Strong Customer Authentication EMV 3DS 2.1.0 User Experience Recommendations

Mastercard®'s recommendations for optimal user experience with Card Not Present transactions in an EMV 3DS 2.1.0 protocol

December 2018

For Issuers and ACSs

mastercard

mastercard

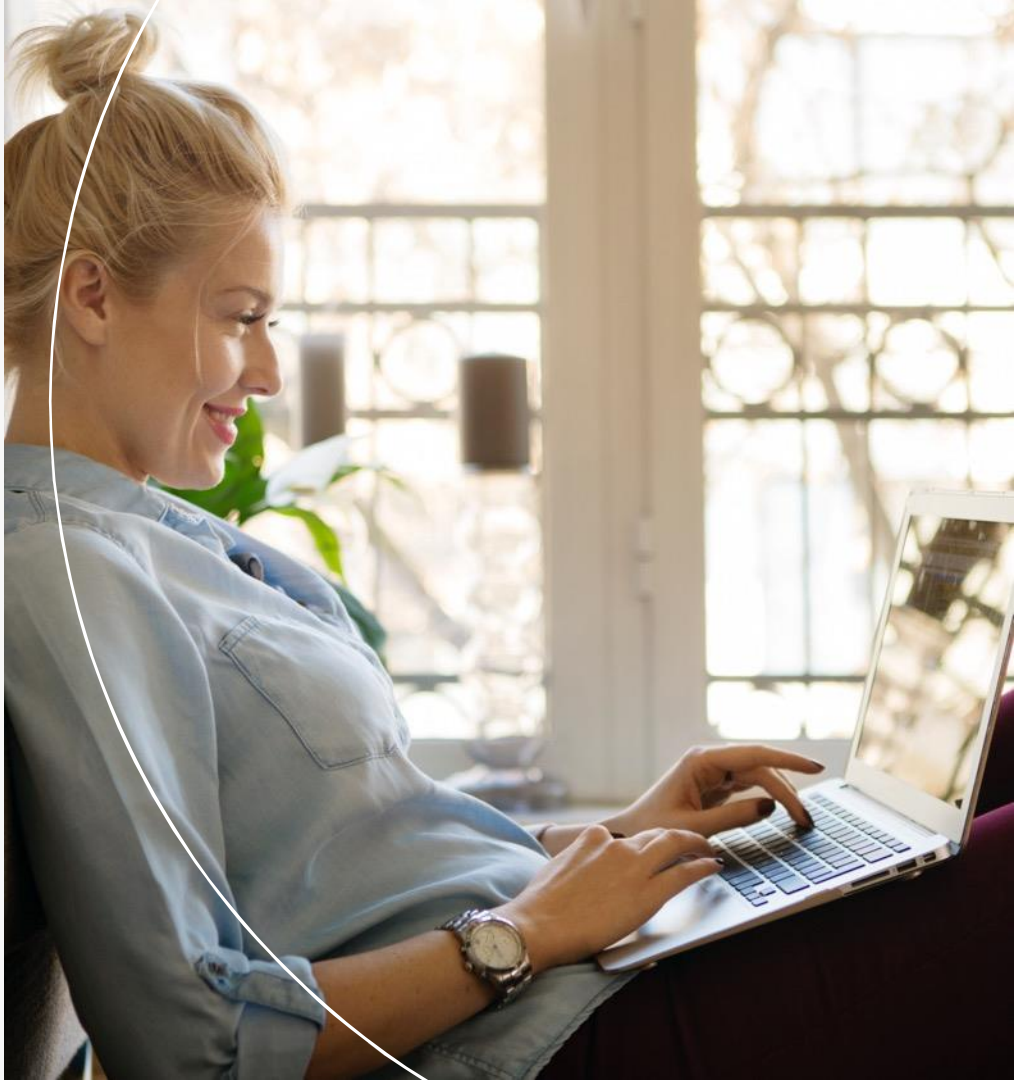


Table of contents

INTRODUCTION

This document provides strong recommendations for all EEA countries.
Where published, these recommendations are transformed into local country mandates.

EMV 3-D Secure (3DS) is a messaging protocol that facilitates frictionless cardholder authentication when making card-not-present (CNP) e-commerce purchases. It enables cardholders to actively authenticate themselves with their card issuers, if cardholder verification is required; a key requirement of the Strong Customer Authentication (SCA) regulation which comes into force in the EEA region from September 2019.

Cardholder authentication, by the exchange of 3DS data between the merchant and a card issuer may increase authorisation approval rates, as well as potentially reduce the risk of fraud for issuers, acquirers and merchants.

Version 2.1.0 of the EMV 3DS protocol includes enhancements to promote secure, consistent cardholder e-commerce transactions across all channels and connected devices, while optimising the cardholder's experience and was first released in October 2017.

INTRODUCTION (Cont'd)

The underlying basis of the protocol is to provide an enhanced data stream between issuers and merchants to achieve better informed authentication and authorisation decisions. Such a substantial expansion of the existing 3DS concept requires a large amount of planning and preparation by all participants in the payments ecosystem.

The key challenge for cardholder adoption is in providing easy, user-friendly user experiences.

This document provides requirements from Mastercard that issuers and Access Control Servers (ACS) need to take into consideration for a good cardholder user experience (UX) as they plan their move to support EMV 3DS 2.1.0 adoption to maximise cardholder engagement and increase transaction completion rates.

This document is subject to further revisions based on:

- Updates in EMVCo 3DS specifications
- Comments from EU Regulators
- Best practices gathered by Mastercard
- Consumer research results periodically performed by Mastercard

CONTENT

To clearly show the recommended UX flow when SCA will be applied for the four major use cases that cardholders will face, plus high level enrolment recommendations, this document has been constructed in the following way:

ENROLMENT

Cardholder's enrolment to EMV 3DS protocol should happen "by default". EMV 3DS should be treated as a card functionality, not as an opt-in feature cardholders choose to activate. This section will provide high level enrolment recommendations

FRICTIONLESS CHECKOUT

In this instance, the cardholder is not challenged with an authentication request e.g. as a result of the issuer assessment on the low risk of the transaction

OUT OF BAND *Single device*

The Out of Band (OOB) checkout flow allows for issuer authentication to occur outside of the merchant shopping environment. This section describes where the same device is used for both the purchasing transaction and authentication

OUT OF BAND *Multiple devices*

As an extension of OOB single device, here two different devices are used: one for shopping (a desktop browser in this case) and one for authenticating the transaction via a separate authentication application (app). This flow sets out Mastercard®'s requirements to cover this scenario

OTP via SMS

If the cardholder does not have (i) an authentication app installed, (ii) does not have a device capable of supporting such an app or (iii) the issuer is not offering biometric authentication, here we show how the transaction can be authenticated using a OTP sent via SMS to the cardholder's registered mobile number

DOCUMENT STRUCTURE

Each page has been constructed with (a) a screenshot on the right hand side, and (b) a text column on the left. The text column provides important information to explain and aid understanding of the flows:

Explanation

At the beginning of each chapter a short introduction to the use case is provided. This section provides information around the applicability of the specific authentication flow based on either PSD2 or Mastercard Identity Check™ requirements.

Context

This section will briefly describe the specific use case and the assumptions behind the authentication flow (e.g. the transaction is initiated via a merchant app/website).

Authentication flow

This section will explain in detail each step of the authentication flow as a walkthrough of the screenshots displayed either by the merchant, issuer or ACS based on either the EMV 3DS 2.1.0 protocol or UX best practices, as recommended by Mastercard

Recommendations

This section is used to provide recommendations based on best practices, cardholder research and acquired expertise in the field of online authentication.

For additional support, some pages include specific callouts to design enhancements planned to be released by EMVCo with future versions of the EMV 3DS protocol.

ENROLMENT

mastercard

mastercard

ENROLMENT

Enrolment by default to Mastercard Identity Check™

Mastercard® mandates within the Identity Check Programme that Issuers deploy an 'enrolment by default' policy for cardholders into the authentication methods that they utilise for all existing and new issued cards.

Issuers will need to ensure that their Mastercard branded portfolios are enabled to support the Mastercard Identity Check™ Programme (using Bank Identification Numbers/BINs and card ranges).
Mastercard recommends that issuer's cards include SCA and biometry enablement. SCA enablement will require the activation of two-factor authentication.

Auto-enrolment may require the amendment of card related terms and conditions. Issuers will need to ensure that they are able to collect any information required to undertake auto-enrolment, e.g. mobile phone numbers to evidence possession of a mobile device and functionality to receive push notifications.

For knowledge factors, additional registration requirements may be needed.

