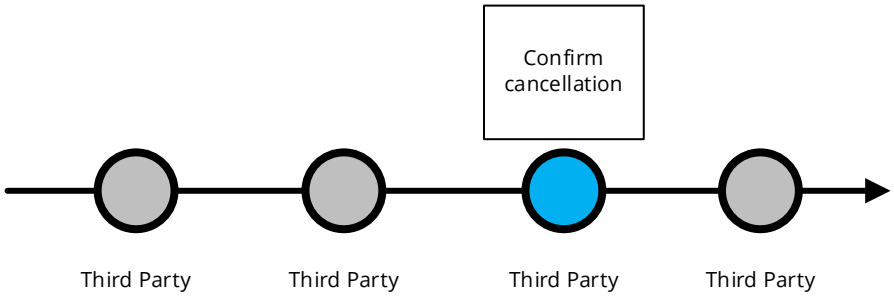
- The purpose of the data request (including whether any other parties will have access to the information). Where the request is for multiple product types, the detail should explain to the customer the product type to which it applies or state that it is shared across multiple product types.
- If relevant, the length of time for which this consent is valid (e.g. one off use, for a set period of time e.g. one year, or with no end date).
- The period for which the transaction data has been requested (e.g. transactions for the last 12 months).
- When the Third Party access to the data will expire.
- The date the consent was granted.
- If the customer-facing entity is acting on behalf of a Third Party as its agent, the Customer must be made aware that the agent is acting on behalf of the Third Party.

The consent dashboard **should** allow a Customer to view or cancel the access they have given consent to. These functions "Cancel Consent" and "Back" **should** be displayed with equal prominence to the Customer.
"Permitted User" means a person or entity who acts on behalf of an authorised payment institution or a small payment institution in the provision of payment services including account information services.

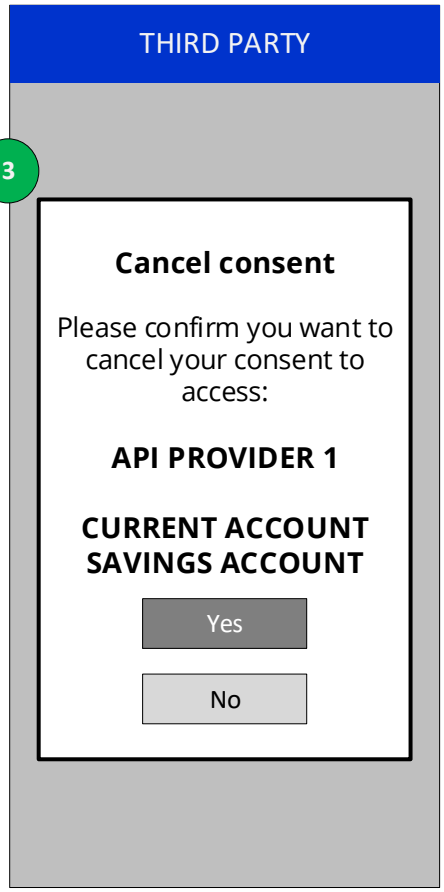


The Third Party **should** make the exact consequences of cancelling the consent clear to the Customer - i.e. they will no longer be able to provide the specific service to the Customer

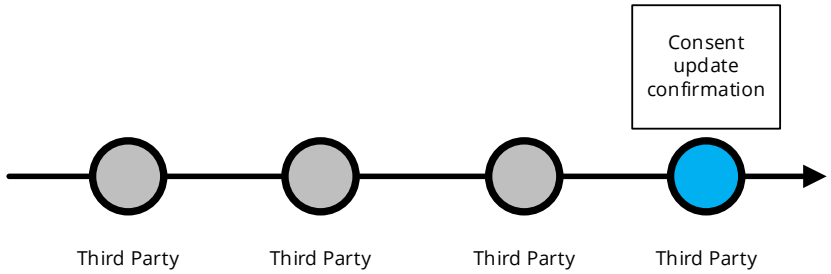
4.1.2.3.3 Confirm revocation



The Third Party **should** seek confirmation they wish to cancel consent for access - i.e. they will no longer be able to provide the specific service to the Customer

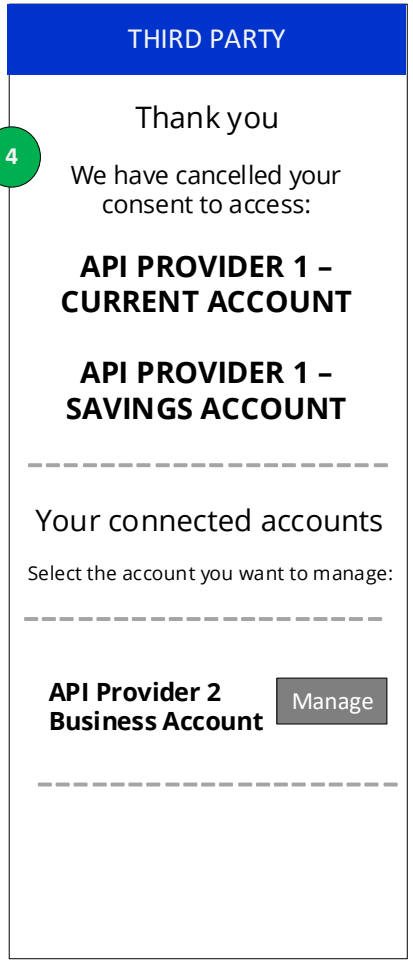


4.1.2.3.4 Consent update confirmation



The Third Party **must** inform the API Provider that the Customer has withdrawn consent by making a call to DELETE the account-access-consent resource as soon as practically possible. This will ensure that no further account information is shared.

The API Provider **must** support the Delete process . (This is not visible to the Customer but will ensure no further account information is provided by the API Provider to the Third Party).

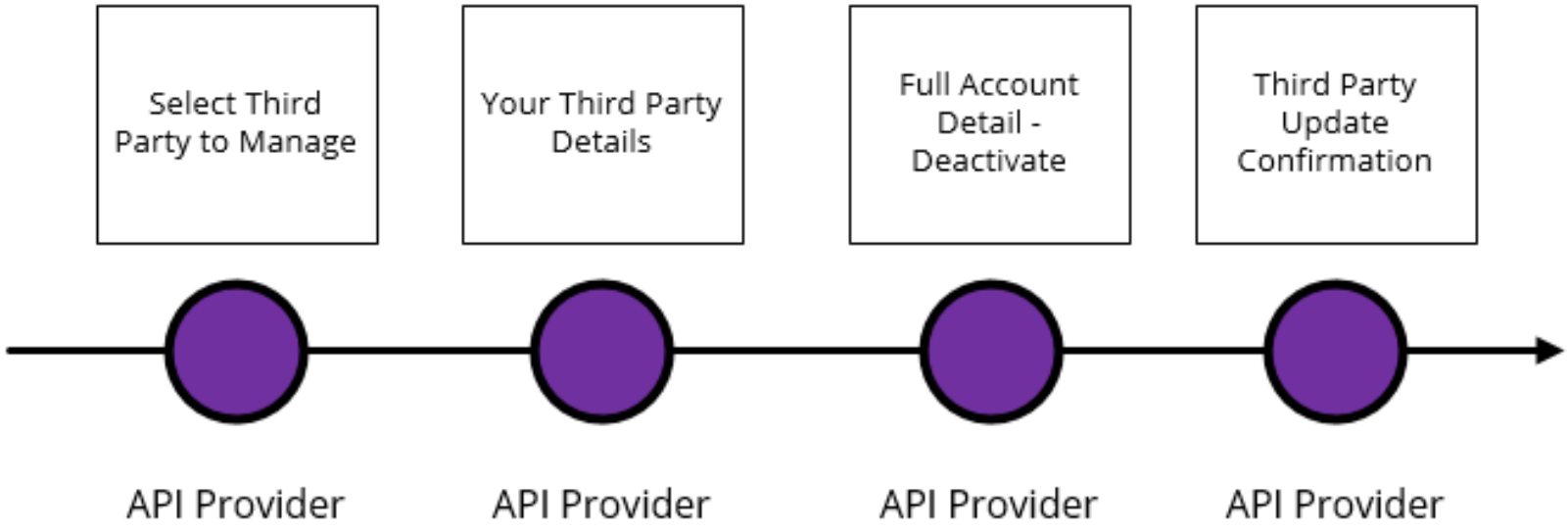


4.1.3 Access dashboard and revocation

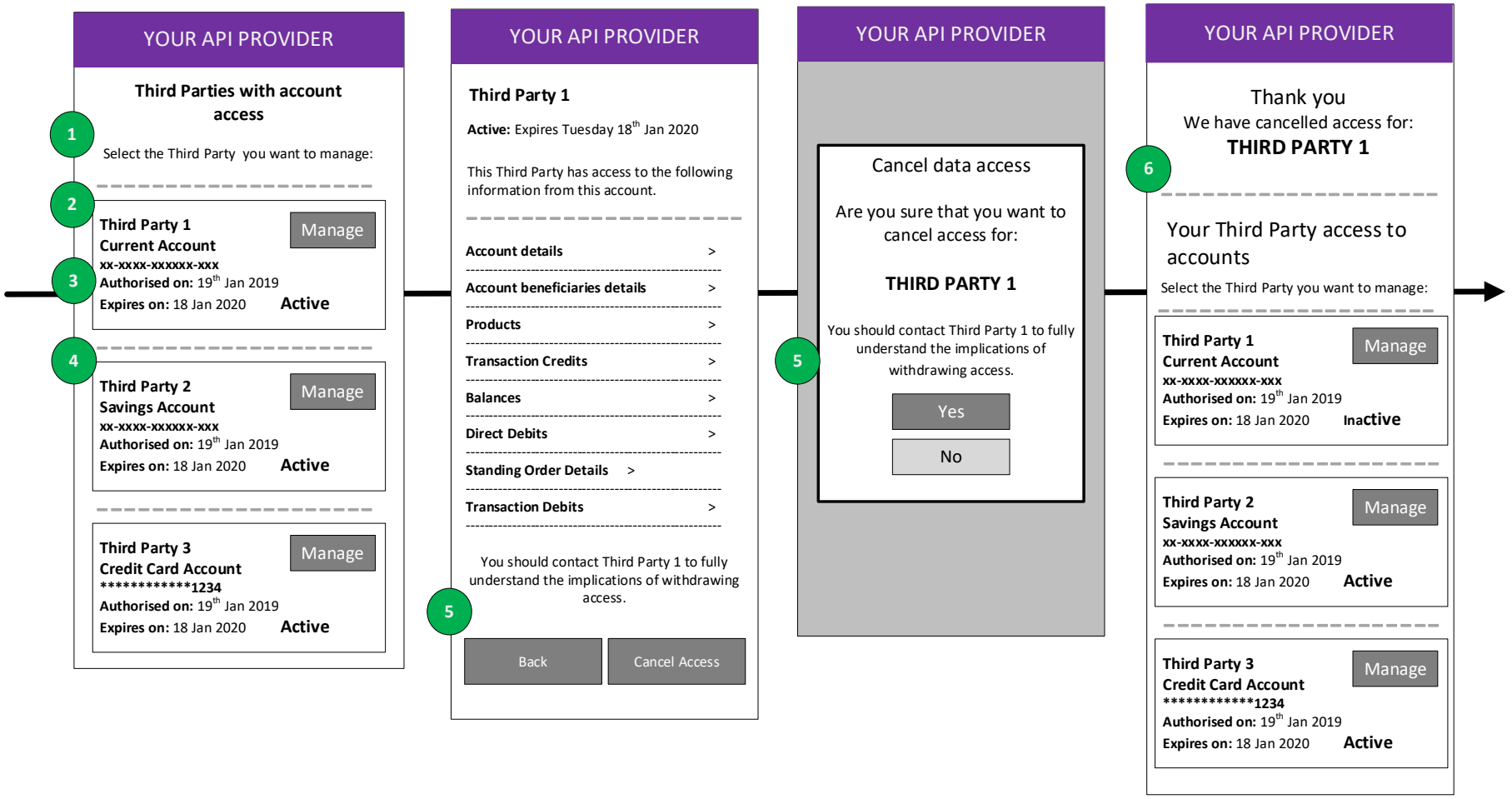
4.1.3.1 Journey description

API Providers should provide Customers with a facility to view and cancel on-going access that they have given to any Third Parties for each account held at that API Providers. This section describes how Third Party access should be displayed and how the Customer journey to cancel it should be constructed.

4.1.3.2 Journey map

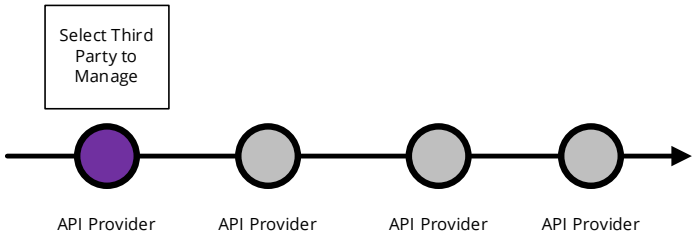


4.1.3.3 Wireframe journey



4.1.3.4 Wireframe annotations

4.1.3.4.1 Select Third Party to manage

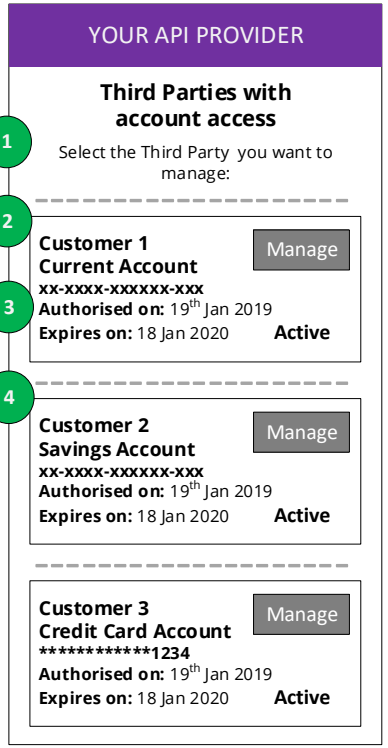


If the customer-facing entity is acting on behalf of a Third Party as its Permitted User, the Customer **should** be made aware that the Permitted User is acting on behalf of the Third Party.
This can be presented to the Customer by displaying both the Permitted User name and the Third Party name in the list of service providers, where applicable.
"Permitted User" means a person or entity who acts on behalf of an authorised payment institution or a small payment institution in the provision of payment services including account information services.

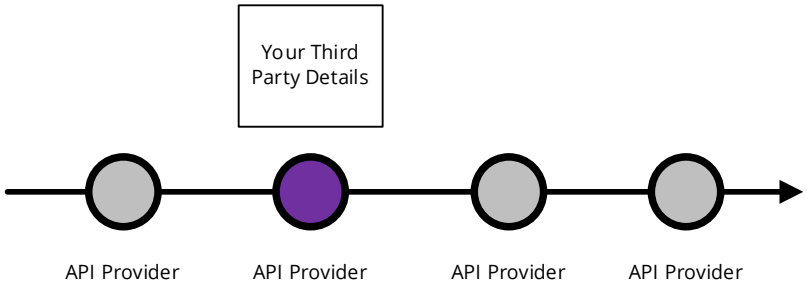
The API Provider **should** offer functionality (e.g. search, sort, filter) to enable a Customer to search for the relevant access. This will be of particular benefit as the number of consents given by a Customer to Third Parties increases.

The API Provider **should** describe the data being accessed using the structure and language recommended by API Centre.
The API Provider should present the data at a Data Cluster level and allow the Customer to expand the level of detail to show each Data Permission.
If the Customer wants to revoke consent to a Credit Card Account, the account number **should** be displayed in the same format as through a Customers existing online channels.

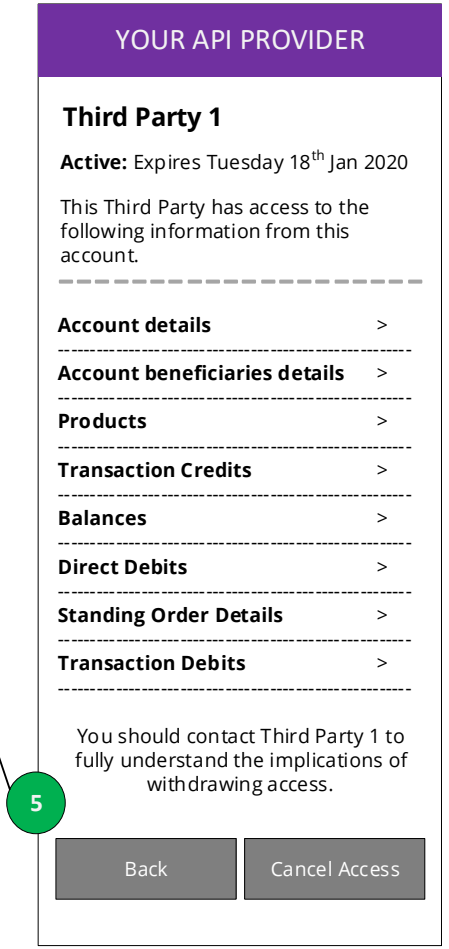
The API Provider **should** make the status of Third Party access clear by the use of emboldened words. The API Provider should also make it clear, which Customer party provided the Third Party access, in the case of joint/multiple account holders.



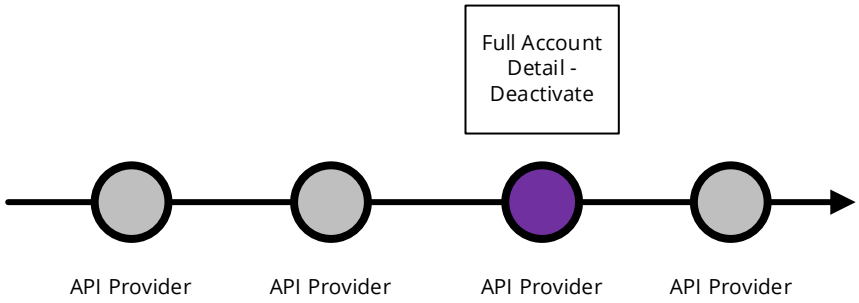
4.1.3.4.2 Your Third Parties details



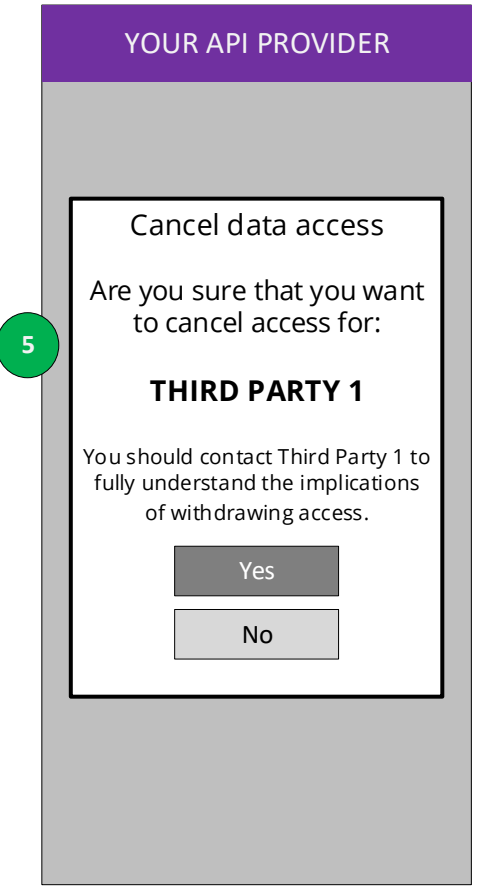
The access dashboard **must** allow a Customer to view or cancel the access they have given consent to. These functions “cancel access” and “back” should be given equal prominence when offered to the Customer.
The API Provider **should** advise Customers that they should contact the associated Third Party to inform them of the cancellation of access and/or understand the consequences of doing so.
If the Customer wants to revoke consent to a Credit Card Account, the account number **should** be displayed in the same format as through a Customers existing online channels.