ENROLMENT

Enrolment by default to Mastercard Identity Check™ (Cont'd)

The following cardholder enrolment methods are therefore mandated:

- Auto-enrolment for new cardholders, the enrolment process for new cardholders includes enrolment in Mastercard Identity Check ™. This could, for example, entail that Mastercard Identity Check ™ is included in the terms and conditions of a card programme and that the mobile phone number is captured to assist the communication process with the cardholder at the point of authentication

- Auto-enrolment for all new online banking users, the enrolment process for new online banking users includes enrolment in Mastercard Identity Check ™. This could, for example, entail that terms and conditions for Mastercard Identity Check ™ are included in the terms and conditions of online banking and that the authentication method used to login to online banking is also used for Mastercard Identity Check ™

- Auto-enrolment for all existing online banking users, the authentication method used for accessing online banking can be reused for Mastercard Identity Check ™ without any manual enrolment by the cardholder. It is recommended that banks inform cardholders, for example via the online banking service (eg using pop-up messages), that the online banking authentication method is also available for card payments. This communication could also include the terms and conditions for Mastercard Identity Check ™

ENROLMENT

Enrolment to biometric authentication via app

Issuers are mandated to offer cardholders biometric authentication in most European countries with effect from 1 April 2019, unless other specific dates have been defined for their country.
Please refer to the following documentation for additional information:

Mastercard® Biometric Authentication—Europe Region (11 January 2018)

Issuers are faced with three technical approaches to offer biometric in-app authentication:

1. Embedding the authentication feature into the issuer's existing mobile banking app so that cardholders will have one combined app to undertake both banking and authentication operations (e.g. through integration of Mastercard ID Check Mobile® SDKs). Cardholders will have a consistent authentication experience based on the same authentication methods they are used to for their mobile banking activities
2. Embedding the authentication feature into the Issuer's existing MCBP wallet app so that consumers will have one combined app to make payments both in physical and virtual environments. Consumers will have a consistent authentication experience based on the same authenticators for both contactless NFC and remote payments
3. Use a separate app, independent of the issuers existing mobile banking app, solely for authentication purposes (either an issuer app or a third party app, such as Mastercard ID Check Mobile®). This approach should result in a simpler technical implementation but will also lead to lower adoption, as cardholders will have to be motivated and directed to download an additional app

ENROLMENT

For the proposed approaches on the previous page, issuers will have to consider the following key situations:

1. Authentication feature embedded in the mobile banking app or MCBP Wallet:

    a) Where a cardholder already has the mobile banking or MCBP wallet app downloaded to their mobile device, the cardholder should be prompted to choose this safer and more convenient authentication method. The Issuer will have to implement a best in class UX and communication to guide the cardholder through the biometric activation process to increase the instances of uptake and avoid the inconvenience of not being able to authenticate at the time of undertaking card not present e-commerce transactions

    b) Where a cardholder does not have the mobile banking or MCBP wallet app downloaded to their mobile device, the first effort will be to push the cardholder to download the app. This can be undertaken in multiple ways and across different channels, for example:
        i. Marketing communication and activities
        ii. SMS with link to app stores
        iii. Post-login popup in the internet banking portal
        iv. Physical touchpoint in branch (i.e. at the moment of the current account creation)
        v. Other channels used by the Issuer

Also in this case, the issuer will have to implement a best in class UX and communication process to guide the cardholder through the mobile banking app download and biometric activation process to increase the instances of uptake and avoid the inconvenience of not being able to authenticate e-commerce transactions

ENROLMENT

2. Authentication app separated from the mobile banking app:

a) Where the cardholder already has the mobile banking app, but does not have the authentication app. the issuer should communicate to the cardholder to instruct them to download the authentication app. Multiple avenues are available to achieve this, for example:

   i. Push Notifications to the mobile banking app
   ii. Post-login popup in the mobile banking app
   iii. Marketing communication and activities
   iv. SMS with link to app stores
   v. Post-login popup in the internet banking portal
   vi. Physical touchpoint in branch (i.e. at the moment of the current account creation)
   vii. Other channels used by the issuer

b) Where the cardholder has no app, the issuer should utilise the listed communication channels above to motivate the cardholder to download both mobile banking and authentication apps.

This section is intended to provoke thought around how to create a frictionless and intuitive enrolment process for new and existing cardholders.
Additional user experience guidelines and enrolment process best practices will be released at a later stage.

FRICTIONLESS CHECKOUT

mastercard

mastercard

FRICTIONLESS CHECKOUT (1/5)

A frictionless checkout happens when the cardholder is not challenged with an authentication request as a result of the Issuer assessment on the low risk of the transaction.

Article 98 of Directive 2015/2366 (PSD2), Regulatory Technical Standards (RTS), sets specific thresholds and requirements for when exemptions to cardholder authentication can be applied. These are specifically set out in *Chapter 3, Articles 13, 14, 15 and 16*).

Examples of uses cases where a frictionless checkout may occur:

- Acquirer PSP applies for Transaction Risk Analysis (TRA) exemption
- The cardholder has previously indicated that the merchant is a trusted beneficiary (Merchant Whitelisting)

FRICTIONLESS CHECKOUT (2/5)

Explanation

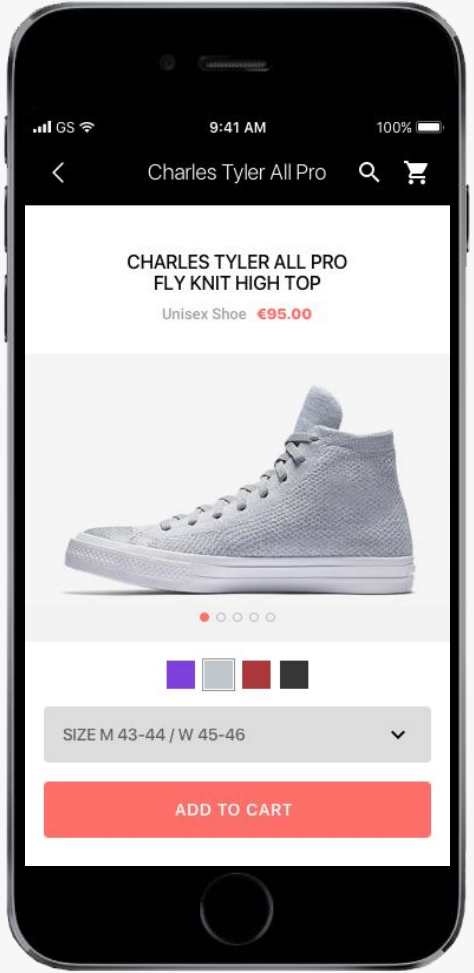
The cardholder is shopping from within a merchant app.

The authentication flow would look the same if the cardholder was within a mobile browser or a web view environment embedded in a merchant app.

The authentication experience would look the same regardless of the device manufacturer / Operating System.

Please note:

Mastercard® is not proposing best practice/ user experience for checkout / shopping cart flows throughout this document, as these remain within the merchant/PSP domain. These pages are shown as an example to portray the customer journey and aid explanation.



FRICTIONLESS CHECKOUT (3/5)

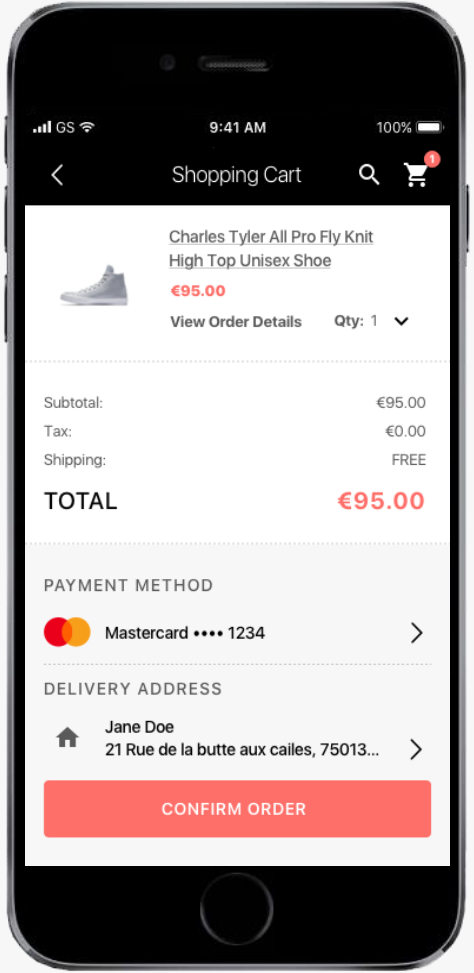
Context

The cardholder adds the selected item into the shopping cart and proceeds to the checkout page.

This example assumes the cardholder has previously purchased items with this merchant. Stored credentials from the merchant's records are prepopulated, e.g.:

- *Registered card*
- *Billing Address*
- *Delivery Address*

The EMV 3DS authentication flow will be initiated once the cardholder proceeds with the purchase and clicks on "Confirm order" button.



FRICTIONLESS CHECKOUT (4/5)

Context

Once the cardholder clicks on "Confirm Order" the EMV 3DS 2.1.0 flow is initiated.

Authentication flow

The 3DS requestor communicates with the 3DS Server to initiate the authentication flow.

The processing screen is displayed and the Scheme Brand is shown.

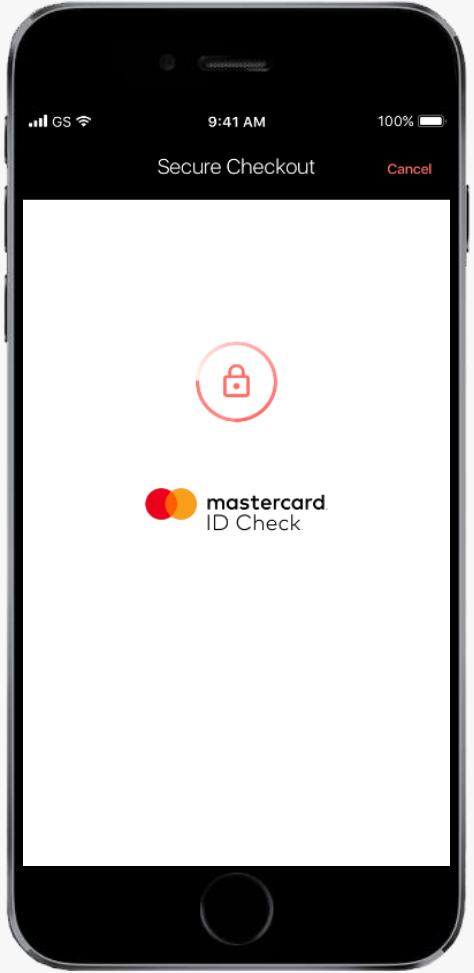
While this screen is on view to the consumer, the issuer's ACS is evaluating the risk of the transaction based on the information sent by the 3DS requestor via the EMV 3DS 2.1.0 message.