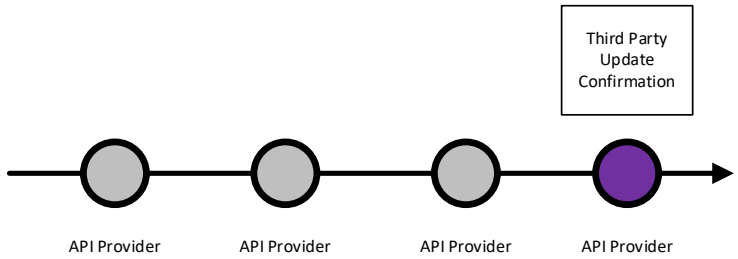
4.1.3.4.3 Full account detail – Deactivate



The API Provider **should** advise the Customer that they should contact the Third Party to inform them of the cancellation of access and/or understand the consequences of doing so.



4.1.3.4.4 Third Party update confirmation



The API Provider **must** inform the Customer that the Third Party access to specific accounts has been withdrawn by making It clear that access to the specific account is inactive.
If a Customer has a consent established against a Credit Card Account, the account number **should** be displayed to the Customer in the same format as through their existing online channels.

6

YOUR API PROVIDER

Thank you
We have cancelled access for:
THIRD PARTY 1

Your Third Party access to accounts

Select the Third Party you want to manage:

Third Party 1
Current Account
xx-xxxx-xxxxxx-xxx
Authorised on: 19th Jan 2019
Expires on: 18 Jan 2020 **Inactive**
Manage

Third Party 2
Savings Account
xx-xxxx-xxxxxx-xxx
Authorised on: 19th Jan 2019
Expires on: 18 Jan 2020 **Active**
Manage

Third Party 3
Credit Card Account
**************1234**
Authorised on: 19th Jan 2019
Expires on: 18 Jan 2020 **Active**
Manage

4.2 Permissions and Data Clusters for Account Information Services journeys

4.2.1 Permissions

In the Account Information Services Standards API design, data elements are logically grouped together into "permissions". It is at this level that Third Parties 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 Third Parties to be selective but at the same time creating a consent process that is at an acceptable level of granularity for the Customer. Details of the data elements within each permission are included in the API technical specifications.

4.2.2 Data clusters

OBIE Customer research shows that grouping permissions together and adding another layer of description aids the Customer's understanding of the data they are being asked to consent to share. This approach also allows a consistency of language across Third Parties and API Providers to provide additional comfort to Customers that they are sharing the data they intend to. If consistent language is used across all Standards Users this will drive Customer 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 Customer understanding.

4.2.3 Data clusters structure and language

The following table describes how permissions should be grouped into Data Clusters and the language that **should** be used to describe the data at each of these levels. Both Third Parties and API Providers **should** describe the data being shared at a Data Cluster level and allow the Customer 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, and/or the currency of the account.*	Currency of the account, Nickname of account (E.g. 'Jakes Household account')
		Accounts Detail	*Your account name, number*	Account Name, Account Number
	Balances	Balances	*Your account balance*	Amount, Currency, Credit/Debit, Type of Balance, Date/Time, Credit Line
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, 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 information
		Standing Order Detail	*Details of your Standing Orders*	Details of Creditor Account Information (Name, Account) (plus all data provided in Standing Order Basic)
	Direct debits	Direct Debits	*Your Direct Debits*	Mandate info, Status, Name, Previous payment information

Data cluster language	API end points	Permissions	Permissions language	Information available
	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.

Data cluster language	API end points	Permissions	Permissions language	Information available
		Transactions Basic	*Your transactions*	Transaction Information on payments for both credits in and debits out of the Customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code. Does not include information about the payer/payee.
		Transactions detail	*Details of your transactions*	Transaction Information on payments made both credits in and debits out of the Customer's account (Reference, Amount, Status, Booking Data Info, Value Date info, Transaction Code). Includes information about the payer/payee.
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.
	Offers	Offers	*Offers available on your account*	Balance transfer, promotional rates, limit increases, start and end dates.
Contact and party details	Account specific: Parties	Party	*The full legal name(s) of account holder(s).*	The name of the account. Full Legal Name(s), Account Role(s), Beneficial Ownership, Legal Structure, Address or addresses, telephone numbers and email address as held by the bank/card issuer and party type (sole/joint etc.).

Data cluster language	API end points	Permissions	Permissions language	Information available
	Party		*Address(es), telephone number(s) and email address(es)**	

4.2.4 Optional data

If, with the consent of the Customer, a Third Party requests additional information, an API Provider may only provide this to a Third Party if it has authority from the Customer to use and disclose the additional information in that manner.

4.2.5 Relevance of data cluster against product type

The Third Party should ensure that is has business rules that manage the relationship between Data Cluster to product type and omit access to data clusters that are irrelevant to a product type, as well as its service offering.

For example, if a Third Party requests a cluster of data that is irrelevant to the product type associated to a payment account e.g. Direct Debit cluster requested for a Savings Account product type, the API Provider may provide that cluster as empty.

NOTE: With respect to the clusters and permissions language, the API Provider should consider whether the language that is displayed to the Customer is appropriate when the information being accessed relates to more than one party. For example, "Your data" may need to be adapted to just “data” to indicate to the Customer that the account information being displayed may not be solely specific to them, as is the case of joint accounts when the account information of both parties is requested.

5 Payment Initiation Services (PIS)

One of the primary ambitions of the Guidelines is to provide simplification and consistency of the API Standards implementation. Therefore, we have defined and illustrated a core set of payment initiation journeys.

The API Centre API Standards support Payment Initiation Services that enable a Third Party to:

- initiate a single payment order, with explicit consent, from the Customer's account held at their API Provider.
- establish a long lived enduring payment consent that can be used to initiate multiple payment orders, from the Customer's account held at their API Provider that falls within consented parameters.

The Third Party is then further able to retrieve the status of a payment order and to retrieve a consent from the API Provider.

This section describes how each of the Standard Users (Third Parties and API Providers) in the delivery of these services can optimise the Customer experience for these services. The key components are:

- Payments Initiation Consent – A Customer giving consent to a Third Party to request payments initiation from their API Provider.
- Third Party Enduring Payment Consent Dashboard and Revocation – facility to enable a Customer to view and cancel consents given to that Third Party.
- API Provider Enduring Payment Consent Dashboard and Revocation – facility to enable a Customer to view all Third Parties that have access to their account(s) and the ability to cancel that access. This should be available on those channels that the Customer uses to manage their accounts with the API Provider and be easy and intuitive for the Customer to find and use.
    - This facility should not include unnecessary steps, superfluous information or language which could discourage the use of Third Party services or divert the Customer from the access management process.

Furthermore, it provides some clarifications to these Standard Users on the use of the APIs which are not covered by the technical specifications, and some best practice guidelines for implementation of the Customer journeys.

5.1 Mandatory Payment Initiation Service journeys – Single payments

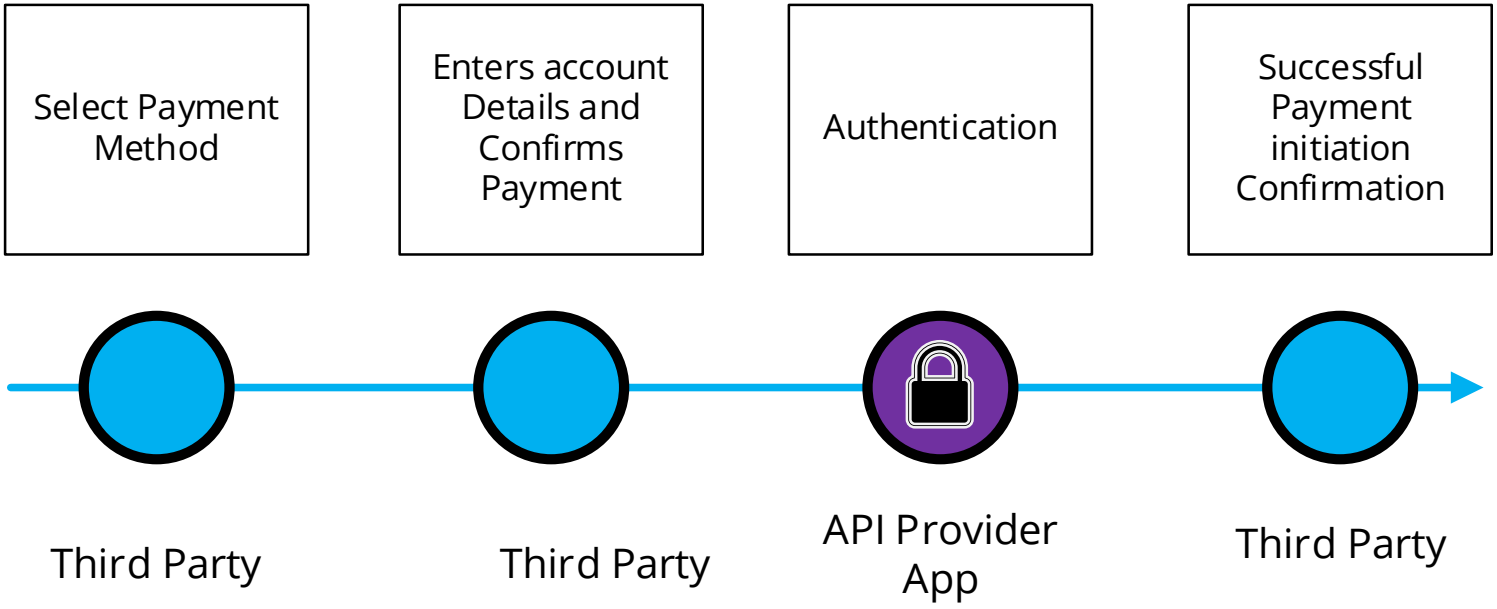
5.1.1 Single domestic payments – Account selection at Third Party

5.1.1.1 Journey description

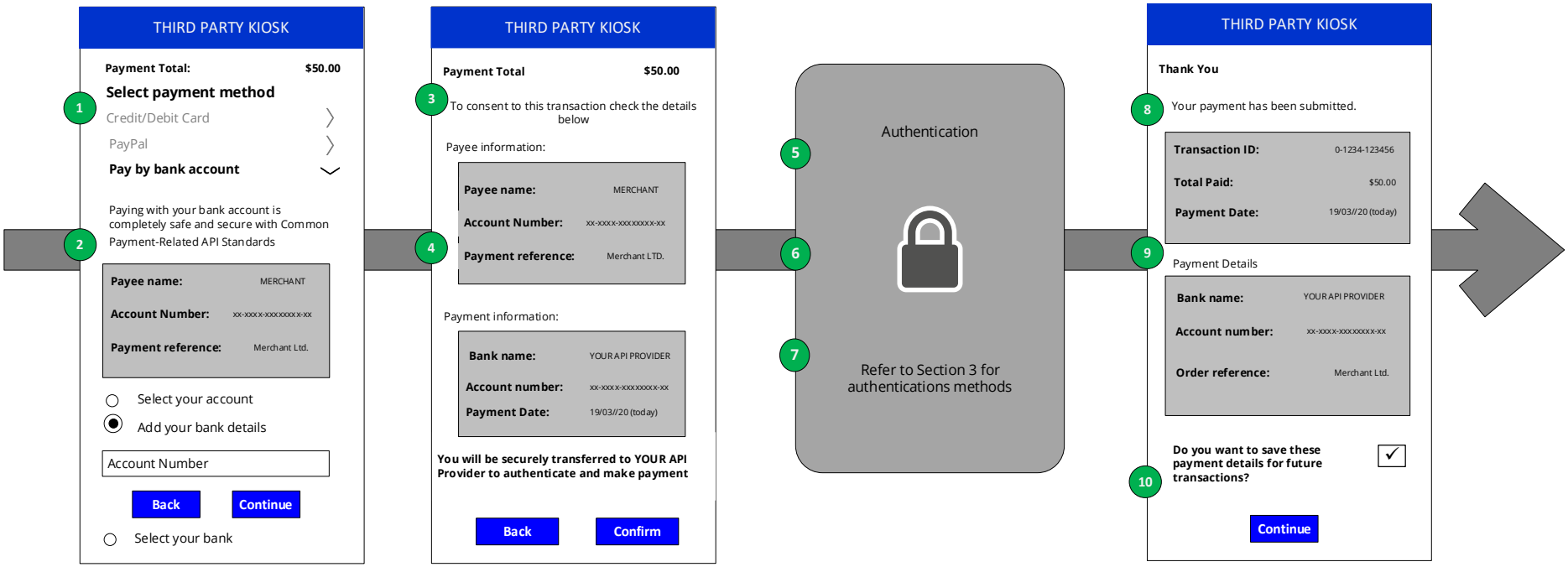
A Customer can initiate an instruction to their API Provider to make a one-off payment for a specific amount to a specific payee by providing their consent to a Third Party.

Once all information for a complete payment order (including the Customer's account details) is passed from the Third Party to the API Provider, and the Customer has been authenticated, the Customer should be directed back to the Third Party domain without any further steps taking place in the API Provider domain.

5.1.1.2 Journey map

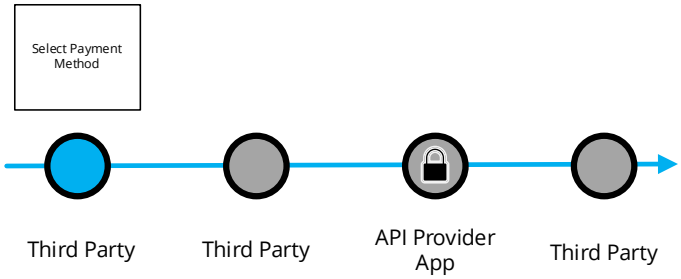


5.1.1.3 Wireframe journey



5.1.1.4 Wireframe annotations

5.1.1.4.1 Select payment method



Minimum Set of Parameters

The Third Party **must** either allow the Customer to specify the below minimum set of parameters or pre-populate them for the Customer:

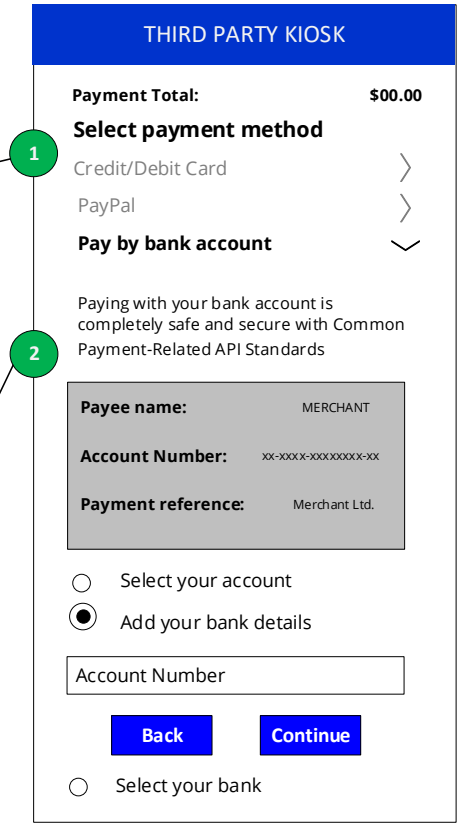
- Payment Amount and Currency.
- Payee Account Name.
- Payee Account Identification details (e.g. account number).
- Payment Reference - This is optional but it is good practice to be populated for a payment.
- Any supplementary information required which the API Provider has published as required and is specific to that API Provider.

Customer payment Account Selection

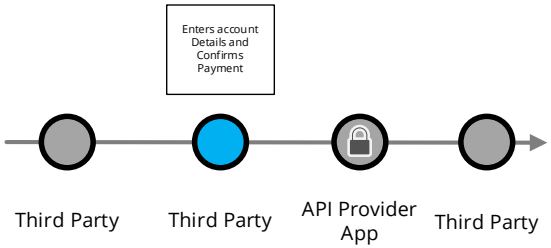
The Third Party **must** provide the Customer at least one of the following options:

- Enter their Payer payment Account Identification details. The Third Party must allow Customers to enter their payment Account Identification details in at least one of the ways specified in the API Centre API Specifications.
- Select their Account Identification details (this assumes they have been saved previously).
- Select their API Provider in order to select their Customers payment Account from there later on in the journey.

Note 1: In some of the above cases, the Third Party may also need the Customer to provide their API Provider name so that the Third Party can check whether an API Provider will be able to match the account identifier to the underlying Customer payment account.



5.1.1.4.2 Enters the account details and confirms payment



Customer Consent to Third Party

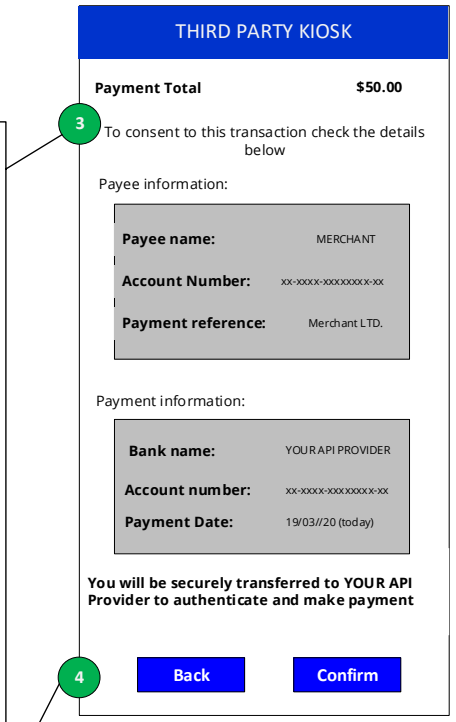
The Third Party **should** request the Customer consent to the payment in a clear and specific manner. The Third Party **must** display the following information in the consent screen:

- Payment Amount and Currency.
- Payee Account Name.
- Payment Reference, and any supplementary info, if it has been entered by The Customer or prepopulated by the Third Party in item #1.
- Customer payment Account Identification and/or the selected API Provider (based on item #2 options)
  - *Note 1: if* Customer *payment Account identification is selected in item #2, the* Third Party ***should*** *mask the* Customer *payment Account details on the consent screen. Otherwise, if the* Customer *payment Account identification has been input by the* Customer *in item #2, the* Third Party ***should not*** *mask these details to allow the* Customer *to check and verify correctness.*
  - *Note 2: if* Customer *payment Account identification is provided by the* Customer *in item #2, the* Third Party *could use this to identify and display the* API Provider *without having to ask the* Customer.

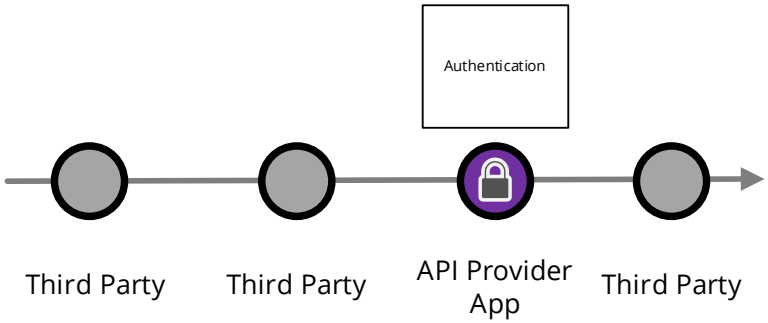
For Payee Account Identification details :

- If this has been provided by the Customer in item #1, then the Third Party **must** also display this in the consent screen to allow the Customer to check and verify correctness.
- If this has been pre-populated by the Third Party (e.g. in a eCommerce payment scenario) the Third Party could choose whether to display this information or not.

The Third Party **should** provide messaging to inform the Customer that they will be taken to their API Provider to complete the payment.
Example wording: *"You will be securely transferred to YOUR API PROVIDER to authenticate and make the payment".*



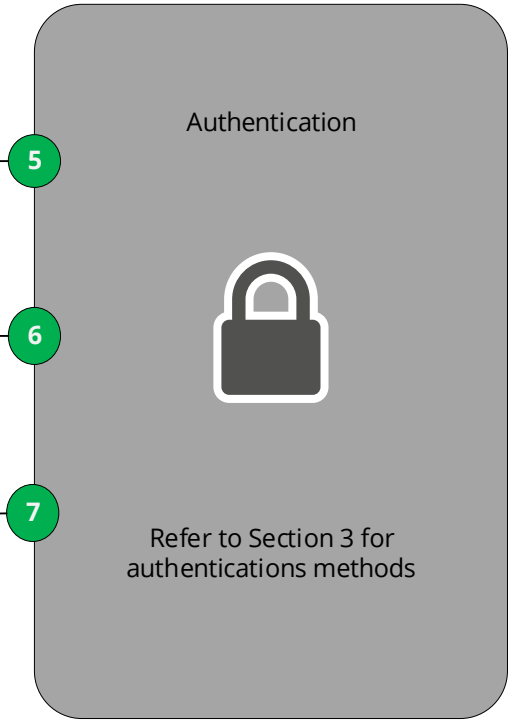
5.1.1.4.3 Authentication



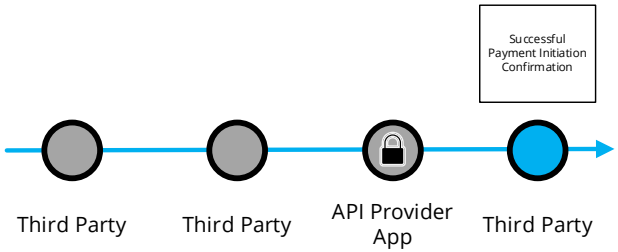
Generic Third Party to API Provider redirection screen and message.