Recommendations

1.1 Scheme Brand must be clearly displayed raising the confidence in this transaction and reinforcing the security

1.2 Processing icon must be displayed

1.3 No other design element should be included in the processing screen



FRICTIONLESS CHECKOUT (5/5)

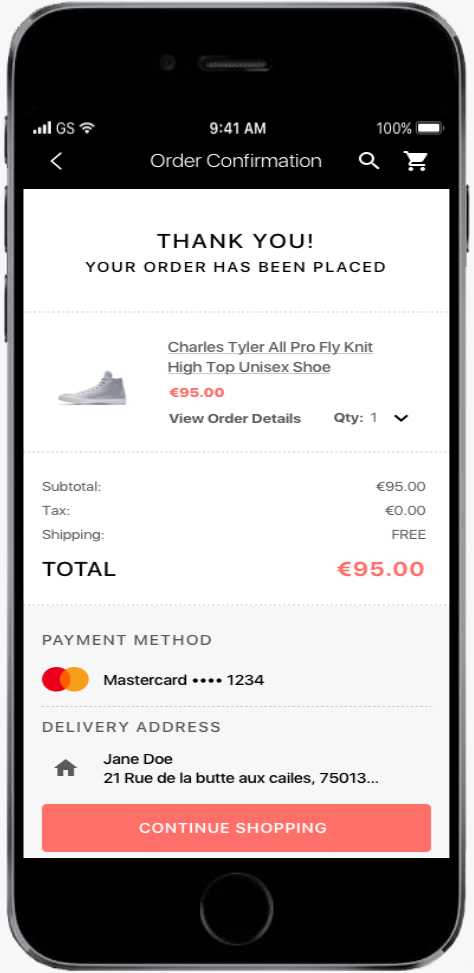
Authentication flow

After the transaction analysis by the issuer, having evaluated the risk of the transaction, the ACS is able to proceed without the need for any authentication challenge of the cardholder.

The merchant confirmation page is displayed back in the merchant domain.

Consumer research conducted by Mastercard® in 8 European markets clearly shows a preference for this flow by the consumer versus other authentication methods.

The **"Frictionless Checkout"** is a one-click experience that Mastercard strongly suggests to issuers and ACS's to support in these specific scenarios.



OUT OF BAND AUTHENTICATION
SINGLE DEVICE

mastercard

mastercard

OUT OF BAND *Single Device* (1/11)

Out of Band (OOB) allows for issuer authentication to occur outside the merchant shopping environment, for example via push notification to a banking app.

The OOB checkout flow is enabled when an app installed on a mobile device is identified to undertake the cardholder authentication. The authentication app could be (i) the issuer banking app, (ii) a specific issuer's app used only for authentication or (iii) a third party app (for example Identity Check Mobile®).

During this flow, the cardholder switches from the EMV 3DS merchant app to the issuer app and then back to the EMV 3DS merchant environment to receive the payment confirmation page.

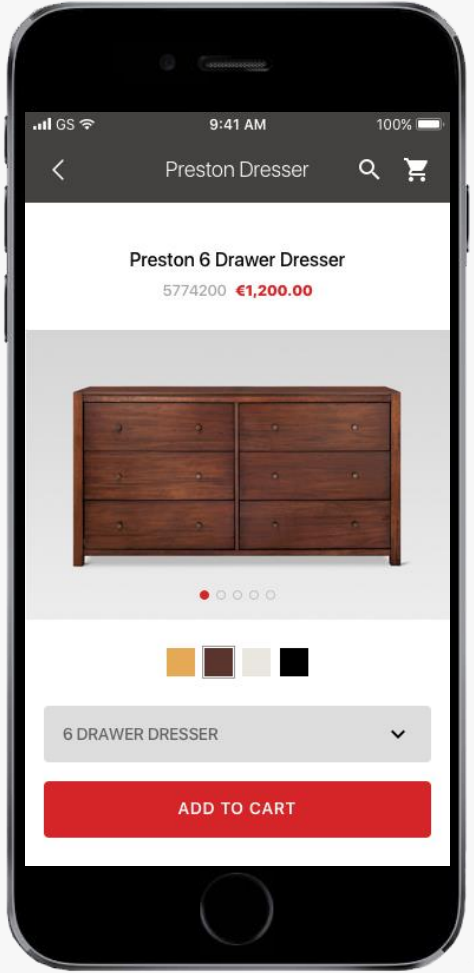
It is possible for two different devices to be used during the transaction (one for shopping, the other for authentication). The two devices checkout flow will be shown in the next section.

OUT OF BAND *Single Device* (2/11)

Context

The cardholder is shopping from within a merchant app.

The authentication flow would look the same if the cardholder was within a mobile browser or a web view environment embedded in a merchant app.



Please note:

Mastercard® is not proposing best practice/ user experience for checkout / shopping cart flows throughout this document, as these remain within the merchant/PSP domain. These pages are shown as an example to portray the customer journey and aid explanation.

OUT OF BAND *Single Device* (3/11)

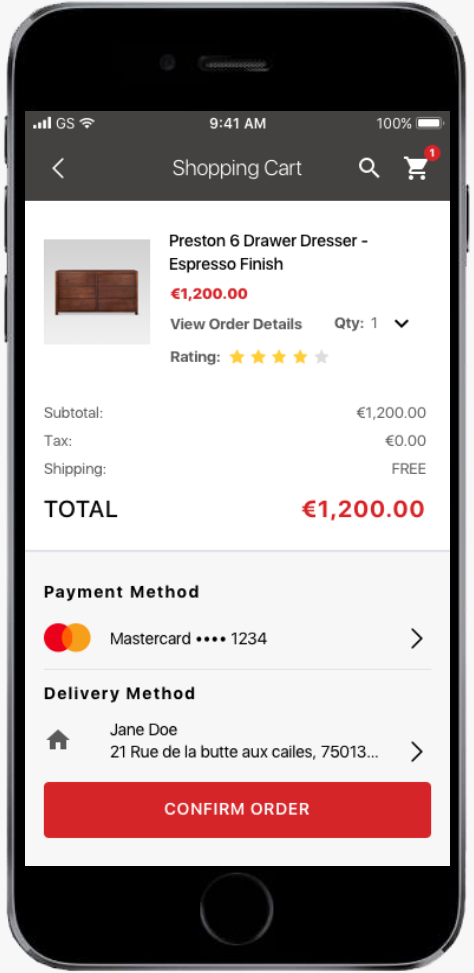
Context

The cardholder adds the selected item into the shopping cart and proceeds to the checkout page.

This example assumes the cardholder has previously purchased items with this merchant. Stored credentials from the merchant's records are prepopulated, e.g.:

- *Registered card*
- *Billing Address*
- *Delivery Address*

The EMV 3DS authentication flow will be initiated once the cardholder proceeds with the purchase and clicks on "Confirm order" button.



OUT OF BAND *Single Device* (4/11)

Context

Once the cardholder clicks on "Confirm Order" the EMV 3DS 2.1.0 flow is initiated.

Authentication flow

The 3DS requestor communicates with the 3DS Server to initiate the authentication flow.

The processing screen is displayed and the Scheme Brand is shown.

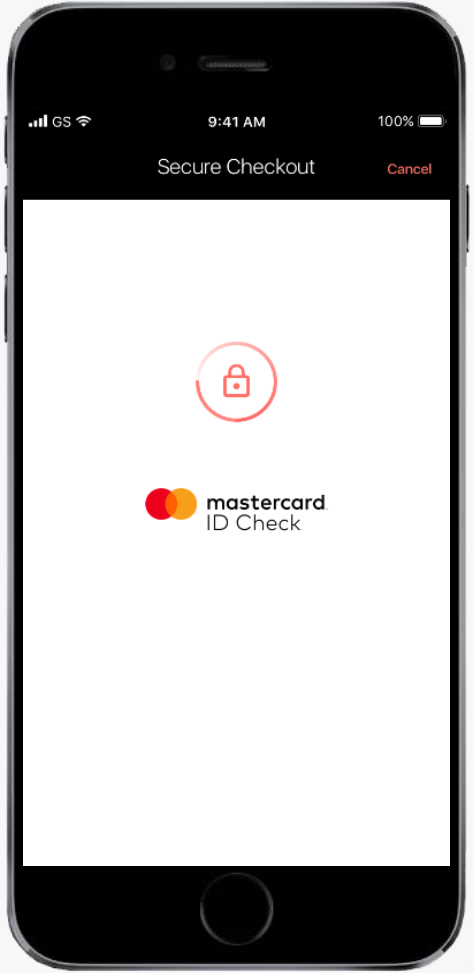
While this screen is on view to the consumer, the issuer's ACS is evaluating the risk of the transaction based on the information sent by the 3DS requestor via the EMV 3DS 2.1.0 message.

Recommendations

2.1 Scheme Brand must be clearly displayed raising the confidence in this transaction and reinforcing the security

2.2 Processing icon must be displayed

2.3 No other design element should be included in the processing screen



OUT OF BAND *Single Device* (5/11)

Authentication flow

The issuer ACS decides to challenge the cardholder with an authentication request and pushes the EMV 3DS challenge screen designed for the OOB checkout flow to the device.

The 3DS Requestor communicates with the SDK to initiate the challenge flow.

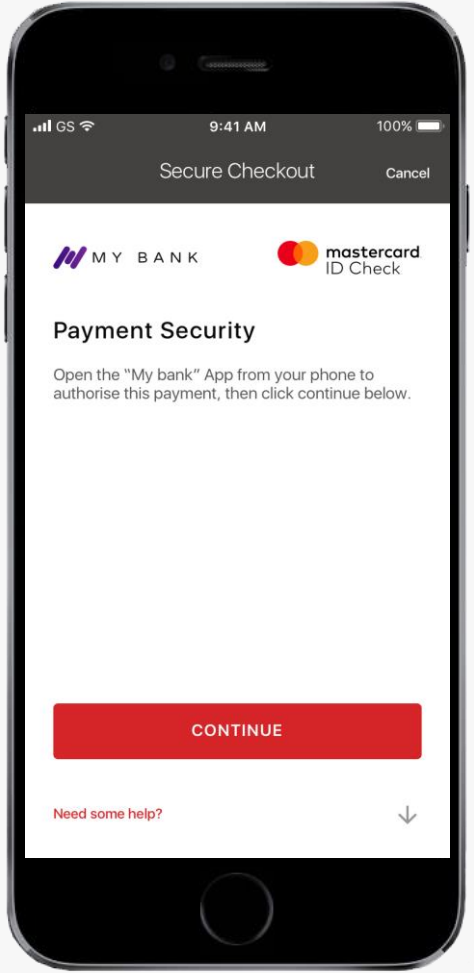
Recommendations

This screen has a consistent look and feel across device channels and authentication methods.
The EMV 3DS screen interface allows for the issuer to provide limited instructions for the OOB method within the checkout flow, as well as the issuer brand and Card Scheme.