An API Provider **should** apply SCA including dynamic linking.
The API Provider authentication **should** have no more than the number of steps that the Customer would experience when directly accessing the API Provider channel.

An API Provider could also display a message to prompt Customers to authenticate to continue with their payment instruction.



5.1.1.4.4 Successful payment initiation confirmation



Third Party Confirmation
A Third Party **must** display the information received from the API Provider. This information may include:

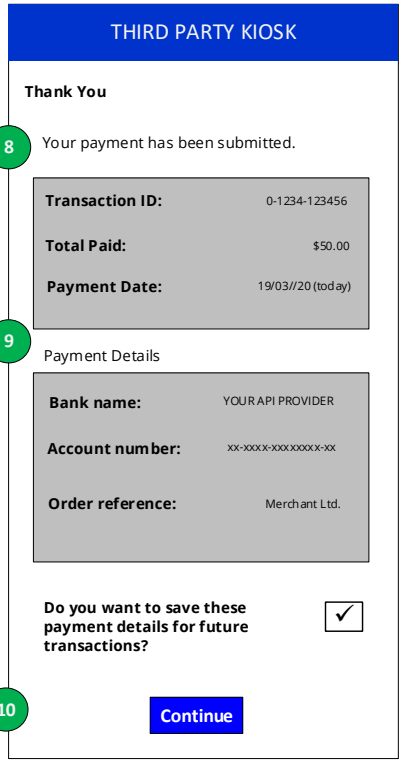
- The unique identifier assigned to the payment instruction by the API Provider.
- The payment status (and status update date & time) – Confirmation of successful payment initiation.

If received by an API Provider, the Third Party 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 API Provider charges (where applicable).

If a Customer provides their payment account identification details (as per item #2 options), the Third Party could, with the consent of the Customer, save the account details for future transactions (such as making further payments or initiating refunds back to a Customer) where this is part of the payment initiation service explicitly requested by the Customer. For example, a merchant, upon request from the Customer, may initiate a refund back to the Customer, by instructing the same Third Party that initiated the initial Customer transaction to use the saved Customer payment account identification details as the beneficiary details for the refund. This will be dependant on the same Third Party being used by both the Customer and the merchant and their specific contractual terms.
Moreover, the Third Party can use this consent to provide a hint of the Customer identity using the customer identifier as part of the payment request to enable the subsequent payment journey.

Further Payment Status Update
The Third Party **should** follow up with the API Provider in order to check and update the Customer with the most updated information that can be received by an API Provider in relation to the execution of the payment.

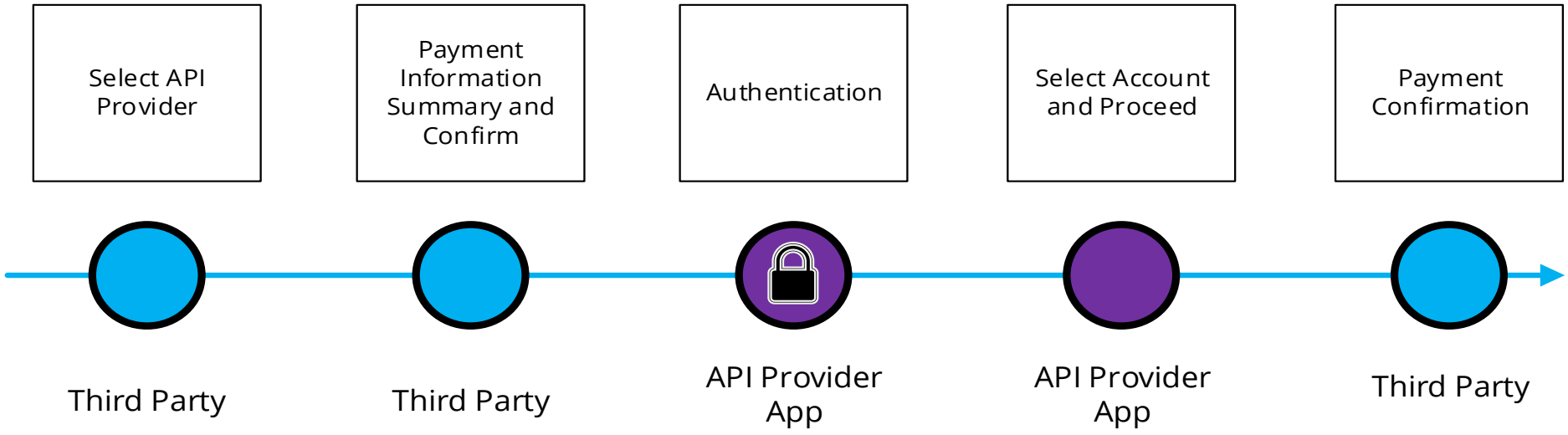


5.1.2 Single domestic payments – Account selection at API Provider

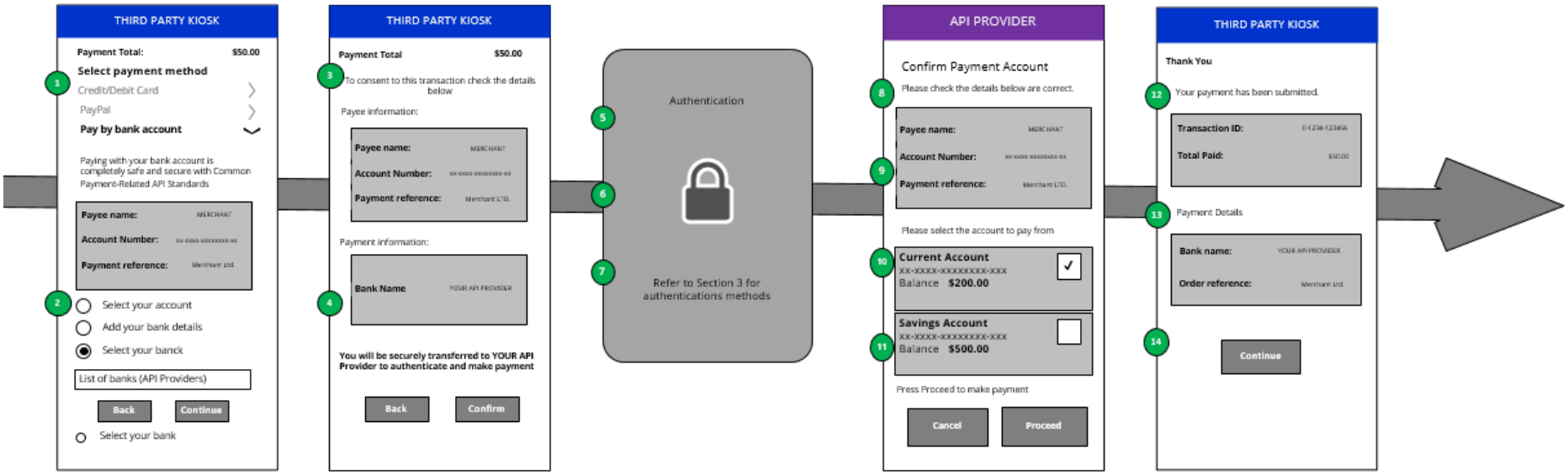
5.1.2.1 Journey description

There are cases where the payment order submitted by Third Parties to API Providers is incomplete, such as where the Customer's account selection has not yet occurred.

5.1.2.2 Journey map

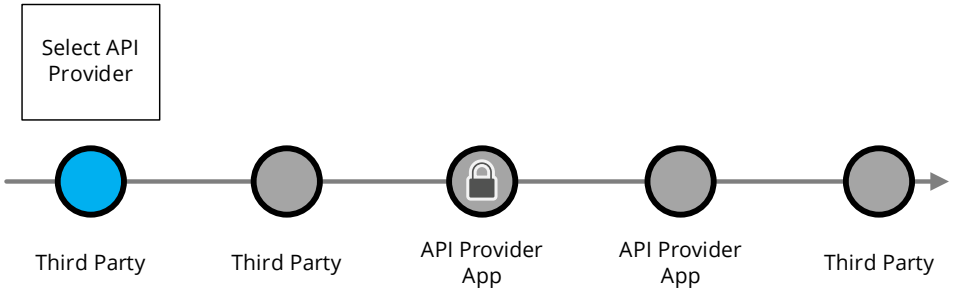


5.1.2.3 Wireframe journey



5.1.2.4 Wireframe annotations

5.1.2.4.1 Select API Provider



Minimum Set of Parameters

A Third Party **must** either allow a Customer to specify the below minimum set of parameters or pre-populate them for the Customer:

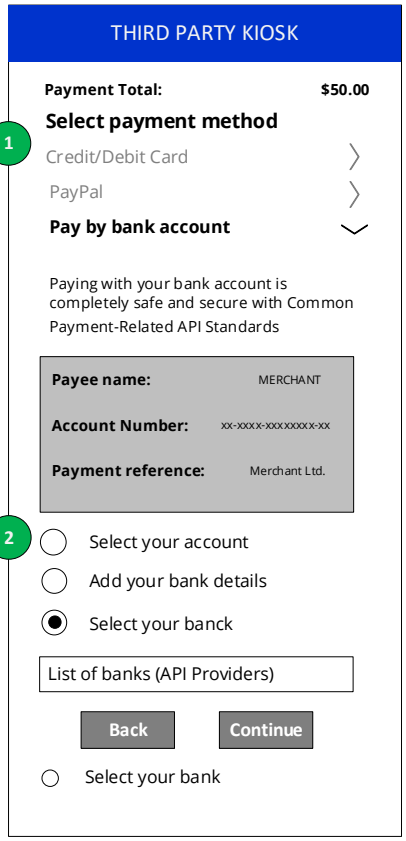
- Payment Amount and Currency.
- Payee Account Name.
- Payee Account Identification details (e.g. account number).
- Payment Reference - This is optional but it is good practice to be populated for a payment.
- Any supplementary information required which the API Provider has published as required and is specific to that API Provider.

Customer payment Account Selection

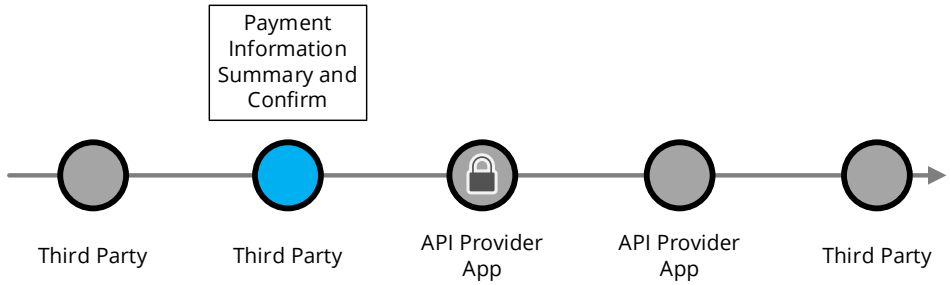
A Third Party **must** provide the Customer at least one of the following options:

- Enter their Payer payment Account Identification details.
- A Third Party must allow the Customer to enter their payment Account Identification details in at least one of the ways specified in the API Centre API Specifications.
- Select their Account Identification details (this assumes they have been saved previously).
- Select their API Provider in order to select their Customer payment Account later on in the journey.

Note 1: In some of the above cases, the Third Party may also need the Customer to provide their API Provider name so that the Third Party can check whether an API Provider will be able to match the account identifier to the underlying Customer payment account.



5.1.2.4.2 Payment Information summary and consent



Customer Consent to Third Party

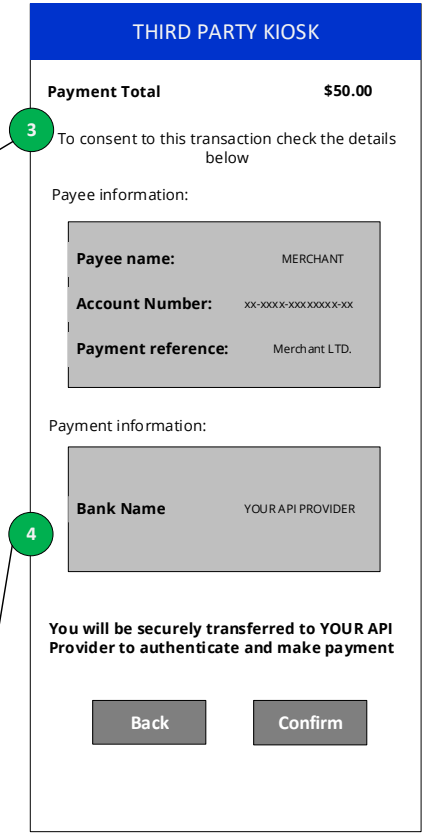
A Third Party **should** request the Customer consent to the payment in a clear and specific manner. A Third Party **must** display the following information in the consent screen:

- Payment Amount and Currency.
- Payee Account Name.
- Payment Reference, and any supplementary info, if it has been entered by the Customer or prepopulated by a Third Party in item #1.
- Customer payment Account Identification and/or the selected API Provider (based on item #2 options)
  - *Note 1: if* Customer *payment Account identification is selected in item #2, the* Third Party ***should*** *mask the* Customer *payment Account details on the consent screen. Otherwise, if the* Customer *payment Account identification has been input by* Customer's *in item #2, a* Third Party ***should not*** *mask these details to allow* Customer's *to check and verify correctness.*
  - *Note 2: if* Customer *payment Account identification is provided by a* Customer *in item #2, a* Third Party *could use this to identify and display the* API Provider *without having to ask the* Customer.

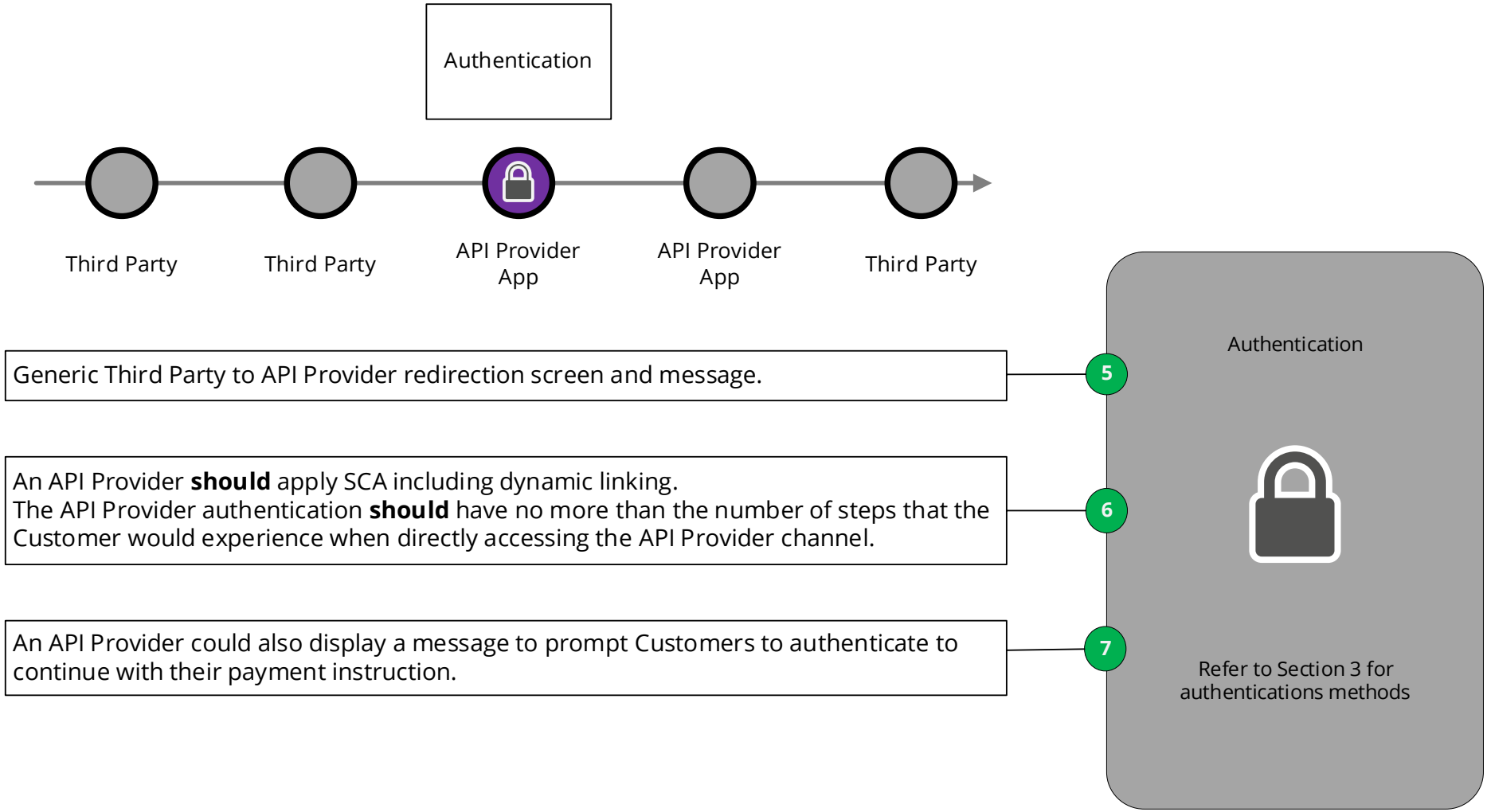
For Payee Account Identification details :

- If this has been provided by the Customer in item #1, then a Third Party **must** also display this in the consent screen to allow a Customer to check and verify correctness.
- If this has been pre-populated by a Third Party (e.g. in a eCommerce payment scenario) a Third Party could choose whether to display this information or not.

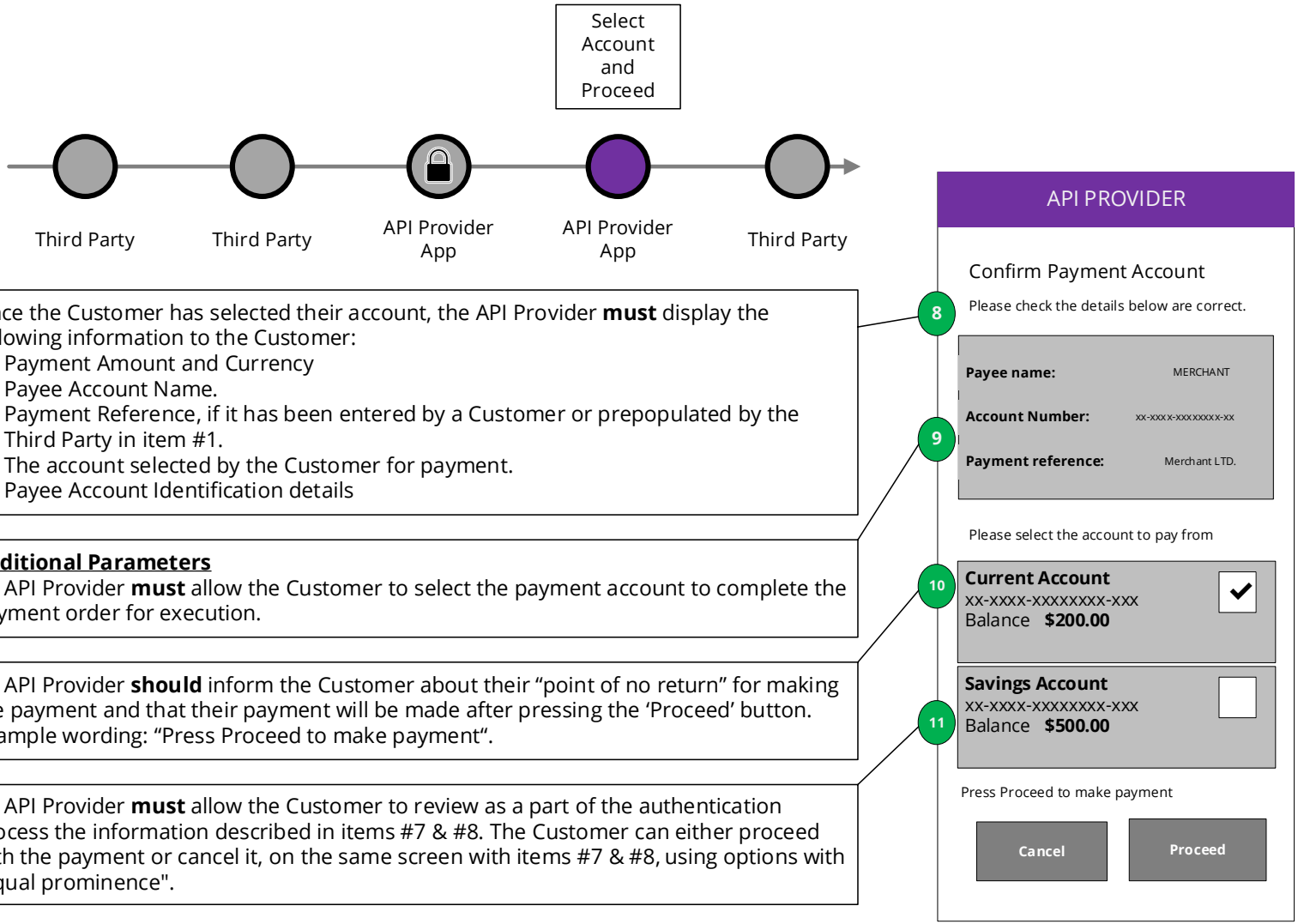
A Third Party **should** provide messaging to inform the Customer that they will be taken to their API Provider to complete the payment.
Example wording: *"You will be securely transferred to YOUR API PROVIDER to authenticate and make the payment".*



5.1.2.4.3 Authentication



5.1.2.4.4 Select account and proceed



Once the Customer has selected their account, the API Provider **must** display the following information to the Customer:

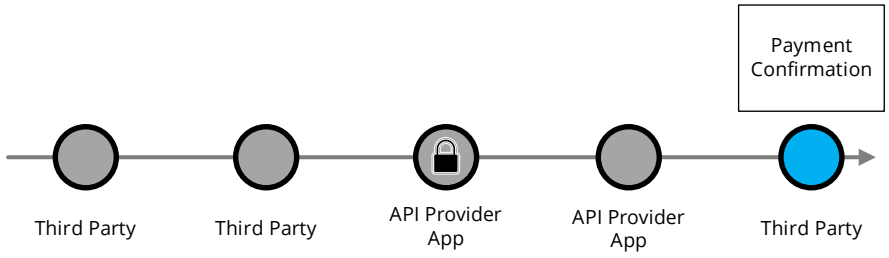
- Payment Amount and Currency
- Payee Account Name.
- Payment Reference, if it has been entered by a Customer or prepopulated by the Third Party in item #1.
- The account selected by the Customer for payment.
- Payee Account Identification details

Additional Parameters
An API Provider **must** allow the Customer to select the payment account to complete the payment order for execution.

An API Provider **should** inform the Customer 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".

An API Provider **must** allow the Customer to review as a part of the authentication process the information described in items #7 & #8. The Customer can either proceed with the payment or cancel it, on the same screen with items #7 & #8, using options with "equal prominence".

5.1.2.4.5 Payment confirmation



Third Party Confirmation
A Third Party **must** display the information received from the API Provider. This information may include:

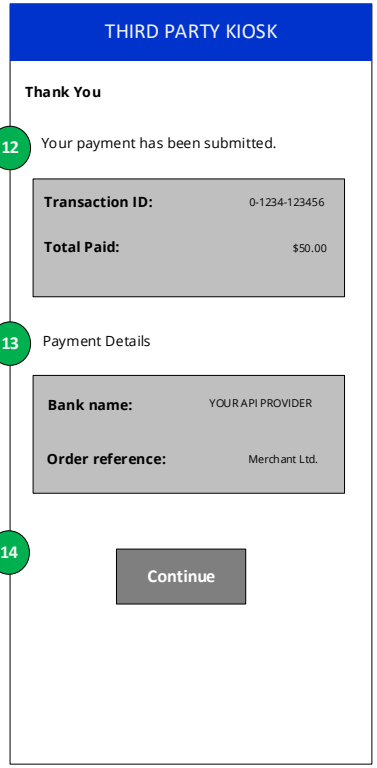
- The unique identifier assigned to the payment instruction by the API Provider.
- The payment status (and status update date & time) – Confirmation of successful payment initiation.

If received by an API Provider, the Third Party 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).
- API Provider charges (where applicable).

If a Customer provides their payment account identification details (as per item #2 options), the Third Party could, with the consent of the Customer, save the account details for future transactions (such as making further payments or initiating refunds back to Customers) where this is part of the payment initiation service explicitly requested by the Customer. For example, a merchant, upon request from the Customer, may initiate a refund back to the Customer, by instructing the same Third Party that initiated the initial Customer transaction to use the saved Customer payment account identification details as the beneficiary details for the refund. This will be dependant on the same Third Party being used by both the Customer and the merchant and their specific contractual terms.
Moreover, the Third Party can use this consent to provide a hint of the Customer identity using the customer identifier as part of the payment request to enable the subsequent payment journey.

Further Payment Status Update
A Third Party **should** follow up with the API Provider in order to check and update the Customer with the most up to date information that can be received by an API Provider in relation to the execution of the payment.



5.2Optional Payment Initiation Services journeys – Enduring payment consent

5.2.1 Establishing an Enduring Payment Consent – Account selection at Third Party

5.2.1.1 Journey description

A Customer can provide their enduring consent to a Third Party to initiate multiple one-time payments from a specific account held at an API Provider.

An enduring payment consent provided by a Customer allows a Third Party to initiate multiple one-time payments that fall within the agreed parameters of that enduring consent without needing the Customer to authenticate each individual payment.

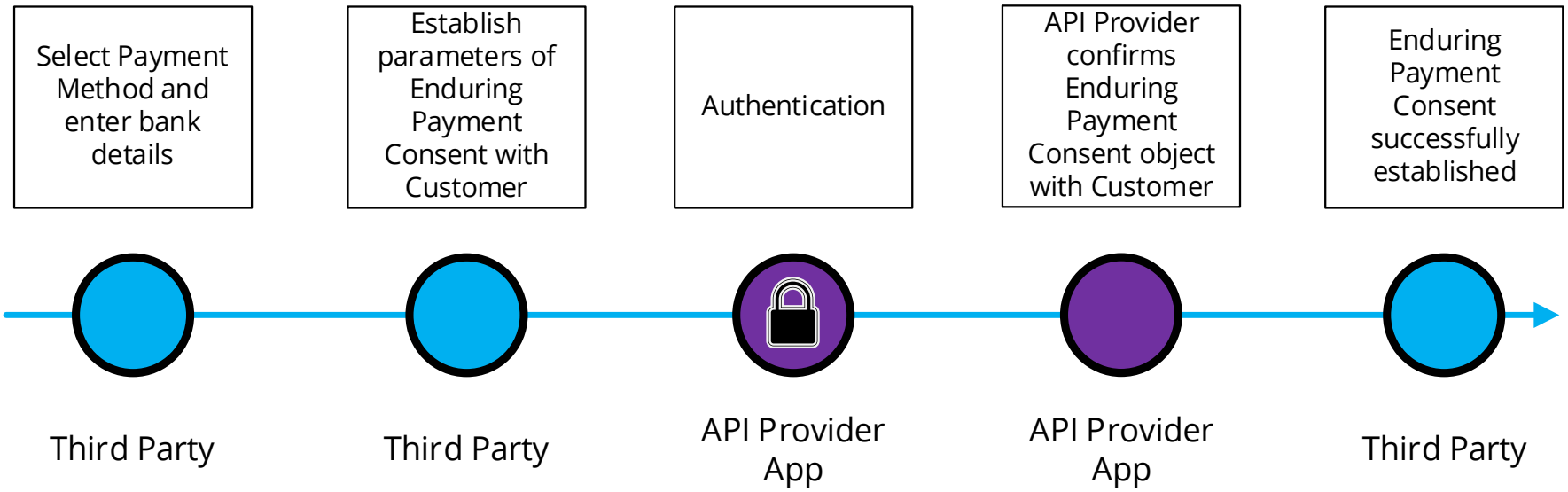
The specification data model defines the variable parameters of the consent object that can be agreed with the Customer[2].

Once a Third Party establishes the parameters of the consent with Customer, the required agreed consent information is passed from the Third Party to the API Provider and the Customer is asked to authenticate and confirm the consent with the API Provider. The customer should be directed back to the Third Party domain without any further steps taking place in the API Provider domain.

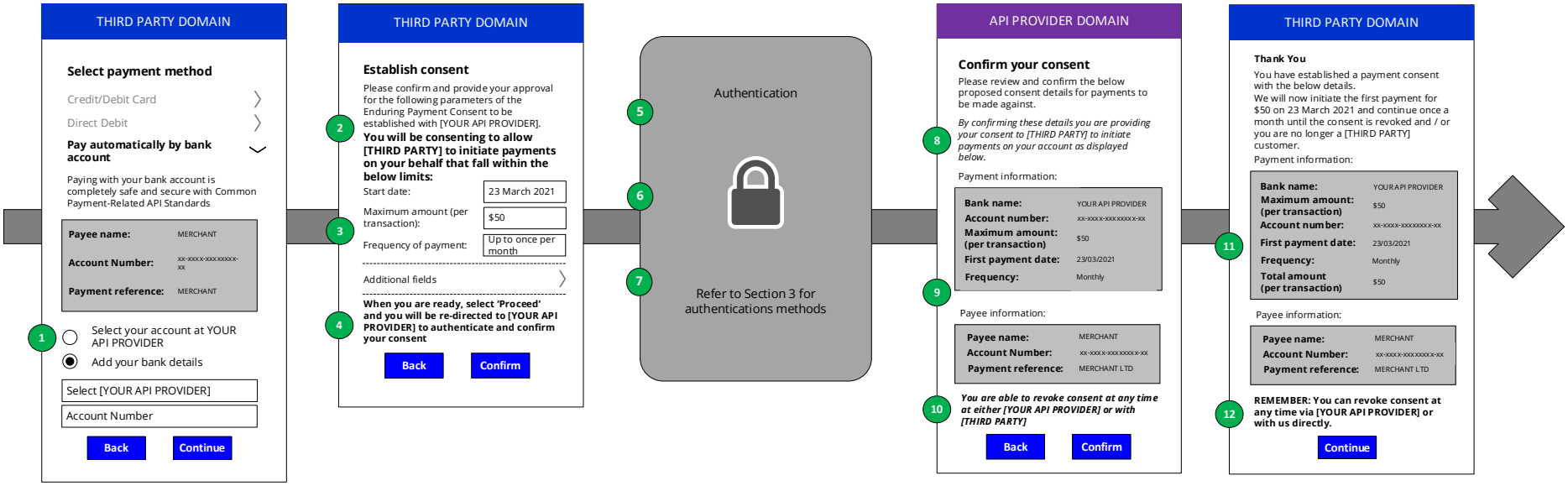
Enduring Payment Consent can be acquired via any of the authentication flows as detailed in Section 3 – 'Authentication Methods'.

[2] https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/pages/800031713/Enduring+Payment+Consents+-+v2.1.0#Data-Model

5.2.1.2 Journey map

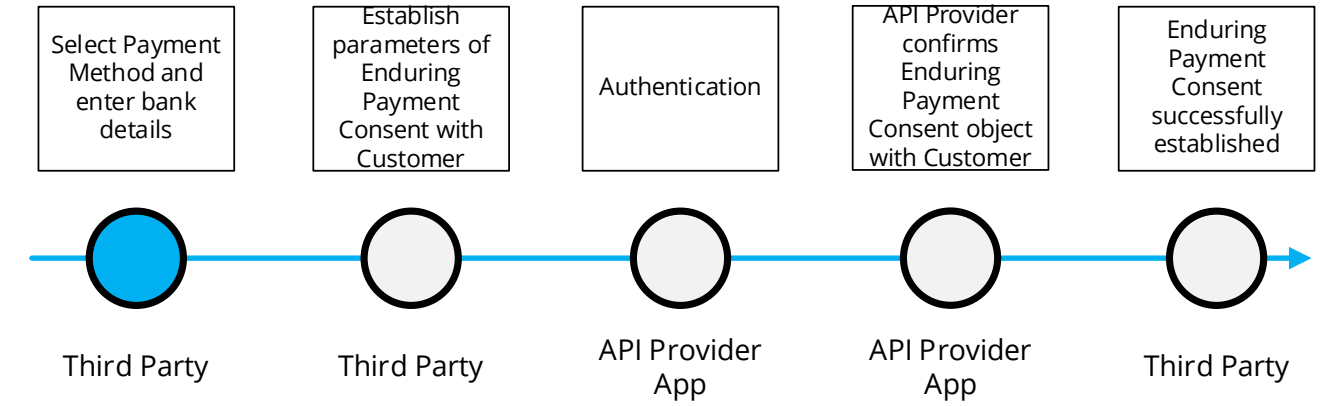


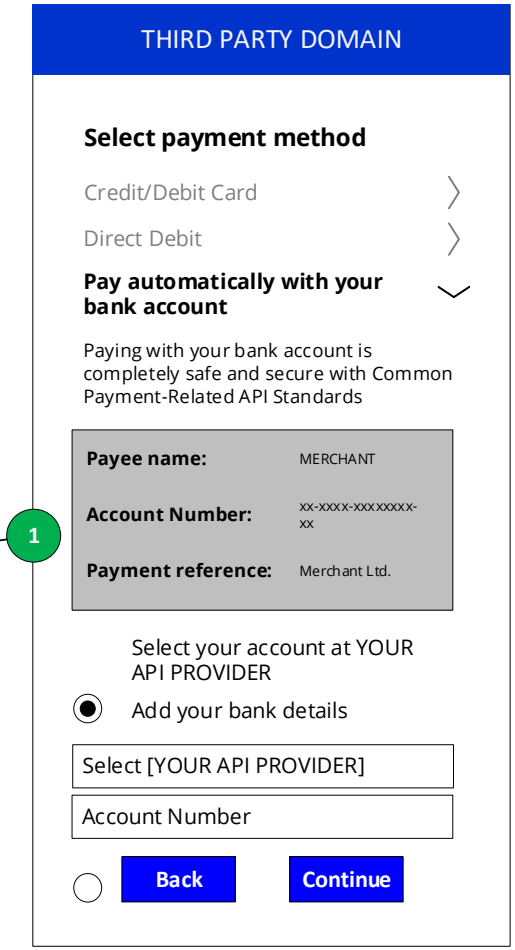
5.2.1.3 Wireframe journey



5.2.1.4 Wireframe annotations

5.2.1.4.1 Select payment method and bank details





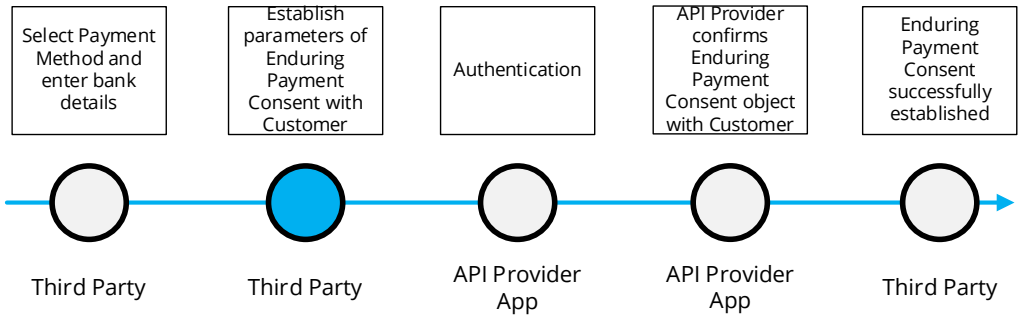
<u>Customer payment Account Selection</u>

The Third Party **must** provide the Customer at least one of the following options:

- Enter their Payer payment Account Identification details. The Third Party must allow Customers to enter their payment Account Identification details in at least one of the ways specified in the API Centre API Specifications.
- Select their Account Identification details (this assumes they have been saved previously).
- Select their API Provider in order to select their Customers payment Account from there later on in the journey.

Note 1: In some of the above cases, the Third Party may also need the Customer to provide their API Provider name so that the Third Party can check whether an API Provider will be able to match the account identifier to the underlying Customer payment account.

5.2.1.4.2 Establish parameters of Enduring Payment Consent with Customer



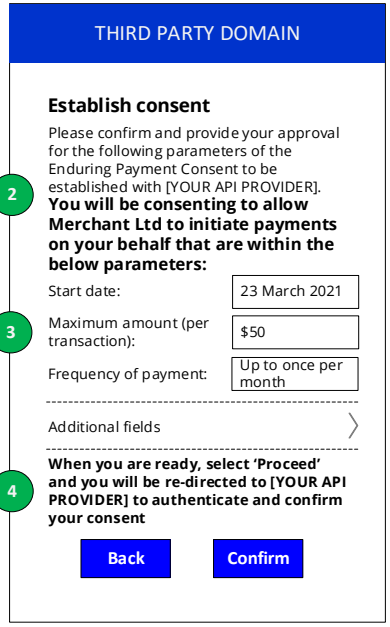
The Third Party **should** provide messaging to inform the Customer that in completing this process, they will be consenting to allow a Third Party to act on their account to initiate payments that fall within the agreed consent parameters.
Example wording: "You will be consenting to allow Merchant Ltd to initiate payments on your behalf that fall within the below parameters:"

The Third Party **should** request the Customer consent to the enduring payment in a clear and specific manner. The Third Party **should** clearly display and communicate the parameters of the proposed consent in plain English and in language that the Customer is familiar with.
The Third Party **must** display the following mandatory elements of the Enduring Consent Object to the Customer as part of the establish consent step:

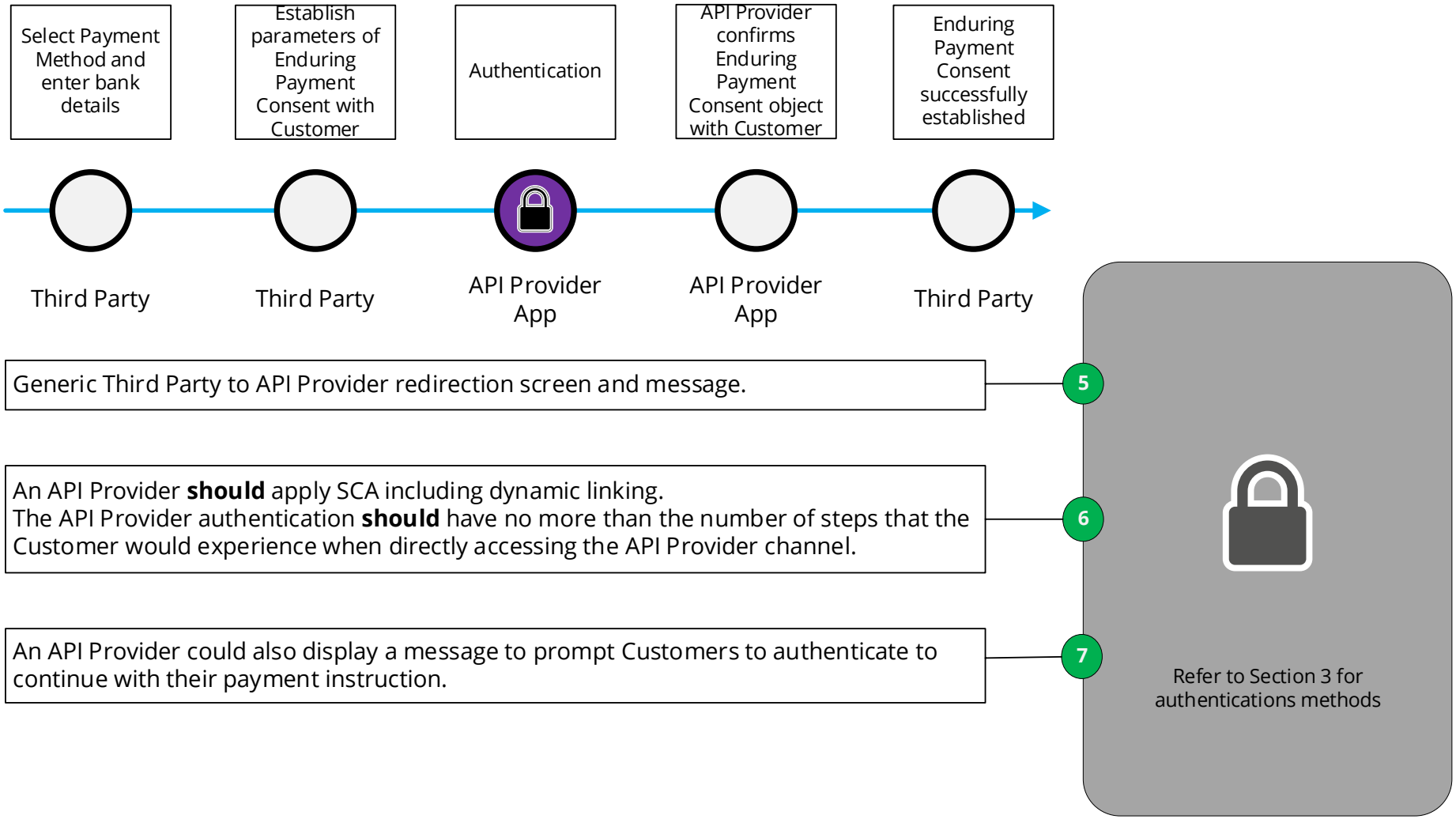
- FromDateTime - which defines when the enduring consent will be valid from ('Start date' in example)
- MaximumAmount – which specifies the maximum individual payment amount that is authorised using the Enduring Payment Consent ('Maximum Amount' in example)
- Frequency & Frequency/Period – these fields define the amount of payments that can be initiated within a given period as defined from the defined start date.