Mastercard® recommends a very light wording and a clear instruction to open the mobile banking app.

EMV 3DS 2.1.0 specifications require a "Continue" button to be displayed.

2.4 In case a consumer clicks the "Continue" button before authenticating in the mobile banking app, an error message should be displayed ie. "First, authorise this payment using your "My Bank" app on your phone, then click continue!"



OUT OF BAND *Single Device* (6/11)

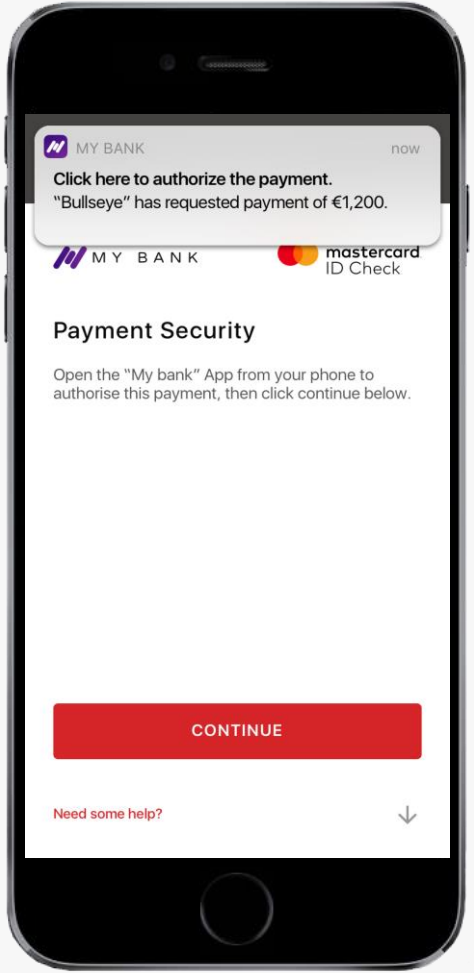
Authentication flow

The issuer ACS sends a "push notification" to the cardholder registered device to start the OOB authentication flow.

Push notification is considered as the first factor of authentication (possession of device).

Recommendations

2.5 The push notification will have a clear and simple action request in the top line *"Click here to authorise this payment"* or similar.



OUT OF BAND *Single Device* (7/11)

Authentication flow

By clicking on the push notification it will trigger the issuer app to open at the authentication page. In this example, the issuer authentication app is displayed.

After having reviewed the transaction details, the cardholder can either "Decline" the authentication request (transaction fails) or "Confirm".

By clicking "Confirm", the authentication app will trigger the fingerprint recognition process.

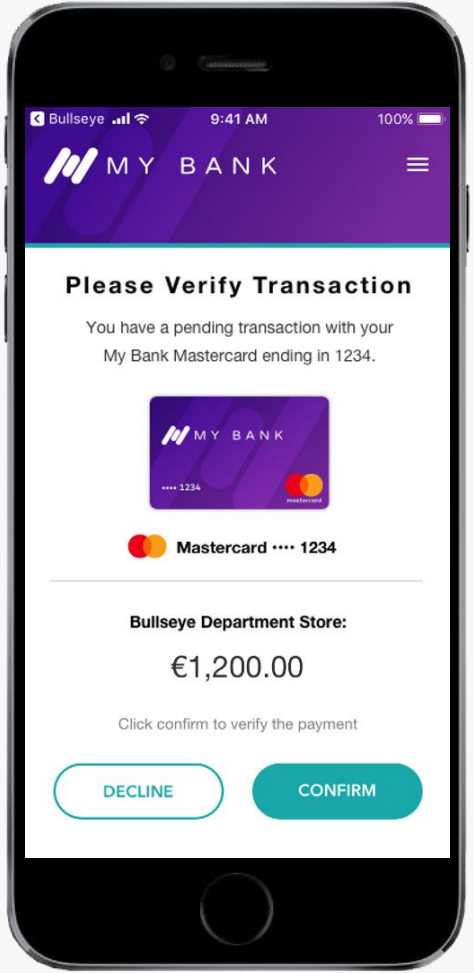
Recommendations

2.6 Only necessary information should be displayed in this step: Transaction amount, Merchant name, Card used

2.7 Card design should be displayed, following the best practice of well-known digital payment solutions

2.8 If card design cannot be displayed for technical reasons, Mastercard ID Check™ logo should be displayed in this page

2.9 If the cardholder does not click the push notification but opens the app manually, it is recommended to display the authentication request page after accessing the app



OUT OF BAND *Single Device* (8/11)

Authentication flow

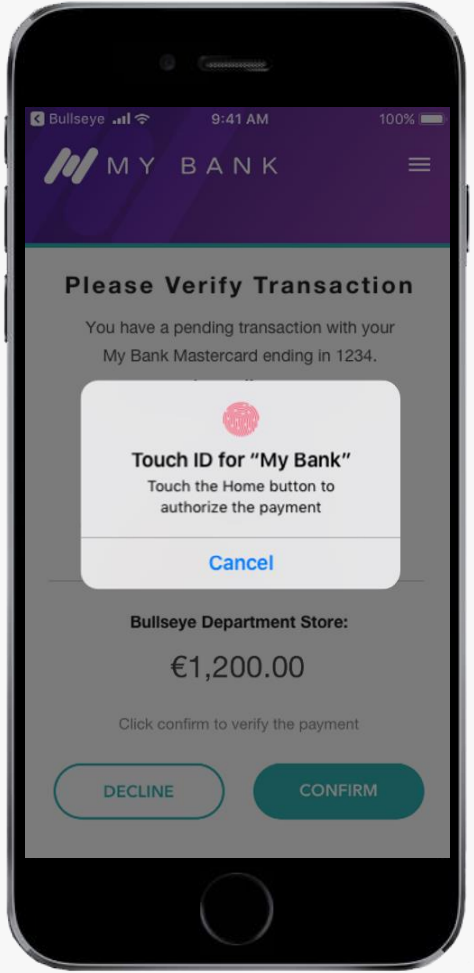
The Operating System will prompt the cardholder to use their fingerprint to authorise the payment.

Fingerprint (in this example) will be considered as the second factor of authentication (Inherence).

In the event that the fingerprint is not recognised, a fall back method must be set by the Bank. This would provide a second factor of authentication (i.e. Inherence using another biometric, or Knowledge, using a PIN).

Recommendations

The choice of fall back method is issuer specific and should build upon the process the issuer uses in order to avoid any new enrolment issues for existing customers



OUT OF BAND *Single Device (9/11)*

Authentication flow

When the second factor (e.g. fingerprint) is recognised, the issuer app will display a confirmation icon.

In EMV 3DS 2.1.0 specification, the cardholder will need to manually click the link on the top left corner of the screen to go back to the ACS challenge page to complete the authentication.
This will be required on iOS devices only.

Android does not have this friction: the app can close automatically, displaying the merchant page that has been in the background.

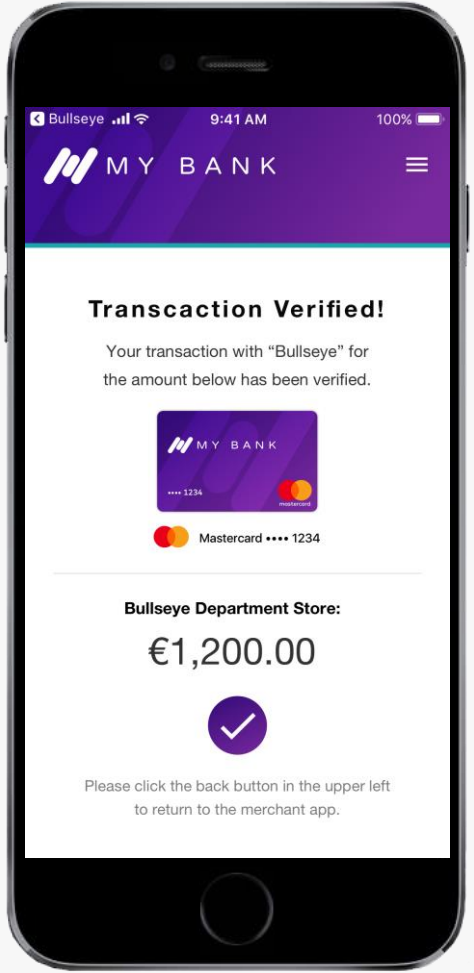
Recommendations

2.10 For the iOS checkout flow only, Mastercard® recommends issuers prompt consumers to return to the merchant app/web by adding clear instructions on the authentication completion page

2.11 For Android devices, Mastercard recommends issuers to implement the automatic closing of the app after authentication

Design Enhancem'ts

The need to manually return to the ACS challenge page in iOS has been resolved in the EMV 3DS 2.2.0 specification. For this flow to work as intended, both the OOB issuer app and the Merchant app will need to support this.



OUT OF BAND *Single Device* (10/11)

Authentication flow

The ACS will then display the second step of the OOB checkout flow within the EMV 3DS 2.1.0 specification.

EMV 3DS 2.1.0 specifications require a "Continue" button to be displayed in this page.

The cardholder clicks "Continue" to finalise the payment.

Recommendations

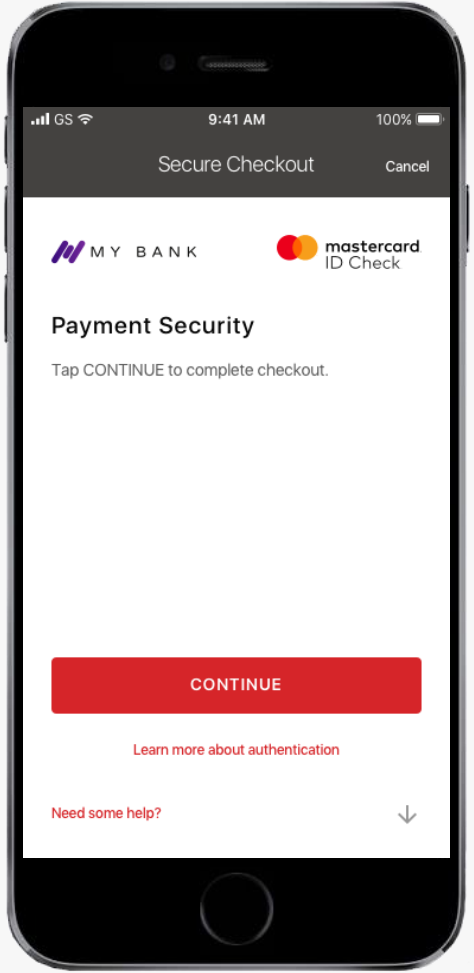
This screen has a consistent look and feel across device channels and authentication methods.

The EMVCo screen interface allows for the issuer to provide instructions for the OOB method within the checkout flows, as well as the Brand of the issuer and Card Scheme.

Mastercard® recommends a very light wording and a clear instructions.

Design Enhancem'ts

In EMV 3DS 2.2.0 specification, the "CONTINUE" step will be removed in case of a positive result. Once the cardholder has authenticated the payment with their fingerprint, the authentication app will close automatically and the merchant payment confirmation page will be displayed



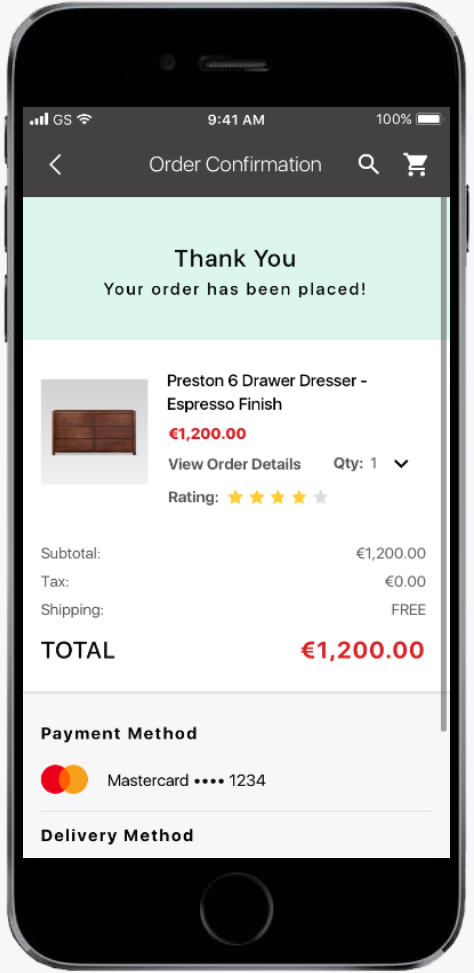
OUT OF BAND *Single Device* (11/11)

Authentication flow

The SDK validates the response with the ACS and the ACS communicates the result of the authentication via the Result Request message back to the 3DS Requestor.

The merchant confirmation page is displayed back in the merchant domain.

A Mastercard® commissioned "Online Checkout" consumer research conducted by InSites Consulting in 6 European markets in early 2018 determined that the OOB checkout flow is the second preferred option, after "Frictionless" checkout previously displayed in this document.



OUT OF BAND AUTHENTICATION
MULTIPLE DEVICES

mastercard

mastercard

OUT OF BAND *Multiple Devices* (1/9)

Multiple research studies conclude that the majority of e-commerce transactions in Europe is initiated from a laptop, tablet or PC. Mastercard® research conducted in 2018 suggests that shopping from these devices will stay relevant the next four to five years.

Mastercard has developed user flows and guidance that support the purchasing activity being undertaken on a desktop/tablet, while authentication can be controlled through the consumer mobile device.

This flow sets out Mastercard's requirements to cover this scenario when using two different devices: one for shopping and one for authenticating the transaction via a separate authentication app.

The following example shows a transaction initiated from within the merchant website (HTML flow).

The way in which the challenge screens are displayed is driven by the merchant's implementation of the EMV 3DS 2.1.0 specifications. It could be an overlay screen (as set out in the following pages) or a section embedded in the merchant checkout page.

OUT OF BAND *Multiple Devices (2/9)*

Context

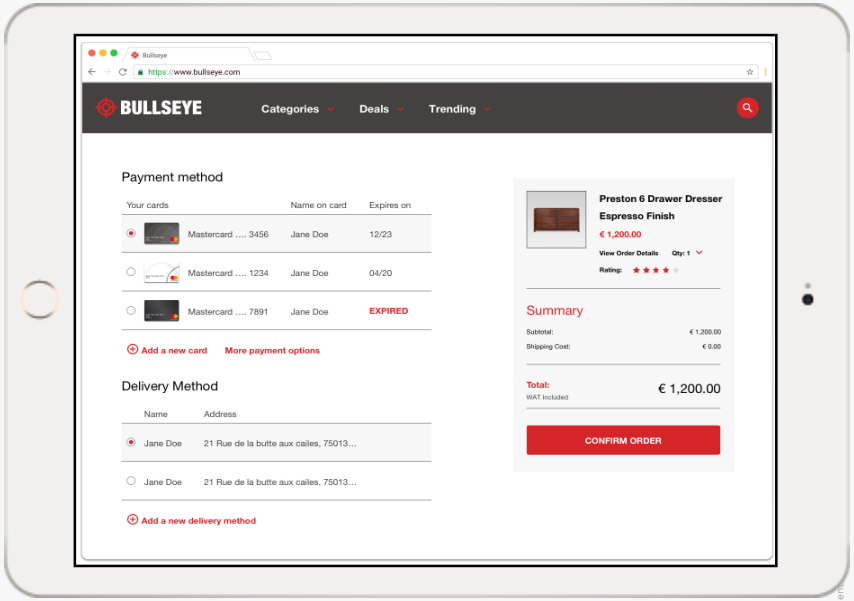
The cardholder is purchasing an item from within the browser using a tablet (image), adding the selected item into the shopping cart and proceeding to the checkout page.

This example assumes the cardholder has previously purchased items with this merchant before. Stored credentials from the merchant's records are pre-populated as previously described.

The EMV 3DS checkout flow will be initiated once the Cardholder clicks on the "Confirm order" button to proceed with the purchase.

We will be showing the activity occurring on the main shopping screen from the browser and the separate mobile device.

The mobile device screen is left blank unless there is an EMV 3DS activity to display.



OUT OF BAND *Multiple Devices (3/9)*

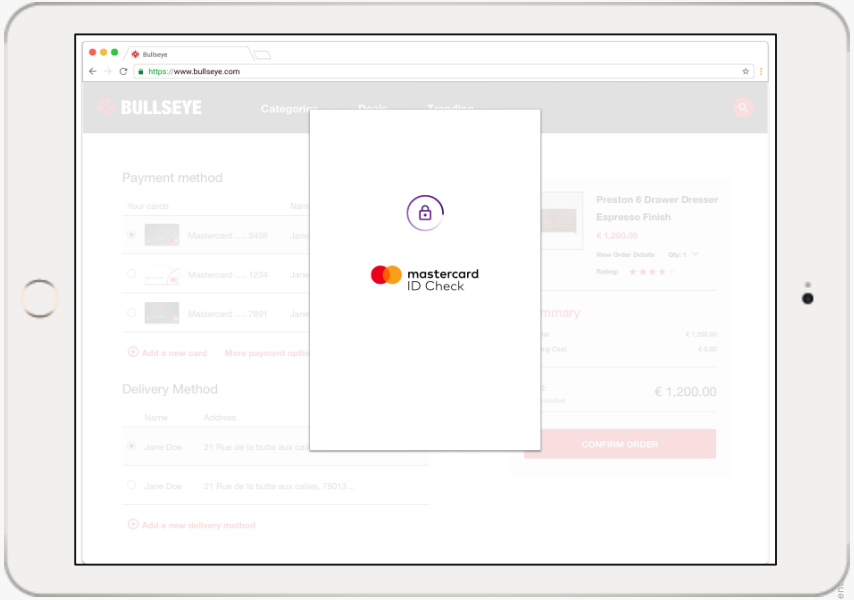
Authentication flow

The 3DS requestor communicates with the 3DS Server to initiate the authentication flow.

The processing screen is displayed and the Scheme Brand is shown.

While this screen is presented to the consumer, the issuer's ACS is evaluating the risk of the transaction.

As mentioned previously, the way in which the challenge screens are presented to the cardholder is driven by the type of EMV 3DS 2.1.0 implementation that the merchant has chosen for its checkout page. In this example, the merchant has chosen an overlay screen.