All optional elements of the enduring consent object can be implemented by a Third Party to meet their Customer use cases and **should** be displayed to the Customer in this screen and clearly articulated before proceeding to authentication.

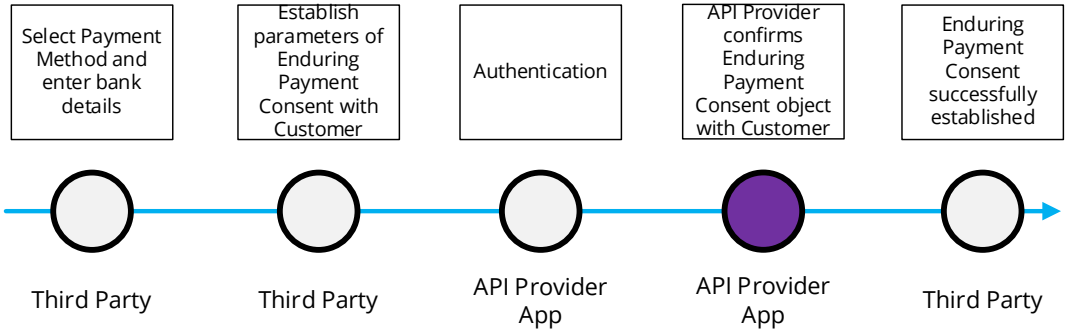
The Third Party **should** provide messaging to inform the Customer that they will be taken to their API Provider to complete the payment.
Example wording: "You will be securely transferred to YOUR API PROVIDER to authenticate and confirm your consent".



5.2.1.4.3 Authentication



5.2.1.4.4 API Provider confirms Enduring Payment Consent object with Customer



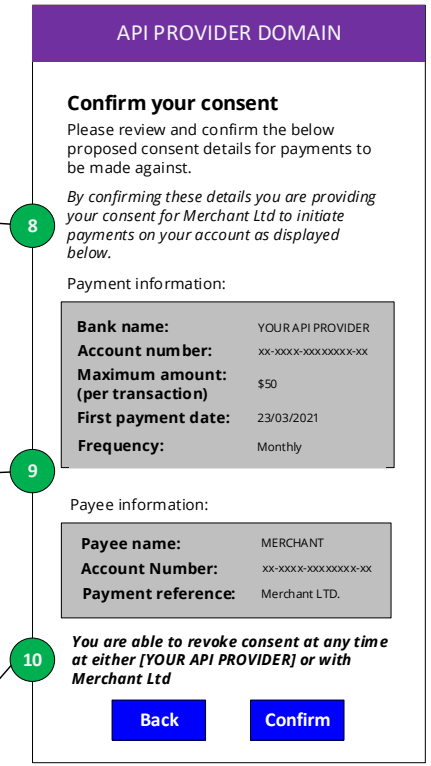
The API Provider **should** inform the Customer that following this step, the Third Party will be able to initiate payments on the specified account within the agreed parameters.

The API Provider **must** display as minimum the Mandatory elements of the enduring consent object to ensure the Customer is explicitly aware of these details (unless an SCA exemption is being applied). These details **must** be displayed as part of the authentication journey on at least one of the following screens without introducing additional confirmation screens.

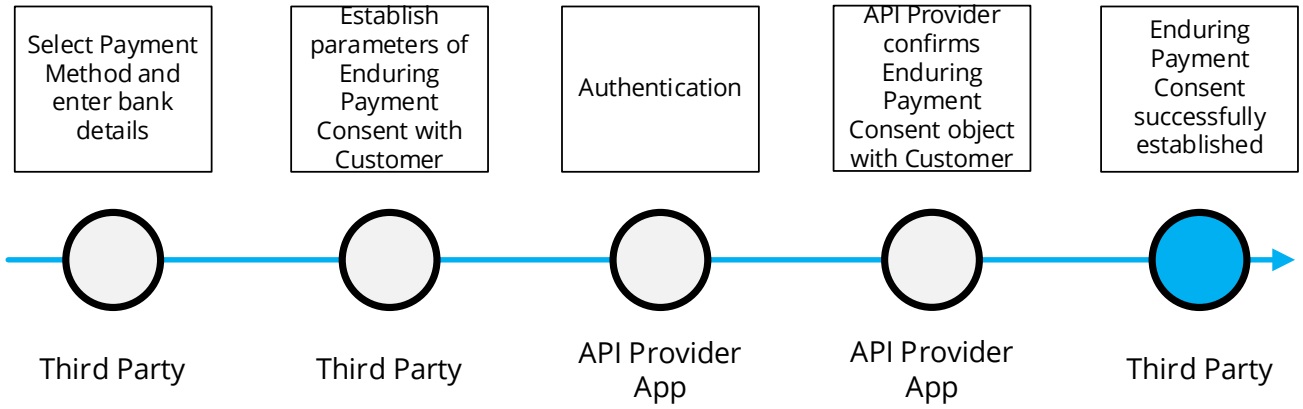
- API Provider confirms Enduring Payment Consent object with Customer (recommended)
- API Provider to Third Party redirection Screen

The API Provider **must** display all other optional parameters passed from the Third Party as part of the Enduring Payment Consent object along with the payee details and payment reference entered with the Third Party.
If an enduring-payment-consent parameter is not specified, the API Provider **should not** enforce a specific limit for the use of the enduring-payment-consent. E.g., if no TotalAmount is specified, there is no specific restriction on the total of all successful InstructedAmount(s) that may be initiated during the lifetime of the enduring-payment-consent.
Note: *The MaximumAmount field is a mandatory parameter of the enduring-payment-consent and as such* ***must*** *be populated when submitted for authentication by a Third Party*

The API Provider **should** ensure the Customer is aware that they are able to control authorised enduring payment content(s) at any time directly with their API Provider or with Merchant Ltd.

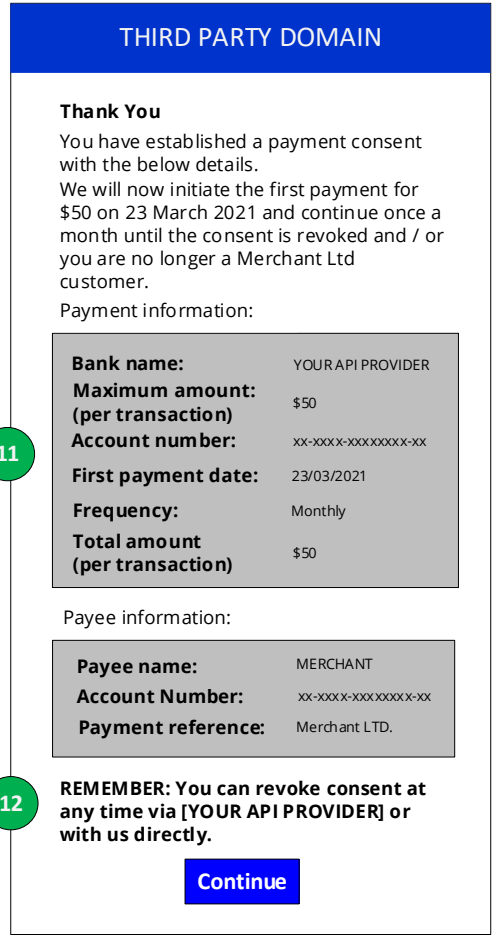


5.2.1.4.5 Enduring Payment Consent successfully established



The Third Party **should** re-confirm with the Customer, in plain English the parameters of the consent that has been established and the expected activity to be carried out on the Customer account.
This **should** include the detail of the enduring consent object, including both payer and payee account details as well as the agreed and consented variable parameters.

The Third Party **should** ensure the Customer is aware that they are able to control authorised enduring payment consent(s) at any time, directly with their API Provider or with the Third Party.



5.2.2 Establishing an Enduring Payment Consent – Account selection at API Provider

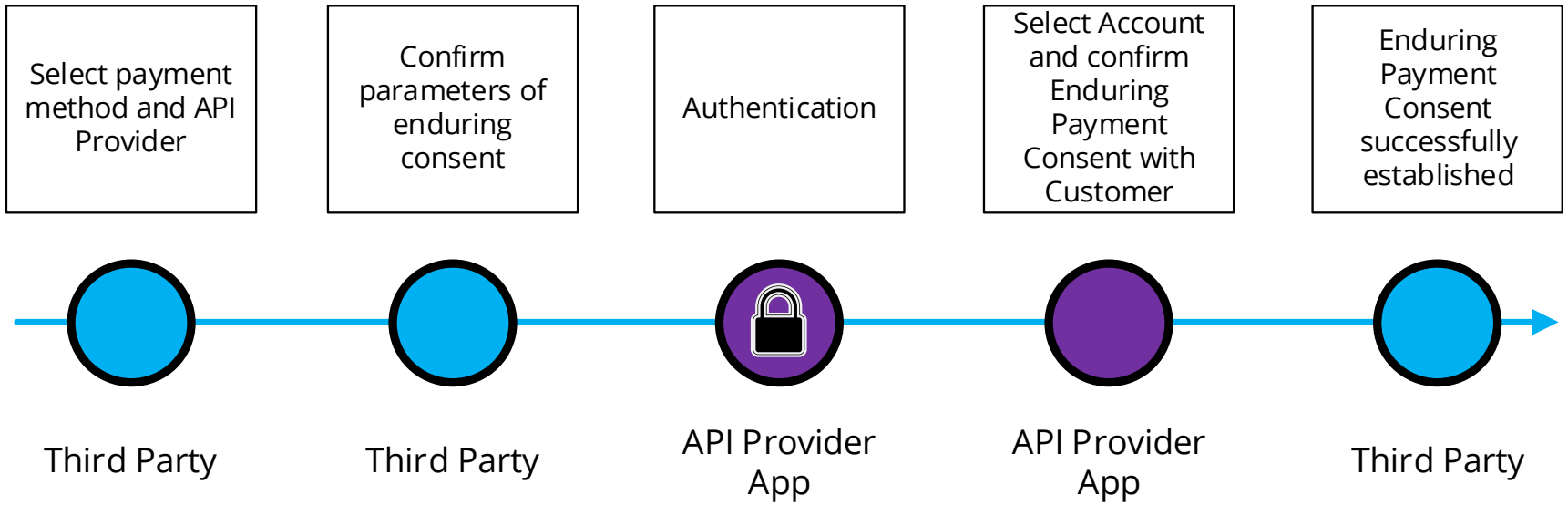
5.2.2.1 Journey description

There are cases where the payment order submitted by Third Parties to API Providers is incomplete, such as where the Customer's account selection has not yet occurred.

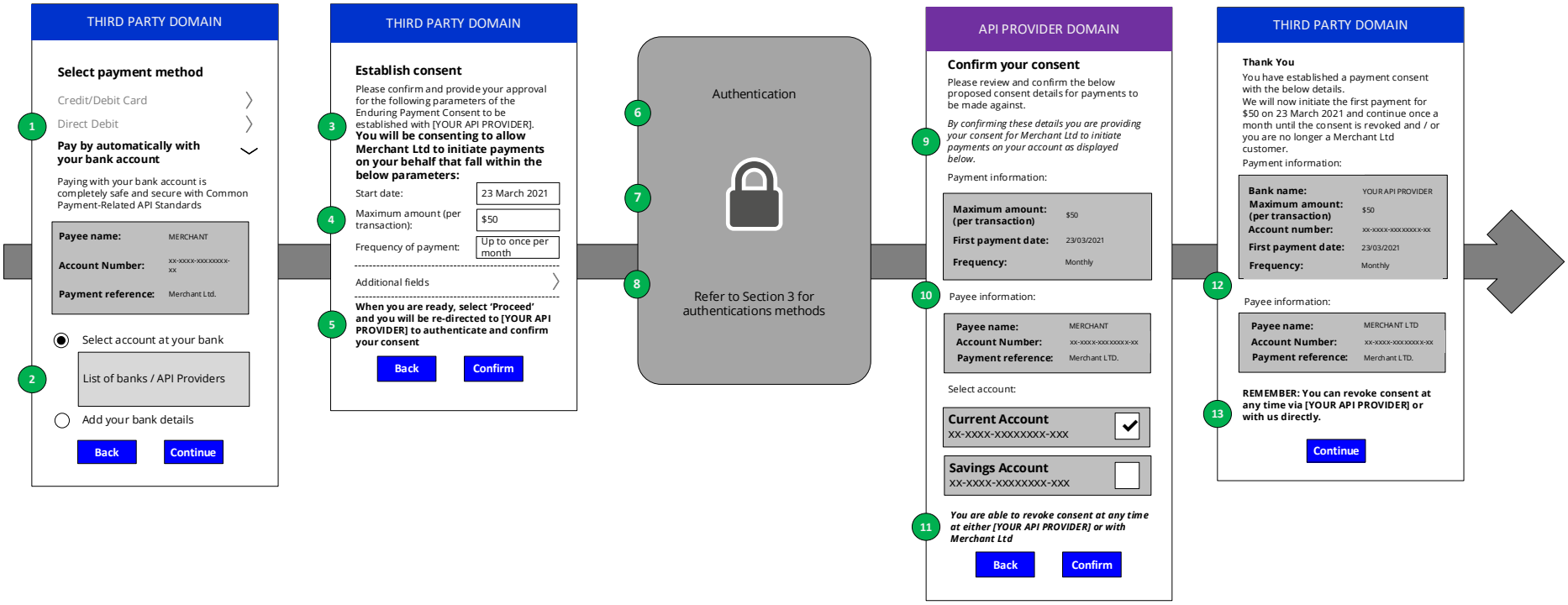
Once a Third Party establishes the bounds of the consent with Customer and passes the Enduring Payment Consent object to the API Provider for account selection and the Customer completes authentication, the Customer should be directed back to the Third Party domain without any further steps taking place in the API Provider domain.

Enduring Payment Consent can be acquired via any of the authentication methods available to single domestic one-time payments as detailed in Section 3 – 'Authentication Methods'.

5.2.2.2 Journey map

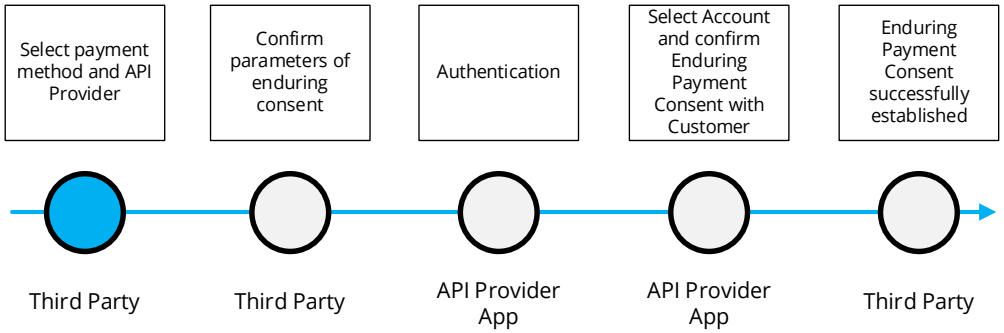


5.2.2.3 Wireframe journey



5.2.2.4 Wireframe annotations

5.2.2.4.1 Select payment method and API Provider



Minimum Set of Parameters

A Third Party **must** either allow a Customer to specify the below minimum set of parameters or pre-populate them for the Customer:

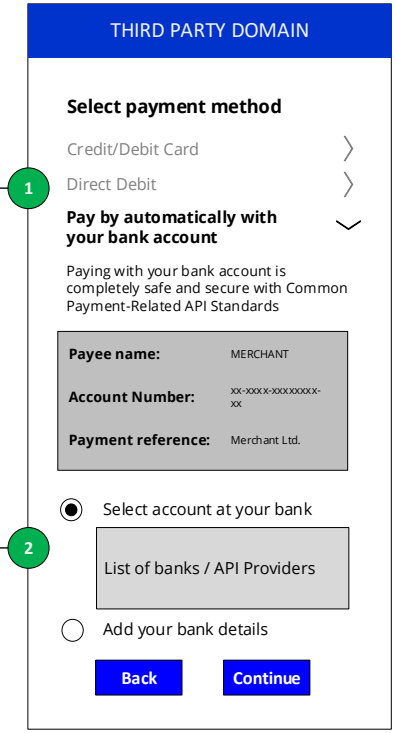
- Payment Amount and Currency.
- Payee Account Name.
- Payee Account Identification details (e.g. account number).
- Payment Reference - This is optional but it is good practice to be populated for a payment.
- Any supplementary information required which the API Provider has published as required and is specific to that API Provider.

Customer payment Account Selection

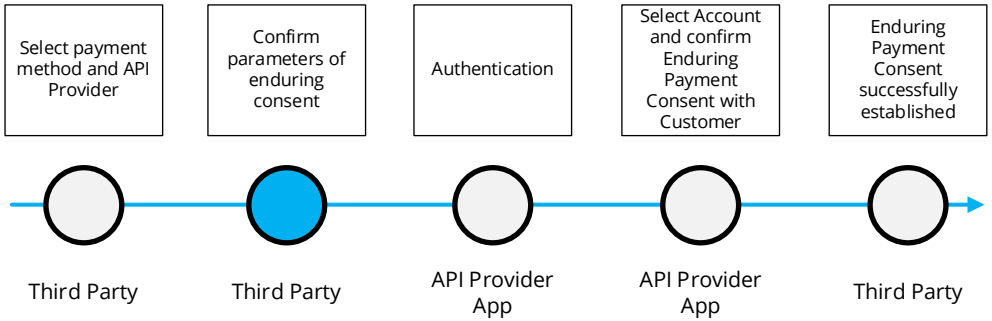
A Third Party **must** provide the Customer at least one of the following options:

- enter their Payer payment Account Identification details.
- allow the Customer to enter their payment Account Identification details in at least one of the ways specified in the API Centre API Specifications.
- select their Account Identification details (this assumes they have been saved previously).
- select their API Provider in order to select their Customer payment Account later on in the journey.

Note 1: In some of the above cases, the Third Party may also need the Customer to provide their API Provider name so that the Third Party can check whether an API Provider will be able to match the account identifier to the underlying Customer payment account.