Recommendations

3.1 Scheme Brand must be clearly displayed raising the confidence in this transaction and reinforcing the security

3.2 Processing icon must be displayed

3.3 No other design element should be included in the processing screen

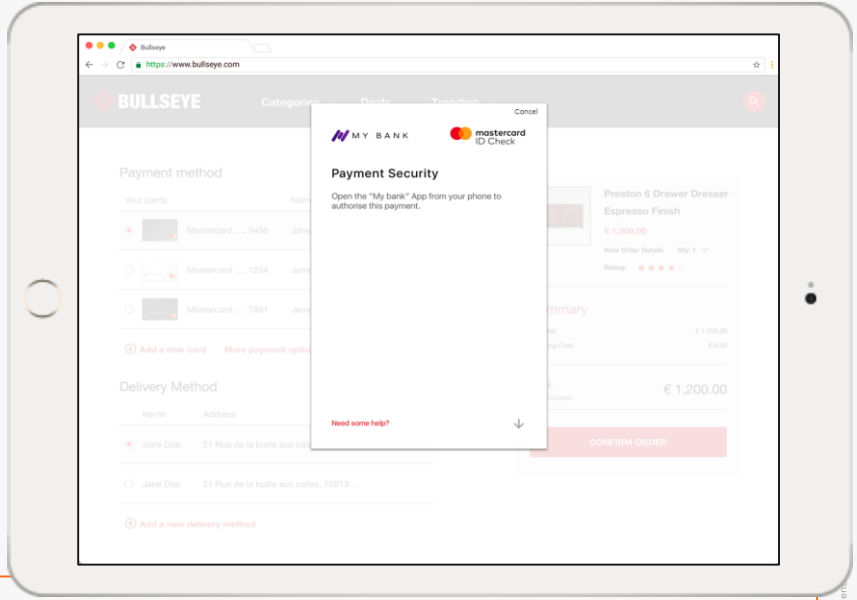
OUT OF BAND *Multiple Devices (4/9)*

Authentication flow

The issuer ACS decides to challenge the cardholder with an authentication request and pushes the EMV 3DS challenge screen designed for the OOB multi-device checkout flow.

The 3DS Requestor initiates the challenge flow, the ACS contacts the OOB back-end to initiate the OOB authentication procedure

EMV 3DS 2.1.0 specification requires a "Continue" button to be displayed. To meet this specification requirement and to ensure an optimal UX, Mastercard® strongly recommends this button to be invisible to the consumer *(see recommendation 3.4 below).*



Recommendations

The challenge screen displayed in the desktop browser is completely under control of the ACS. The EMV 3DS screen interface allows for the issuer to provide limited instructions for the OOB method within the checkout flow, as well as the issuer brand and Card Scheme. Mastercard® recommends a very light wording and a clear instruction to open the mobile banking app.

3.4 As the 'continue' button is not relevant to the transaction flow (authentication occurring through the mobile banking app) it should be displayed in the same colour as the screen background with no border, to avoid drawing the attention of the consumer

OUT OF BAND *Multiple Devices (5/9)*

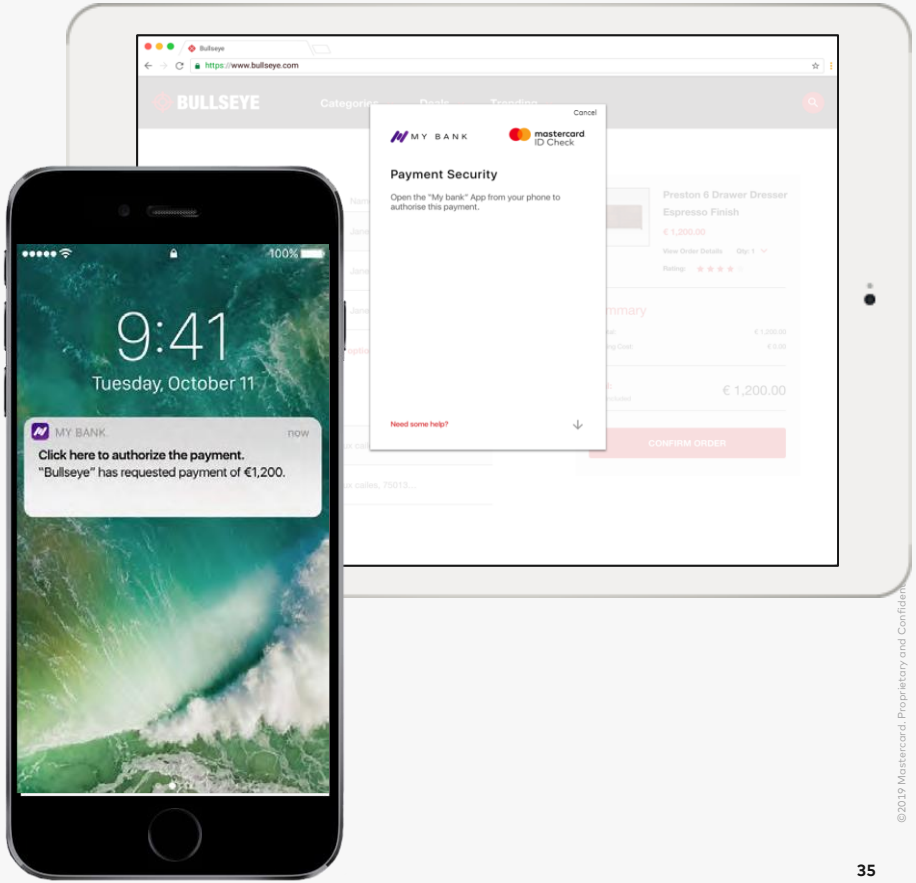
Authentication flow

The issuer ACS sends a "push notification" to the cardholder's registered device to start the OOB authentication flow.

The push notification is considered as the first factor of authentication (possession of device).

Recommendations

3.5 The push notification will have a clear and simple action request in the top line "Click here to authorise this payment" or similar

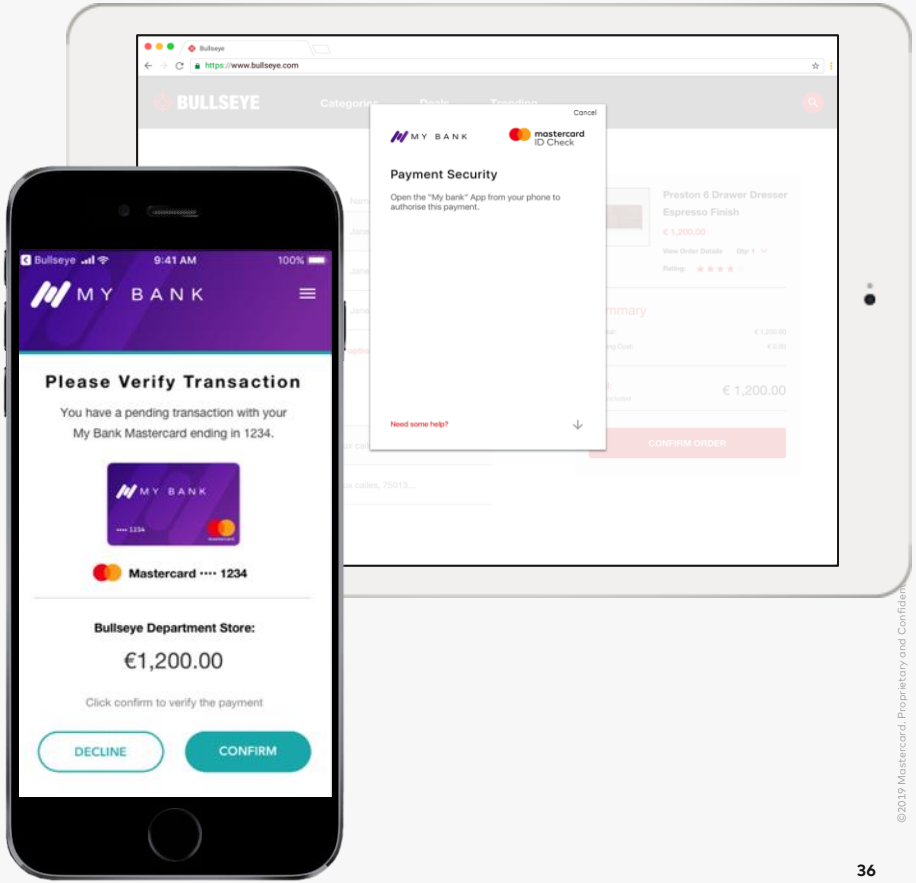


OUT OF BAND *Multiple Devices (6/9)*

Authentication flow

By clicking on the push notification it will trigger the issuer app to open at the authentication page. In this example, the issuer authentication app is displayed after having reviewed the transaction details, the cardholder can either "Decline" the authentication request (transaction fails) or "Confirm".

By clicking "Confirm", the authentication app will trigger the fingerprint recognition process.



Recommendations

3.6 Only necessary information should be displayed in this step: Transaction amount, Merchant name, Card used

3.7 Card design should be displayed

3.8 If card design cannot be displayed for technical reasons, Mastercard ID Check™ logo should be displayed in this page

3.9 If the cardholder does not click the push notification but opens the app manually, it is recommended to display the authentication request page after accessing the app

OUT OF BAND *Multiple Devices (7/9)*

Authentication flow

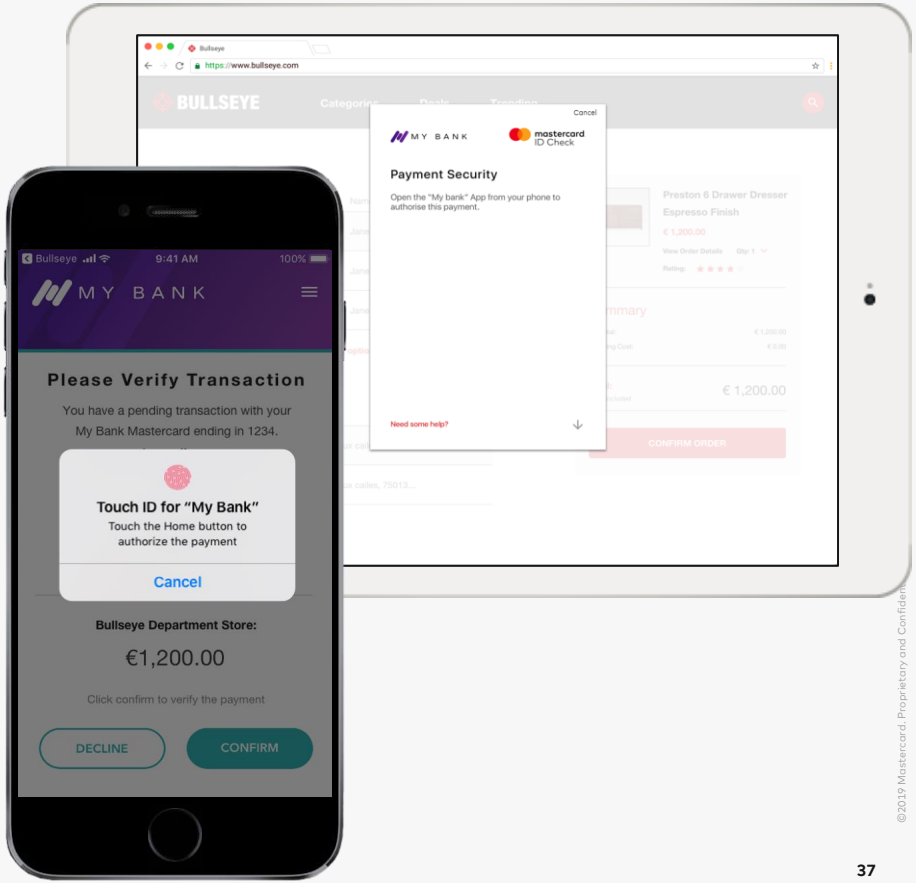
The Operating System will prompt the cardholder to use their fingerprint to authorise the payment.

Fingerprint (in this example) will be considered as the second factor of authentication (Inherence).

In the event that the fingerprint is not recognised, a fall back method must be set by the Bank. This would provide a second factor of authentication (i.e. Inherence using another biometric, or Knowledge, using a PIN).

Recommendations

The choice of fall back method is issuer specific and should build upon the process the issuer uses in order to avoid any new enrolment issues for existing customers.



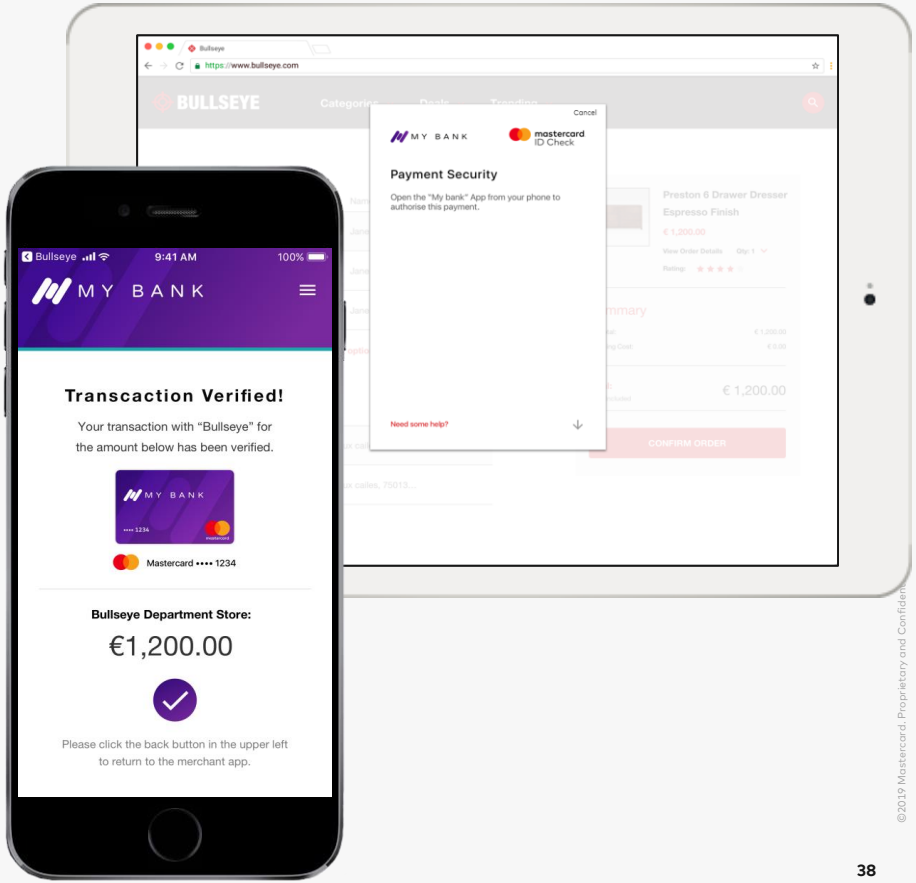
OUT OF BAND *Multiple Devices (8/9)*

Authentication flow

When the second factor (e.g. fingerprint) is recognised, the issuer app will display a confirmation icon.

Recommendations

3.10 As soon as the authentication is completed, the issuer app should communicate the authentication result to the ACS



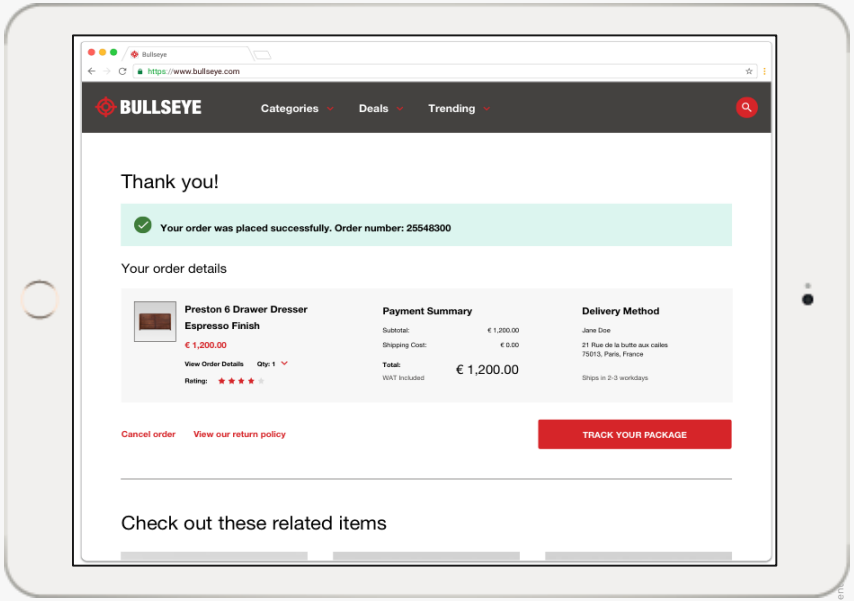
OUT OF BAND *Multiple Devices (9/9)*

Authentication flow

After the cardholder has completed the authentication in the issuer app, the merchant confirmation page is automatically displayed on the desktop with no further processing screens displayed or action required by the consumer.

Recommendations

3.11 Since the "continue" button is now invisible to the consumer, Mastercard recommends the ACS should design the HTML to be able to support "polling functionality" so that the merchant confirmation page is then displayed automatically. This provides the optimum consumer user experience.



ONE TIME PASSCODE VIA SMS

mastercard

ONE TIME PASSCODE VIA SMS (1/9)

One Time Passcode (OTP) via SMS is one of the most commonly used methods for 3DS authentication in Europe today. With the EMV 3DS specifications it is possible to achieve an ideal UX when the issuers ACS decides to adopt OTP via SMS as a two factor authentication method.

Since June 2018, this authentication method is under evaluation as the European Banking Association (EBA) stated that card data is not considered a valid "knowledge" factor. Mastercard® believes that OTP via SMS within EMV 3DS 2 rails represents a new and innovative authentication solution compliant with SCA.

Card data is a valid authentication element by itself. Thanks to technological developments, stealing card data and successfully reusing it has become increasingly difficult and often impossible. Its use as an authentication element together with SMS OTP has decreased fraud to very low levels.

OTP is recognised as an ownership authentication element as it may be sent to a phone securely associated with the cardholder or generated by an app in the cardholder's possession.

EMV 3DS behaviour-based information is a valid inherence authentication element, provided sufficient behaviour based biometric information is transmitted through the EMV 3DS message.

ONE TIME PASSCODE VIA SMS (2/9)

Context

The cardholder is shopping within a merchant app.

The cardholder does not have an authentication app installed (or the issuer is not offering biometric authentication). The transaction will be authenticated using an OTP sent via SMS.

The authentication flow would look the same if the cardholder was within a mobile browser or a web view environment embedded in a merchant app.

Please note:

Mastercard® is not proposing best practice/ user experience for checkout / shopping cart flows throughout this document, as these remain within the merchant/PSP domain. These pages are shown as an example to portray the customer journey and aid explanation.

ONE TIME PASSCODE VIA SMS (3/9)

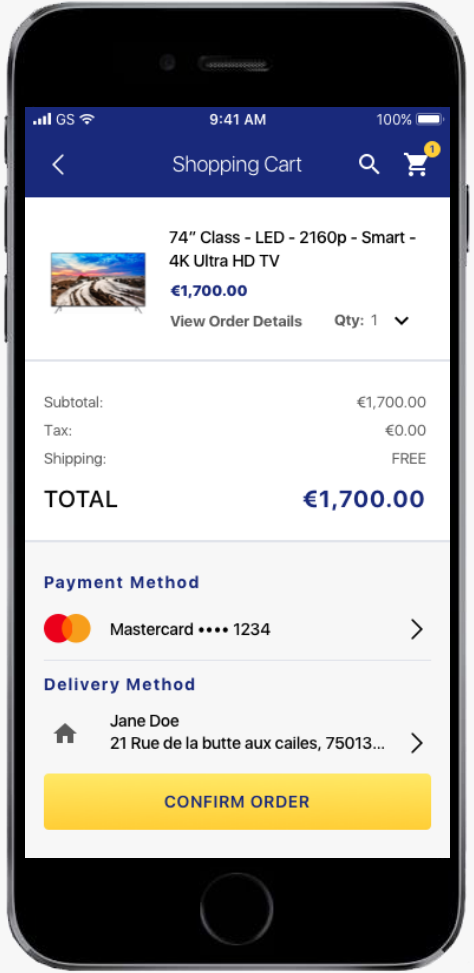
Context

The cardholder adds the selected item into the shopping cart and proceeds to the checkout page.

This example assumes the cardholder has previously purchased items with this merchant. Stored credentials from the merchant's records are prepopulated, e.g.:

- *Registered card*
- *Billing Address*
- *Delivery Address*

The EMV 3DS authentication flow will be initiated once the cardholder proceeds with the purchase and clicks on "Confirm order" button.