5.2.2.4.2 Confirm parameters of enduring consent



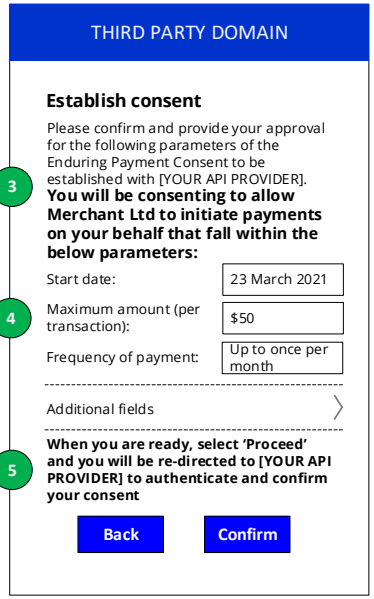
The Third Party **should** provide messaging to inform the Customer that in completing this process, they will be consenting to allow a Third Party to act on their account to initiate payments that fall within the agreed consent parameters.
Example wording: "You will be consenting to allow Merchant Ltd to initiate payments on your behalf that fall within the below parameters:"

The Third Party should request the Customer consent to the enduring payment in a clear and specific manner. The Third Party should clearly display and communicate the parameters of the proposed consent in plain English and in language that the Customer is familiar with.
The Third Party **must** display the following mandatory elements of the Enduring Consent Object the Customer as part of the establish consent step (a mandatory field cannot be left undefined):

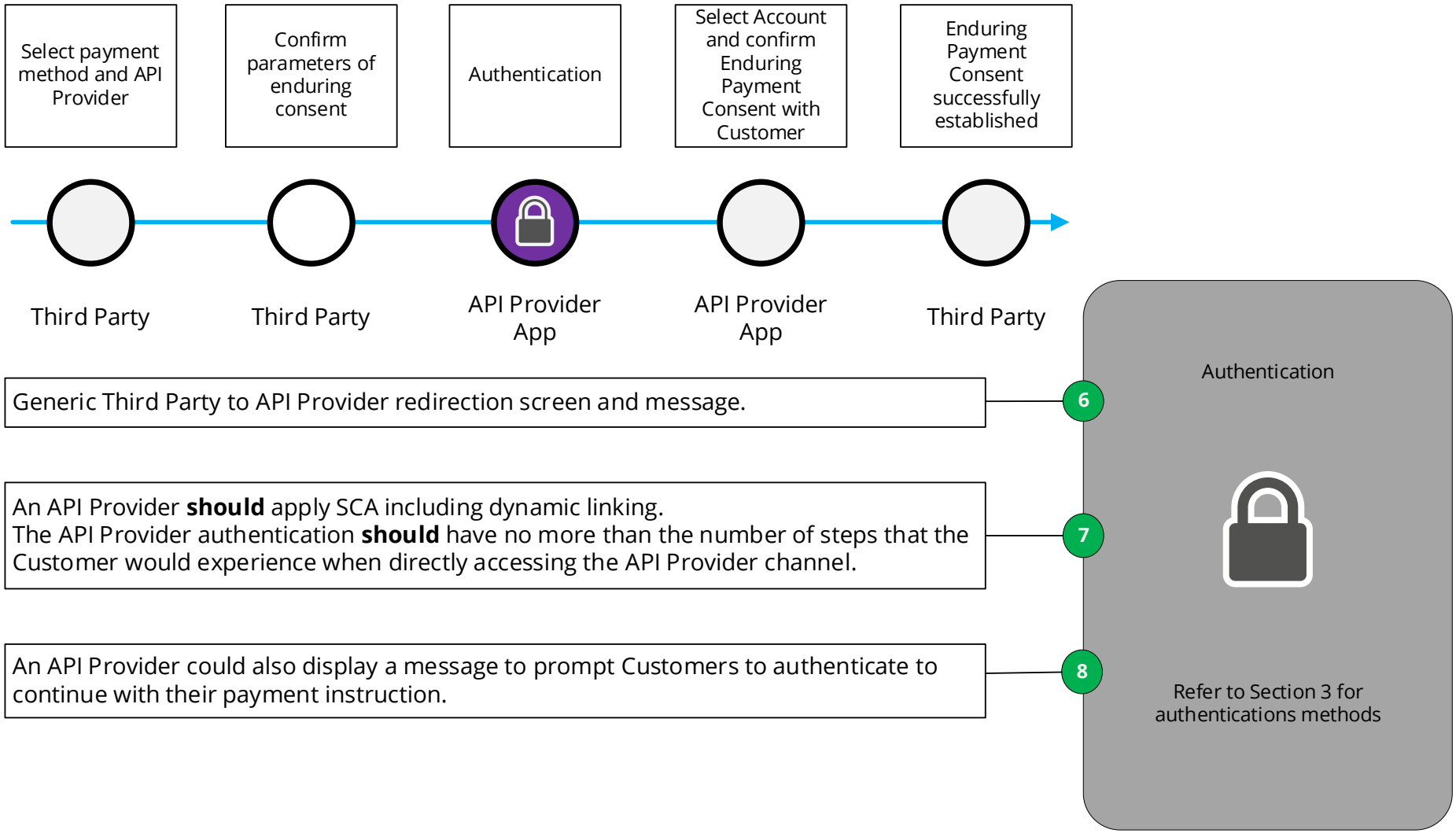
- FromDateTime - which defines when the enduring consent will be valid from ('Start date' in example)
- MaximumAmount – which specifies the maximum individual payment amount that is authorised using the Enduring Payment Consent ('Maximum Amount' in example).
- Frequency & Frequency/Period – these fields define the amount of payments that can be initiated within a given period as defined from the defined start date.

All optional elements of the enduring consent object can be implemented by a Third Party to meet their Customer use cases and should be displayed to the Customer in this screen and clearly articulated before proceeding to authentication.

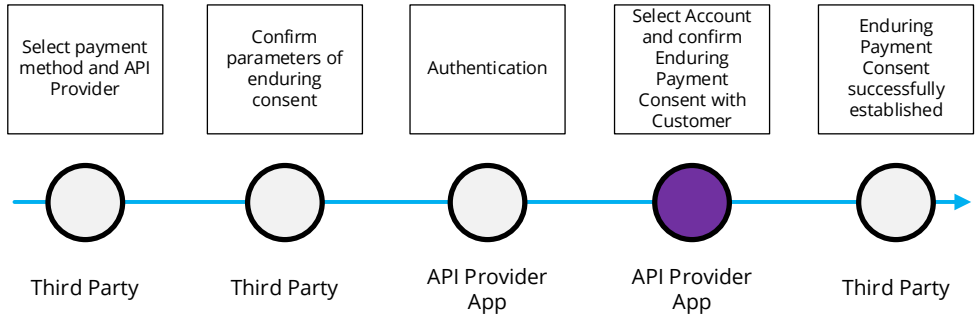
The Third Party **should** provide messaging to inform the Customer that they will be taken to their API Provider to complete the payment.
Example wording: "You will be securely transferred to YOUR API PROVIDER to authenticate and confirm your consent".



5.2.2.4.3 Authentication



5.2.2.4.4 Select account and confirm Enduring Payment Consent with Customer



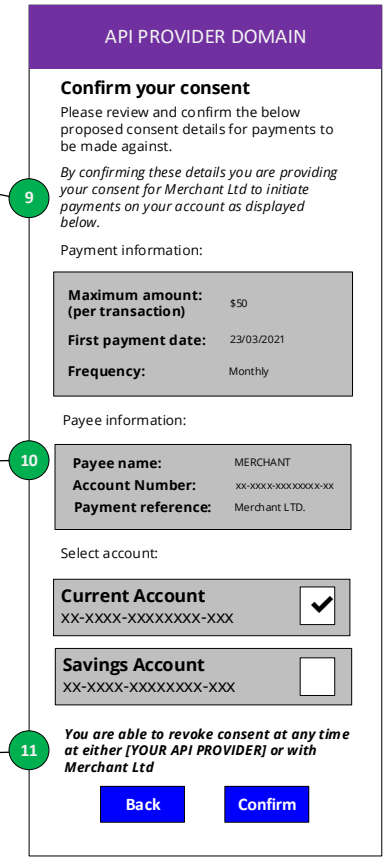
The API Provider **should** inform the Customer that following this step, the Third Party will be able to initiate payments on the specified account within the agreed parameters.

The API Provider **must** display as minimum the Mandatory elements of the enduring consent object to ensure the Customer is explicitly aware of these details (unless an SCA exemption is being applied). These details **must** be displayed as part of the authentication journey on at least one of the following screens without introducing additional confirmation screens.

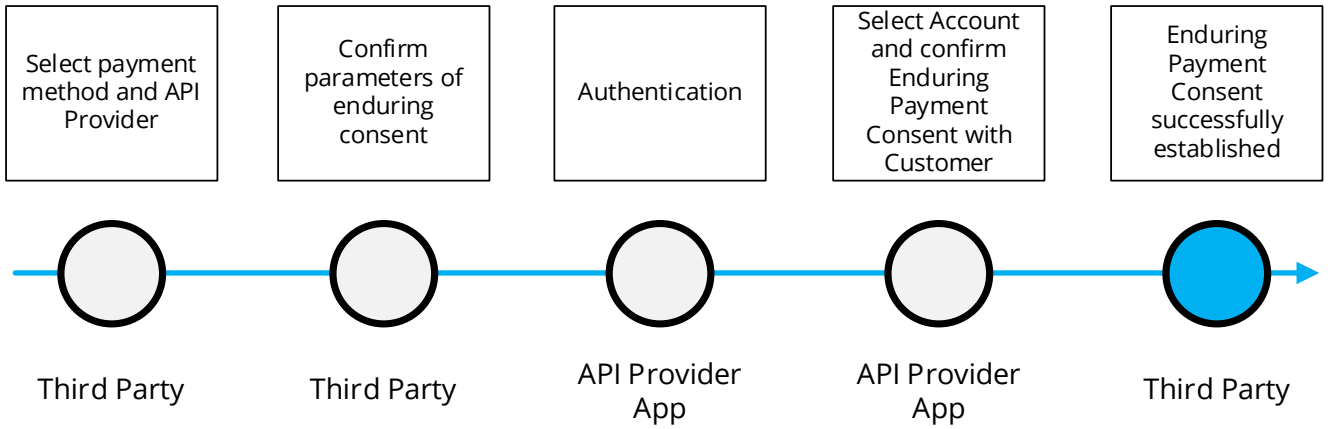
- API Provider confirms Enduring Payment Consent object with Customer (recommended)
- API Provider to Third Party redirection Screen

The API Provider **must** display all other optional parameters passed from the Third Party as part of the Enduring Payment Consent object along with the payee details and payment reference entered with the Third Party.
If an enduring-payment-consent parameter is not specified, the API Provider **should not** enforce a specific limit for the use of the enduring-payment-consent. E.g., if no TotalAmount is specified, there is no specific restriction on the total of all successful InstructedAmount(s) that may be initiated during the lifetime of the enduring-payment-consent.
Note: *The MaximumAmount field is a mandatory parameter of the enduring-payment-consent and as such **must** be populated when submitted for authentication by a Third Party*
The API Provider **must** allow the Customer to select the payment account to be linked to the Enduring Payment Consent to complete the Consent Object.

The API Provider **should** ensure the Customer is aware that they are able to control authorised enduring payment content(s) at any time directly with their API Provider or with the Third Party.



5.2.2.4.5 Enduring Payment Consent successfully established

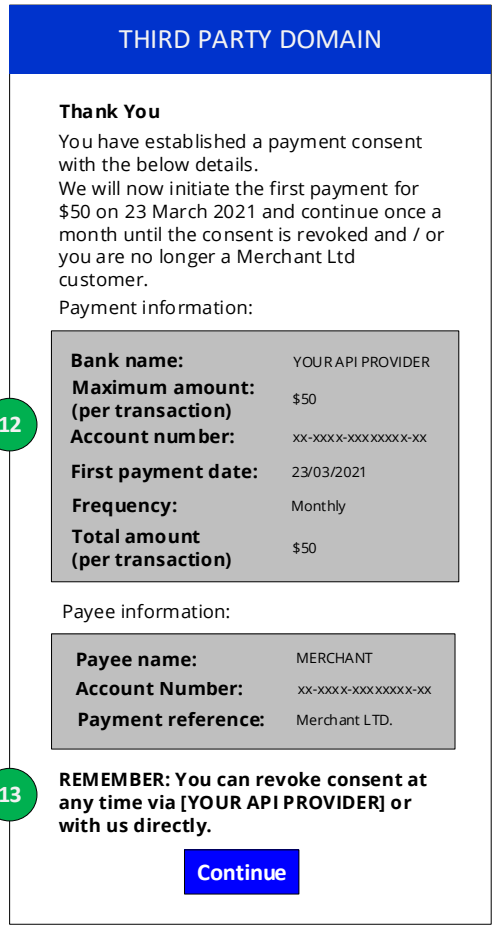


The Third Party **should** re-confirm with the Customer, in plain English the parameters of the consent that has been established and the expected activity to be carried out on the Customer account.
This **should** include the detail of the enduring consent object, including both payer and payee account details as well as the agreed and consented variable parameters.

12

The Third Party **should** ensure the Customer is aware that they are able to control authorised enduring payment consent(s) at any time, directly with their API Provider or with the Third Party.

13



5.2.3 Initiating a single one-off payment using an Enduring Payment Consent

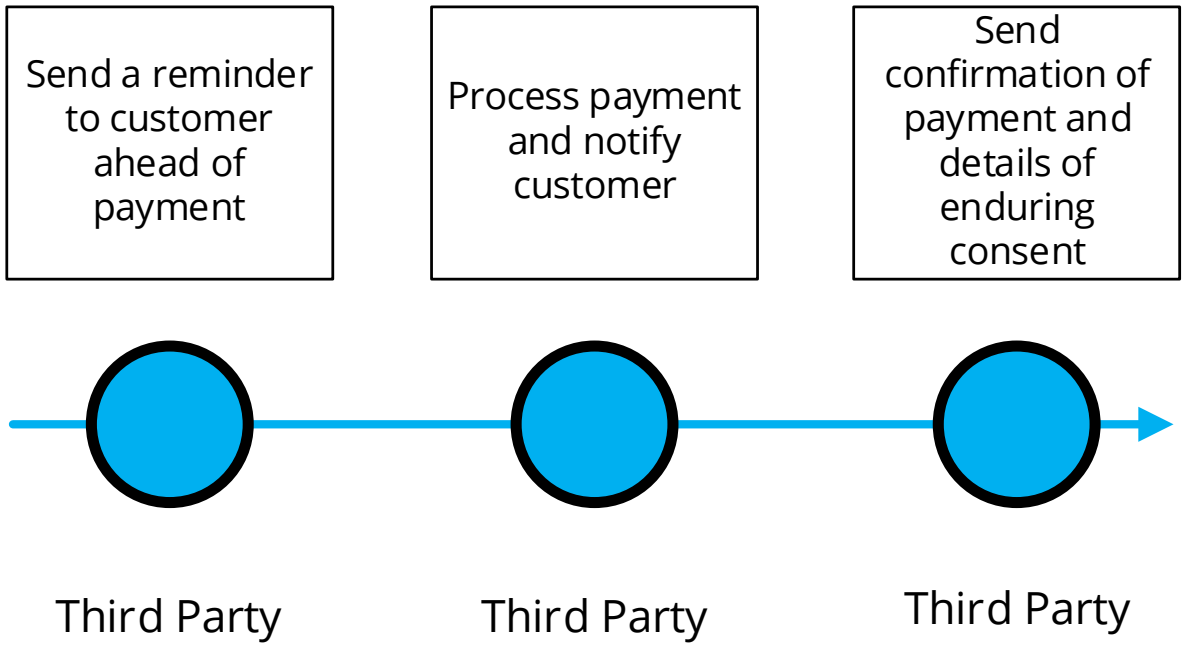
5.2.3.1 Journey description

The Third Party will be able to initiate a one-off payment on behalf of the Customer using the previously authorised enduring payment consent.

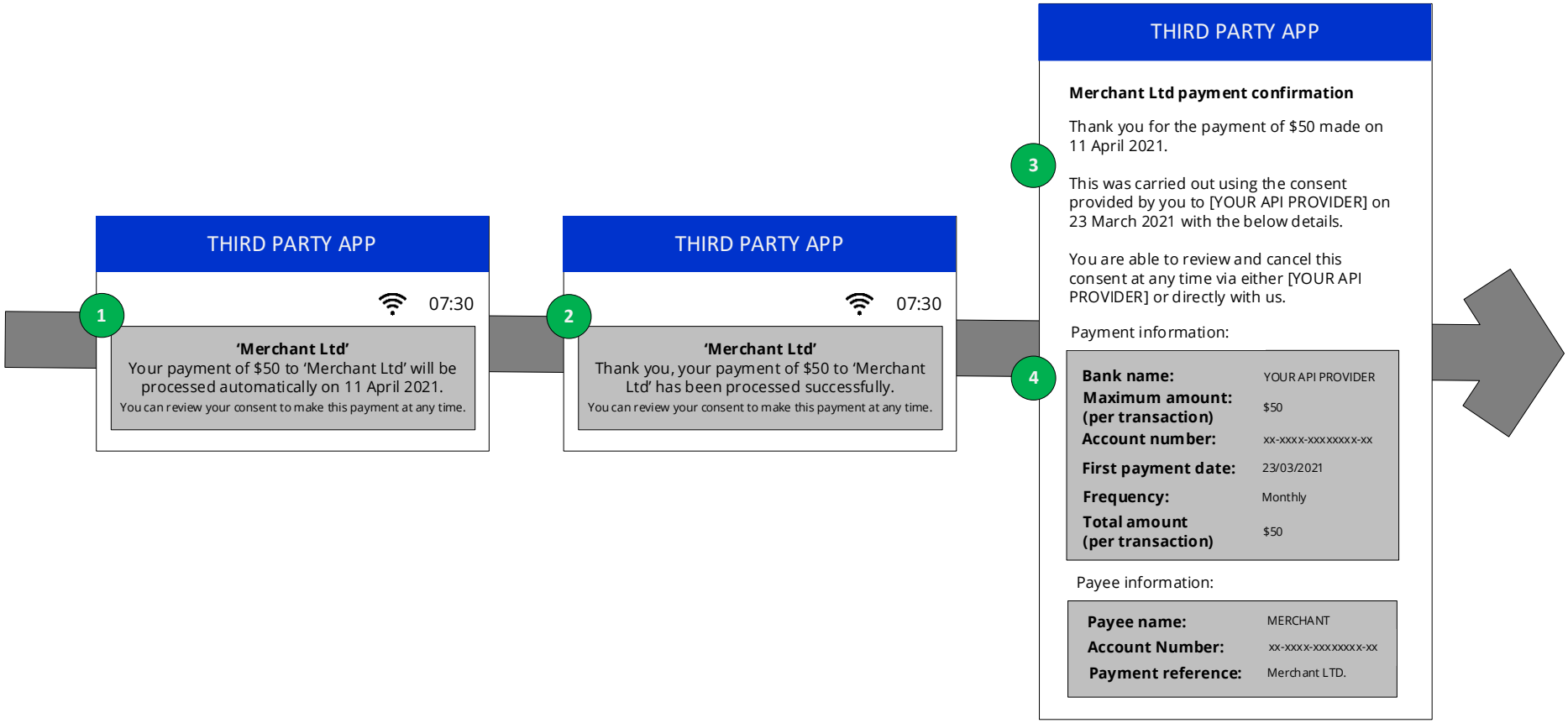
If a single one-off payment is initiated using an enduring payment consent and the payment fails for any reason (e.g., fraud checks, or is deemed outside the agreed enduring consent parameters), the Third Party should inform the Customer and initiate a single one off payment initiation services journey as detailed in Section 5.1 – 'Mandatory payment initiation services journeys'.

This will not invalidate the enduring payment consent object for future payment initiations.