ONE TIME PASSCODE VIA SMS (4/9)

Context

Once the cardholder clicks on "Confirm Order" the EMV 3DS 2.1.0 flow is initiated.

Authentication flow

The 3DS requestor communicates with the 3DS Server to initiate the authentication flow.

The processing screen is displayed and the Scheme Brand is shown.

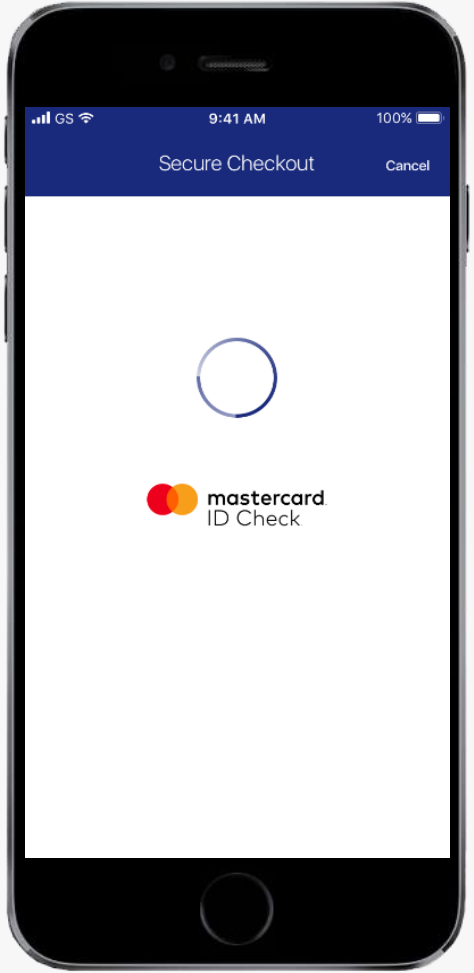
While this screen is on view to the consumer, the issuer's ACS is evaluating the risk of the transaction based on the information sent by the 3DS requestor via the EMV 3DS 2.1.0 message.

Recommendations

4.1 Scheme Brand must be clearly displayed raising the confidence in this transaction and reinforcing the security

4.2 Processing icon must be displayed

4.3 No other design element should be included in the processing screen



ONE TIME PASSCODE VIA SMS (5/9)

Authentication flow

The issuer ACS decides to challenge the cardholder with an authentication request and pushes the EMV 3DS challenge screen designed for the OTP via SMS flow.

The 3DS Requestor communicates with the SDK to initiate the challenge flow.

Recommendations

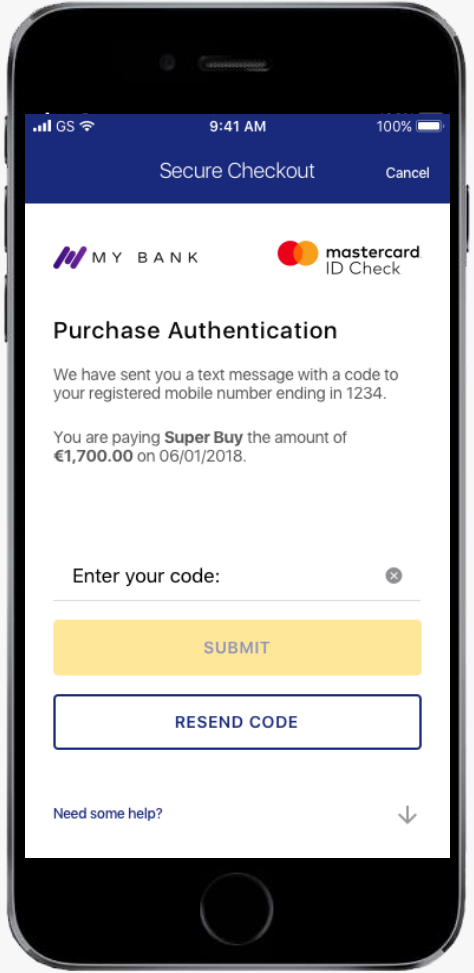
This screen has a consistent look and feel across device channels and authentication methods.

The EMV 3DS screen interface allows for the issuer to provide instructions for the OTP via SMS method within the checkout flow, as well as the issuer brand and Card Scheme.

Mastercard® recommends a very light wording and clear instructions to the cardholder.

EMV 3DS 2.1.0 specifications require both a "Submit" button and a "Resend Code" button to be displayed.

4.4 The "Enter your code" input field is displayed in this screen, together with the "Submit" and "Resend code" buttons



ONE TIME PASSCODE VIA SMS (6/9)

Authentication flow

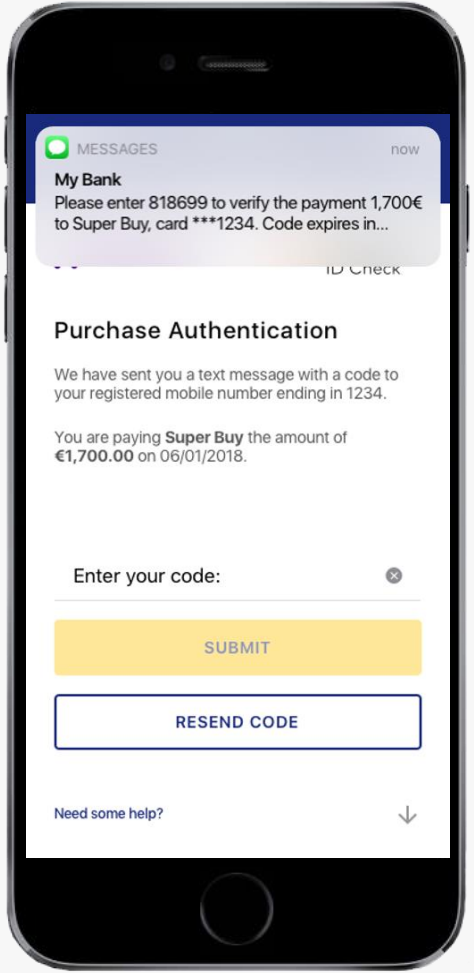
The issuer ACS sends an SMS to the cardholder's registered device to start the OTP via SMS flow.

Recommendations

4.5 OTP code is displayed at the beginning of the SMS, so that the cardholder can read and enter the code into the field without leaving the authentication environment

4.6 OTP code should be no longer than 6 digits

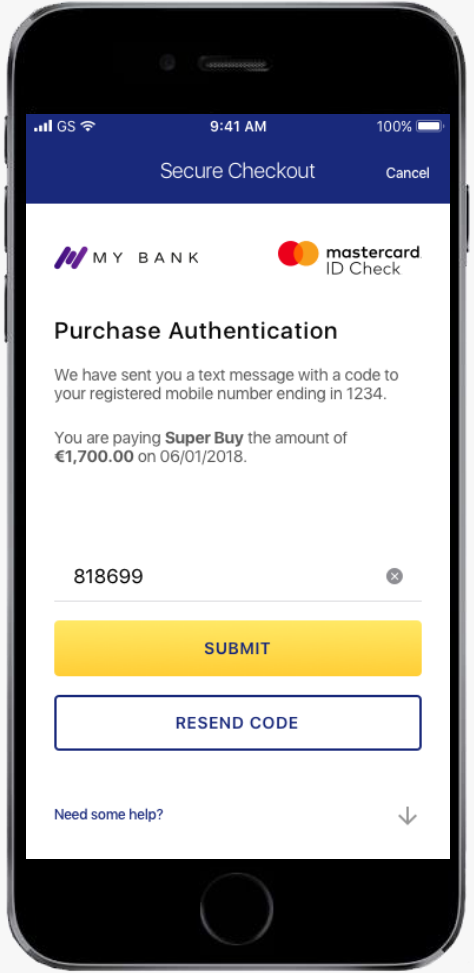
4.7 Avoid the word "OTP" on the authentication pages sent by the ACS, and on the marketing/ communication materials provided by the bank: OTP is a technical acronym that the cardholder does not immediately understand and would require education



ONE TIME PASSCODE VIA SMS (7/9)

Authentication flow

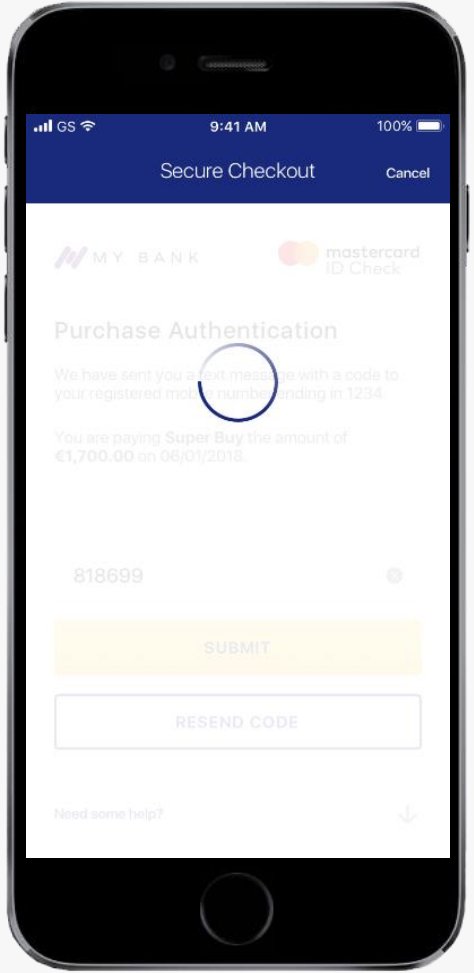
The cardholder enters the OTP code received via SMS and clicks on "Submit" to send the authentication details to the ACS for validation



ONE TIME PASSCODE VIA SMS (8/9)

Authentication flow

The SDK validates the response with the ACS and the ACS communicates the result of the authentication via the Result Request message back to the 3DS Requestor.



ONE TIME PASSCODE VIA SMS (9/9)

Authentication flow

The merchant confirmation page is then displayed to the consumer