5.2.3.2 Journey map

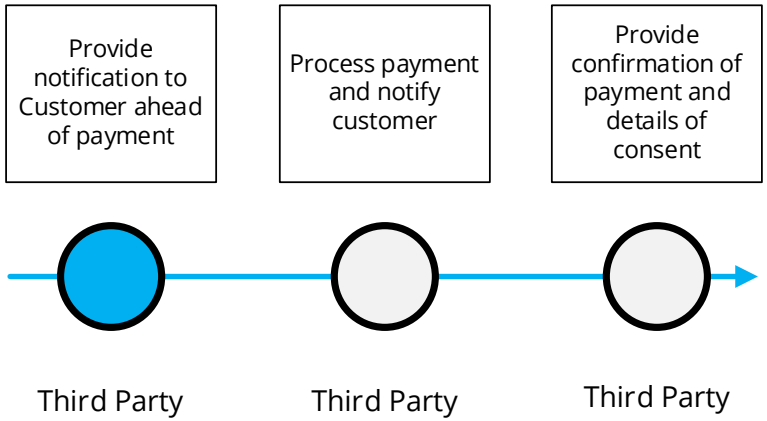


5.2.3.3 Wireframe journey



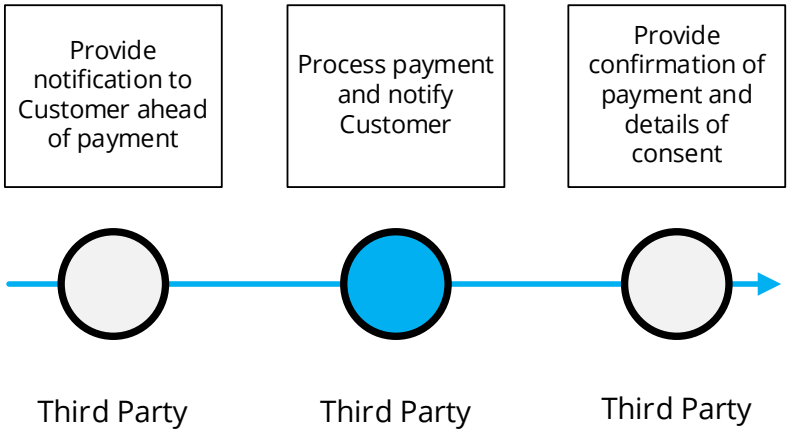
5.2.3.4 Wireframe annotations

5.2.3.4.1 Provide notification to Customer ahead of payment

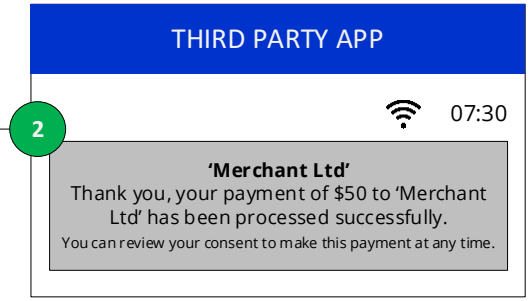


The Third Party **should** notify the Customer at least 48 hours in advance of a payment being made using an authorised enduring payment consent.
This notification **should** include a summary, using clear language of the payment that will be made and when.
It **should** also include a reminder to the Customer that they are always in control of any consent previously granted and are able to revoke consent at any time.

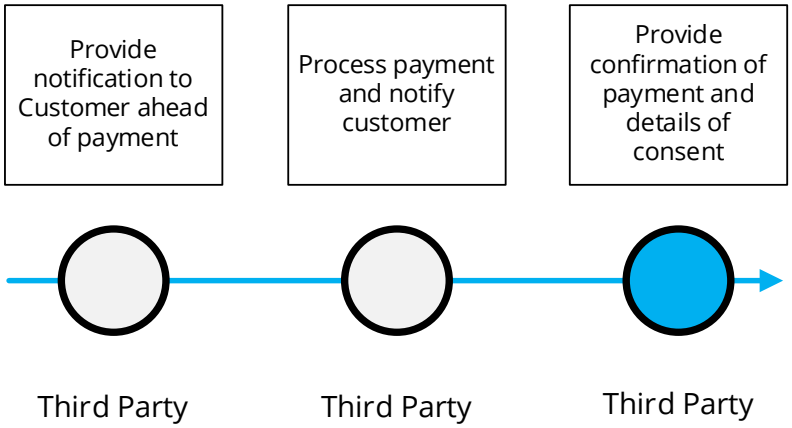
5.2.3.4.2 Process payment and notify Customer



The Third Party **should** notify the Customer when the payment has been made
This notification **should** include a summary, using clear language of the payment that has been made.
It **should** also include a reminder to the Customer that they are always in control of any consent previously granted and are able to revoke consent at any time.

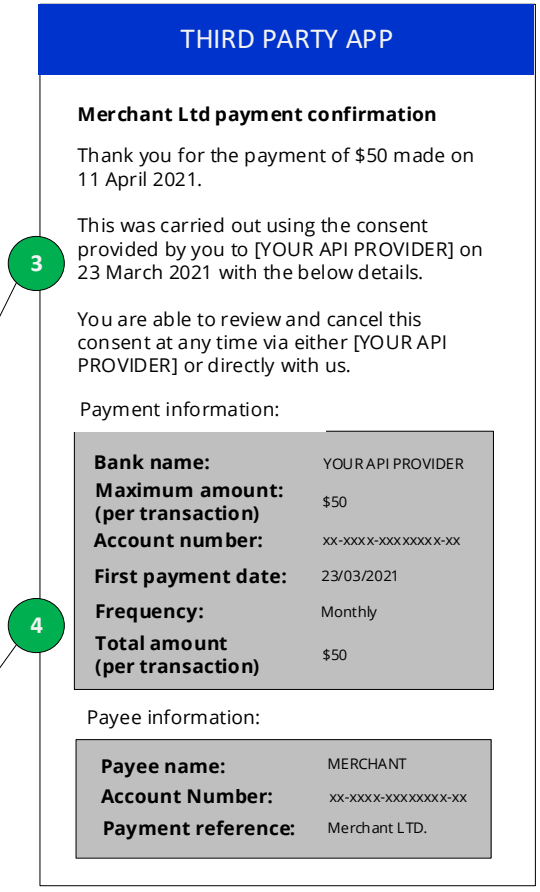


5.2.3.4.3 Provide confirmation of payment and details of consent



The Third Party **should** send confirmation to the Customer following the successful completion of the payment, which provides the full detail of the payment made in clear language and **should** provide a reminder that the Customer can revoke consent at any time.

The Third Party **should** provide full details of the authorised enduring payment consent in order to make the Customer aware when the next payment will be made.



5.2.4 Consent dashboard and revocation – Third Party

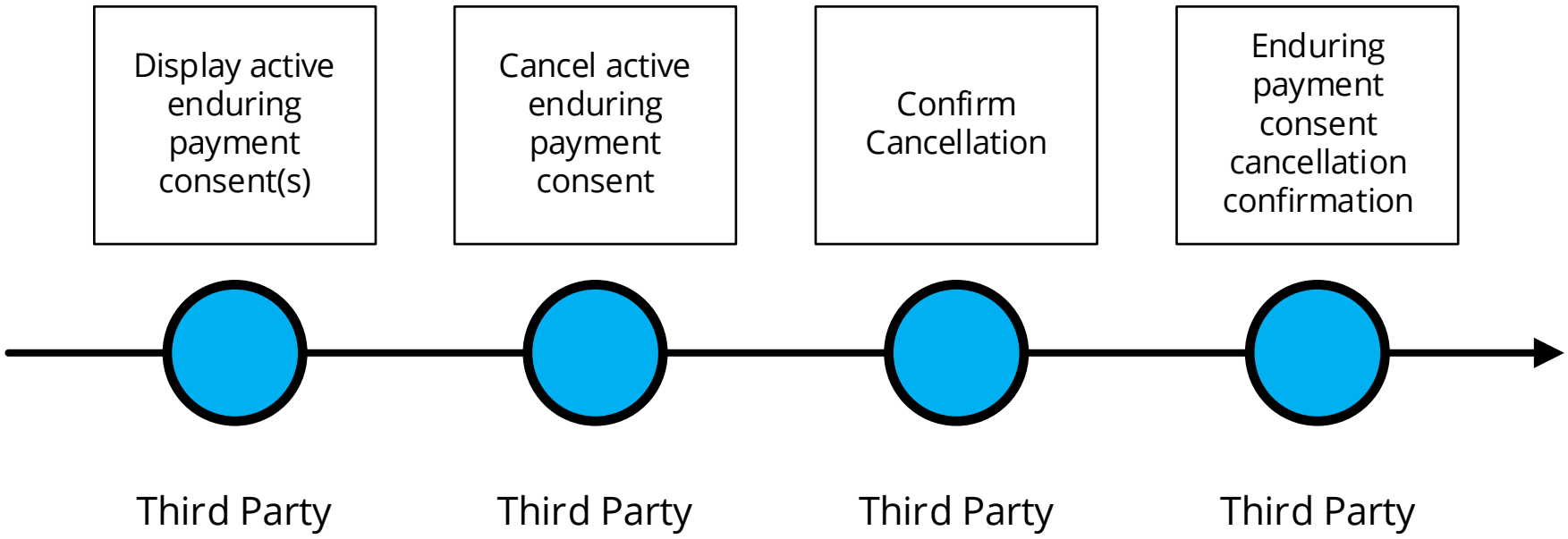
5.2.4.1 Journey description

The Third Party **must** provide Customers with a facility to view and cancel all enduring payment consents that they have given to that Third Party.

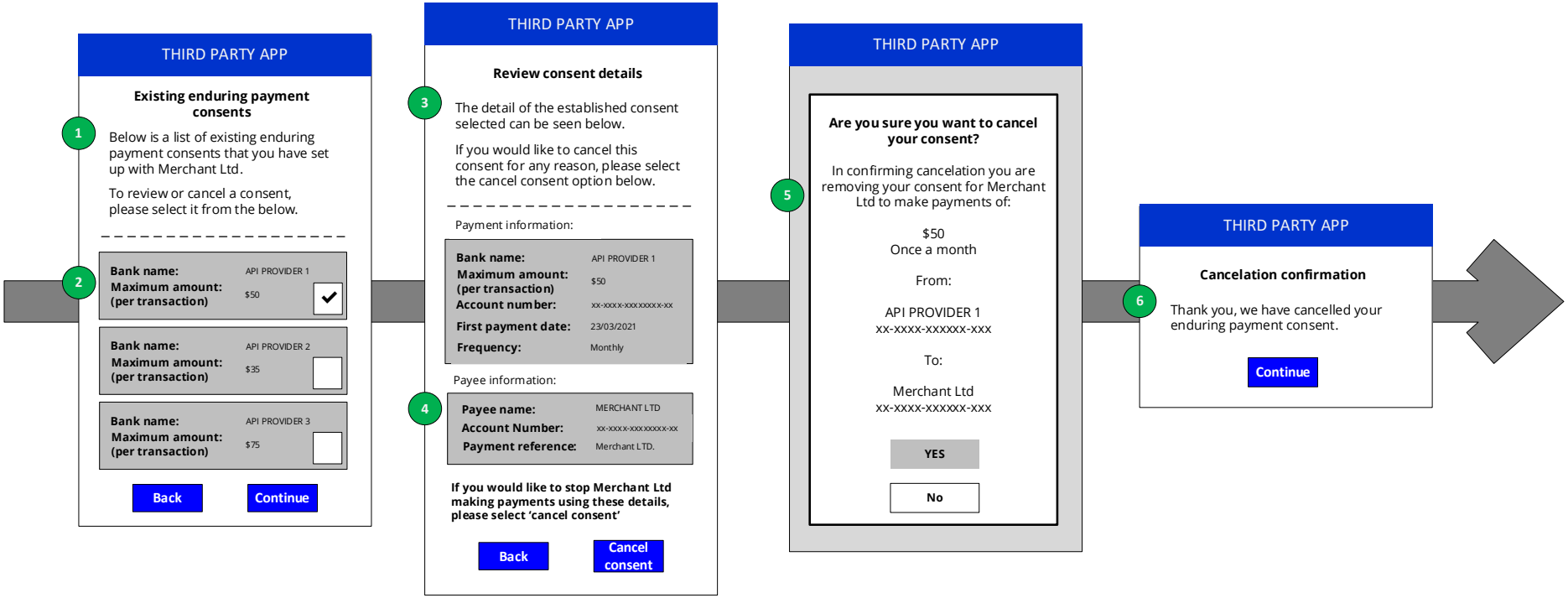
This section describes how these consents should be displayed and how the Customer journey to cancel them should be constructed.

NOTE: It is **not** possible for a customer to edit / adjust a consent after it has been submitted for authentication and should changes need to be made, the consent **must** be cancelled and re-established.

5.2.4.2 Journey map

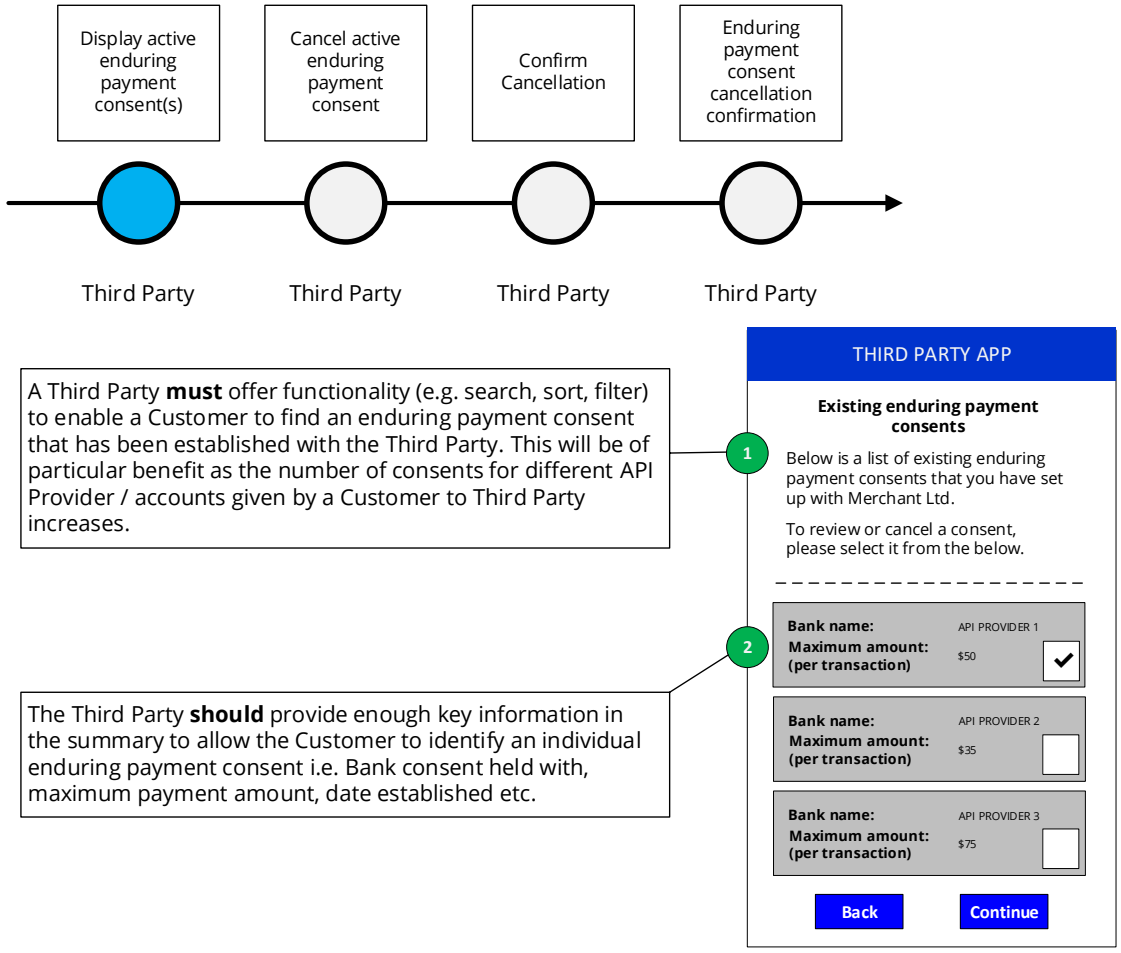


5.2.4.3 Wireframe journey

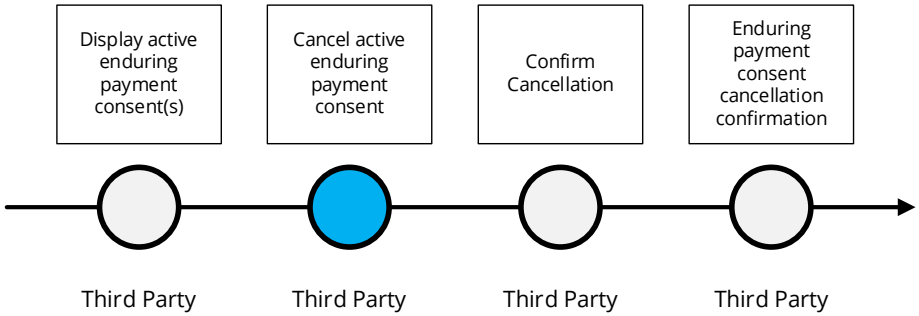


5.2.4.4 Wireframe annotations

5.2.4.4.1 Display active enduring payment consent(s)

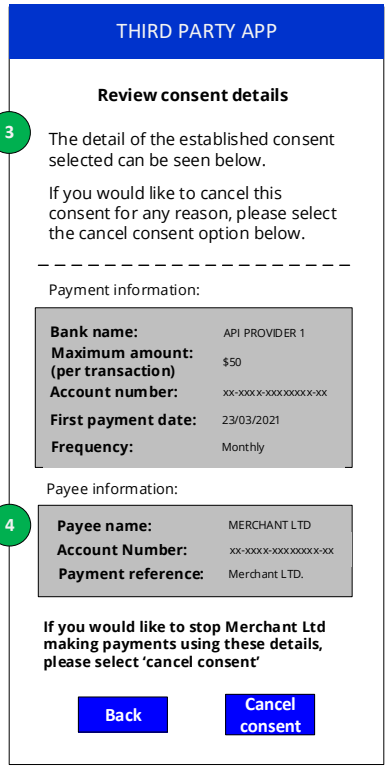


5.2.4.4.2 Cancel active enduring payment consent

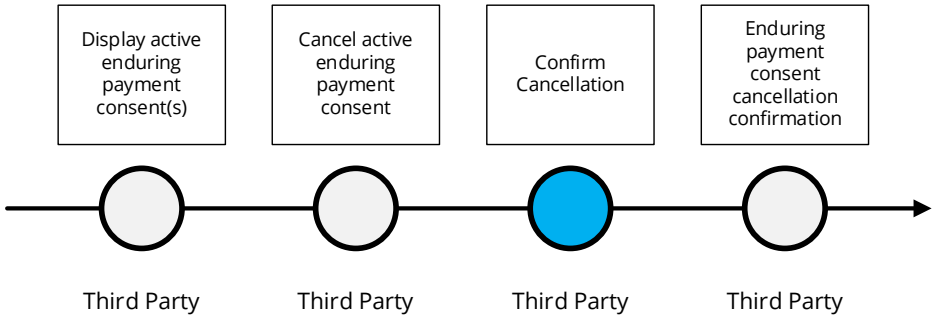


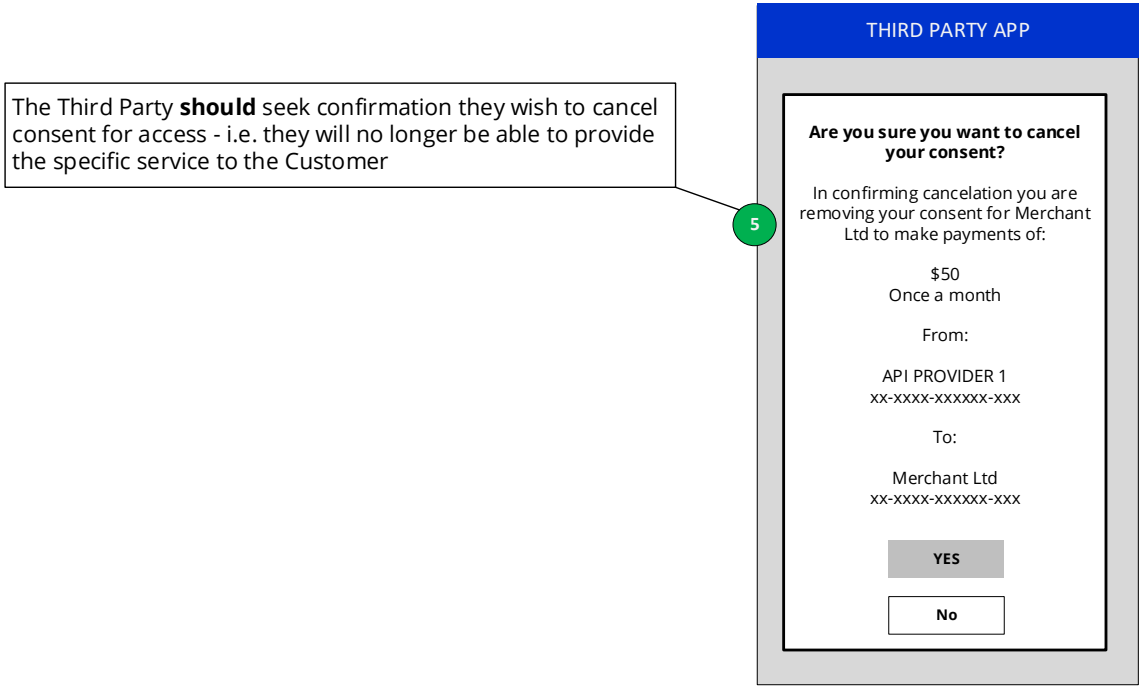
The Third Party **should** inform the customer that they are able to cancel this consent at any time through this page.
Example wording: If you would like to cancel this consent for any reason, please select the cancel consent option below.

The Third Party **should** provide a complete summary of detail of the established Enduring Payment Consent in order for the Customer to make an informed decision whether to revoke the consent.
The Third Party **should** make the exact consequences of cancelling the consent clear to the Customer - i.e. they will no longer be able to provide the specific service to the Customer

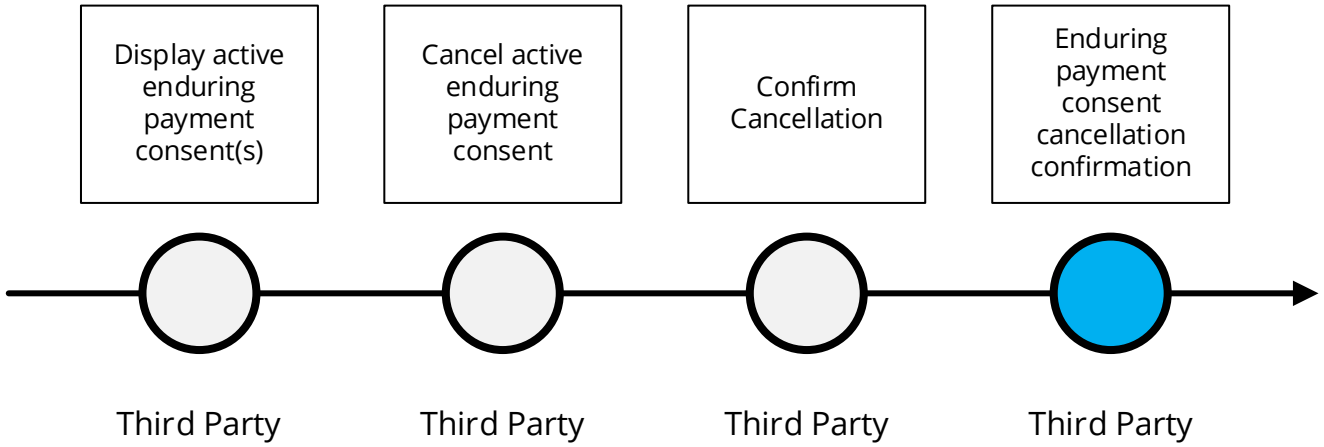


5.2.4.4.3 Confirm cancellation



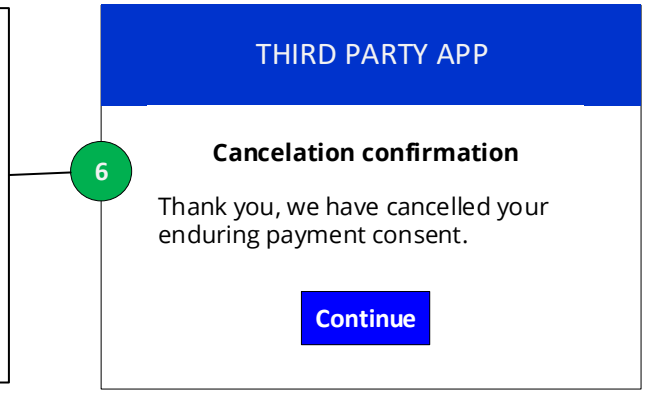


5.2.4.4.4 Enduring payment consent cancellation confirmation



The Third Party **must** inform the API Provider that the Customer has withdrawn consent by making a call to DELETE / enduring-payment-consents/{ConsentId} as soon as is practically possible.

The API Provider **must** support the Delete process . (This is not visible to the Customer but will ensure no further payments are made by the Third Party using the now revoked enduring payment consent.



5.2.5 Access dashboard and revocation – API Provider

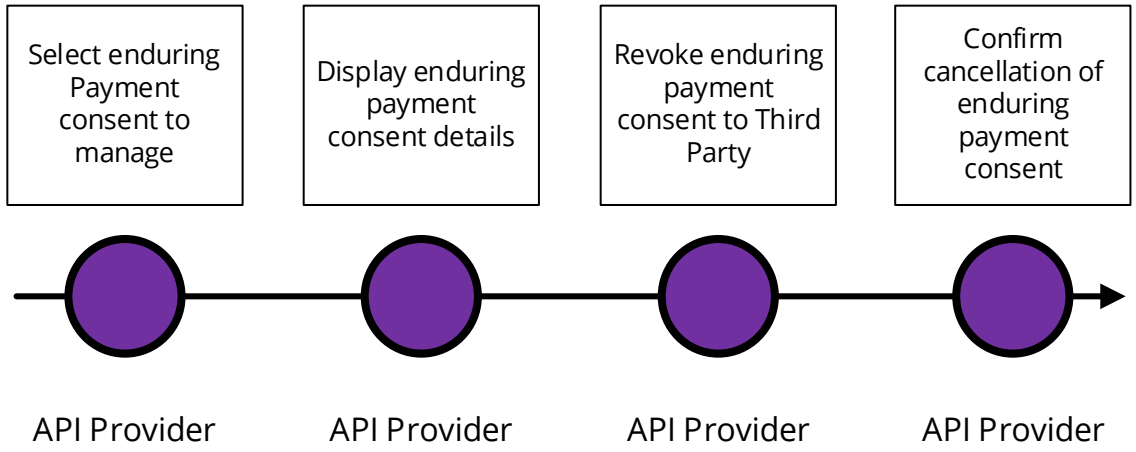
5.2.5.1 Journey description

API Providers should provide Customers with a facility to view and cancel ongoing enduring payment consents that they have given to any Third Party.

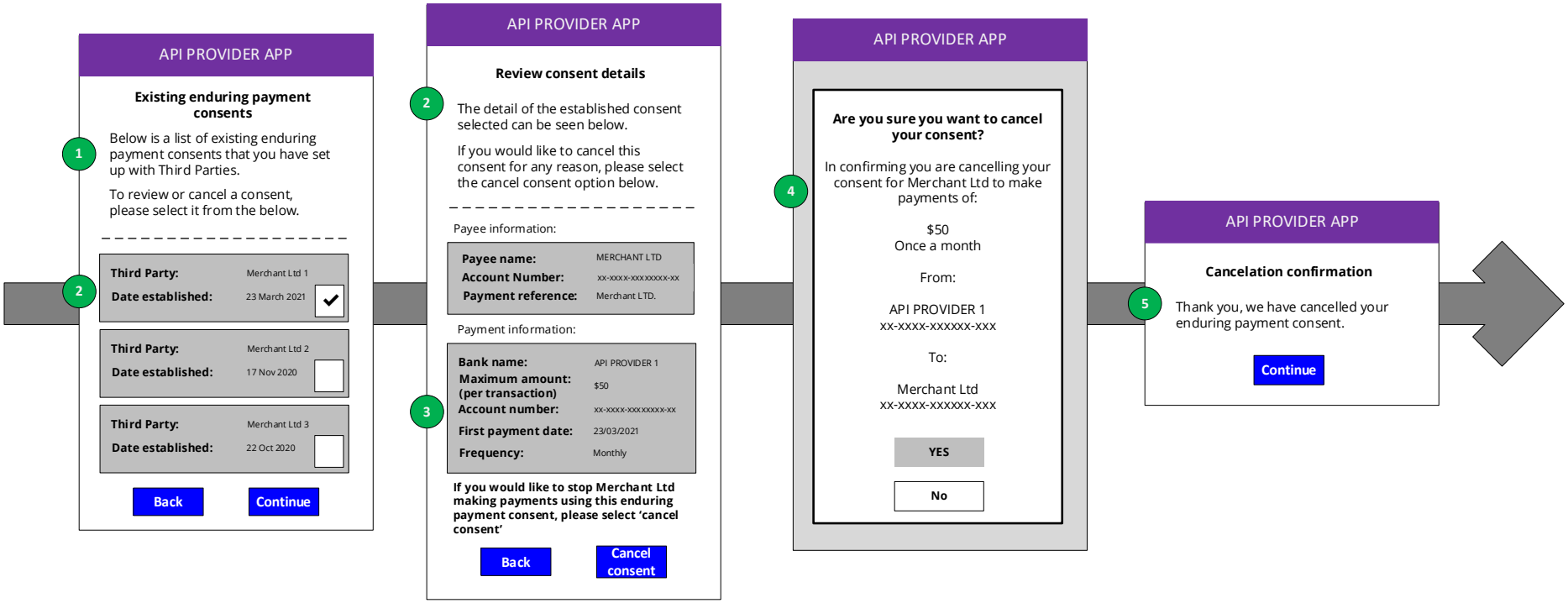
This section describes how all Customer enduring payment consents should be displayed and how the Customer journey to cancel it should be constructed.

NOTE: It is **not** possible for a Customer to edit / adjust a consent after it has been submitted for authentication and if changes need to be made, the consent **must** be cancelled and re-established.

5.2.5.2 Journey map

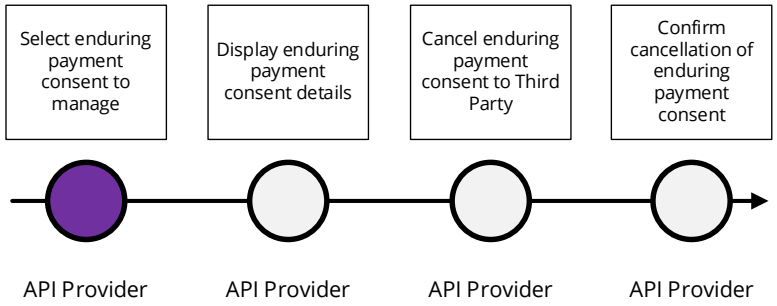


5.2.5.3 Wireframe journey



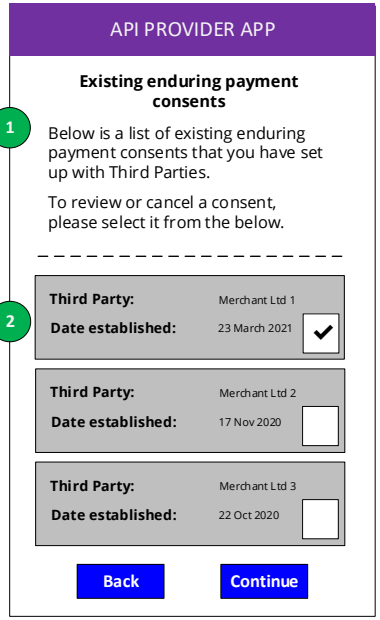
5.2.5.4 Wireframe annotations

5.2.5.4.1 Select enduring payment consent to manage

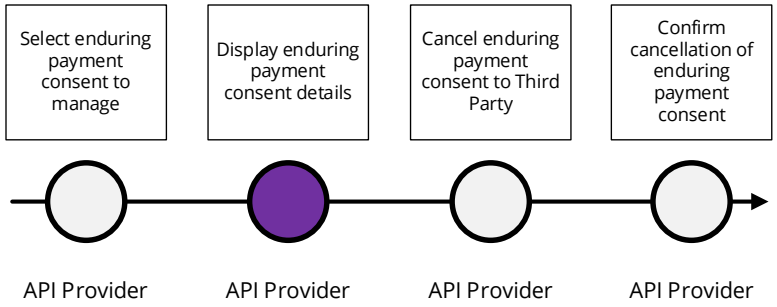


The API Provider **must** offer functionality (e.g. search, sort, filter) to enable a Customer to find an enduring payment consent that has been established with a Third Party. This will be of particular benefit as the number of consents for different API Provider / accounts given by a Customer to a Third Party increases.

The API Provider **should** provide enough key information in the summary to allow the Customer to identify an individual enduring payment consent i.e. Third Party consent granted to, maximum payment amount, date established etc.

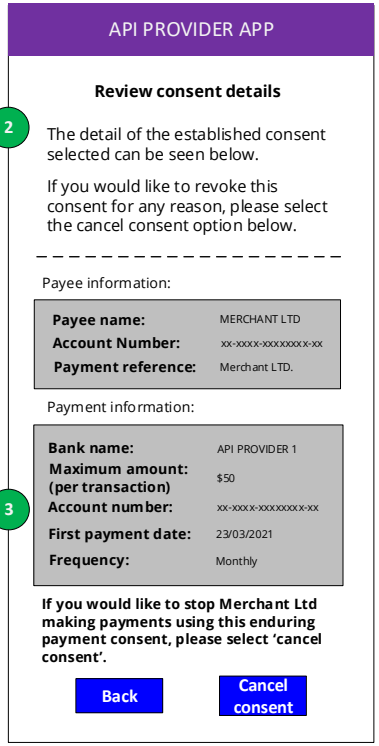


5.2.5.4.2 Display enduring payment consent details

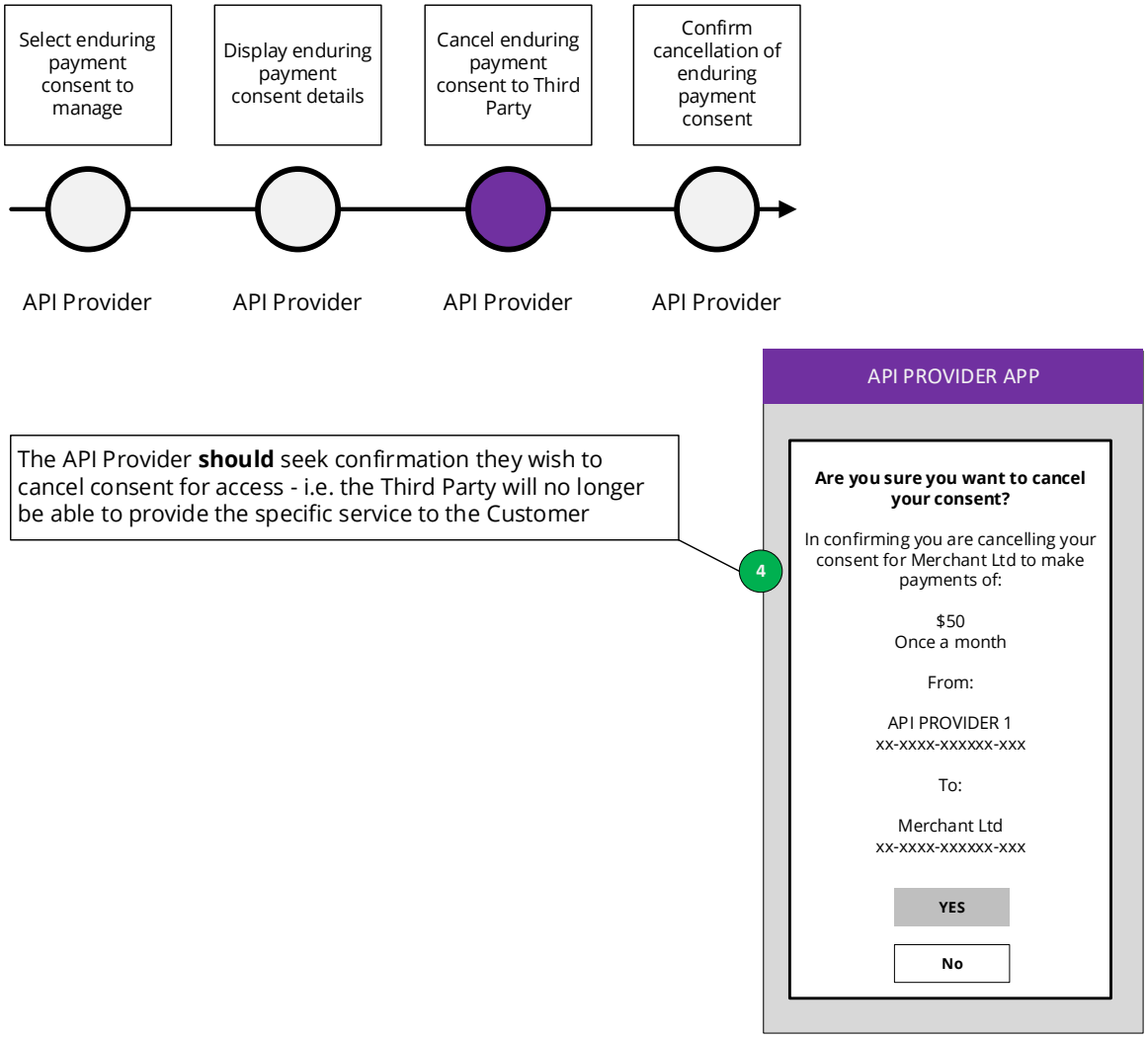


The API Provider **should** inform the customer that they are able to cancel this consent at any time through this page.
Example wording: If you would like to revoke this consent for any reason, please select the revoke option below.

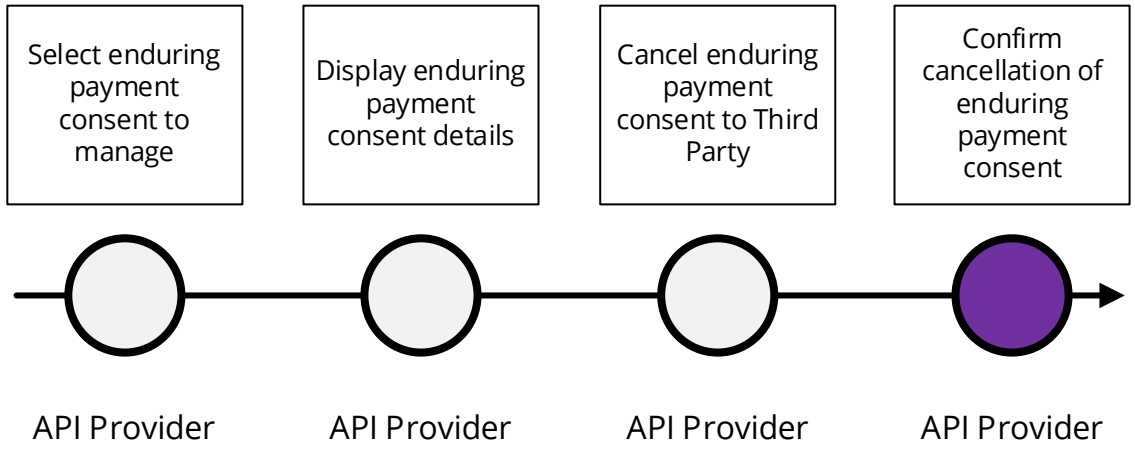
The API Provider **should** provide a complete summary of detail of the established Enduring Payment Consent in order for the Customer to make an informed decision whether to cancel the consent.
The API Provider **should** make the exact consequences of cancelling the consent clear to the Customer - i.e. they will no longer be able to provide the specific service to the Customer and/or advise the Customer to contact the Third Party to inform them of the revocation.



5.2.5.4.3 Cancel enduring payment consent to Third Party



5.2.5.4.4 Confirm cancellation of enduring payment consent



The API Provider **should** Inform the Customer that the enduring payment consent has been cancelled.
The API Provider **must** change the status of the consent to the terminal 'Revoked' state and cannot be reactivated.