EMV® 3-D Secure

White Paper

Frictionless Flow, Out-of-Band and Recurring Transaction Use Cases

Version 1.0

April 2024

Legal Notice

This document is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Contents

Tables

1 Introduction

The purpose of this EMV® 3-D Secure White Paper (White Paper) is to promote a better understanding of certain EMV® 3-D Secure (3DS) features and provide example use cases that highlight their benefits.

The 3DS protocol is a security measure designed to provide an additional layer of protection for online transactions and to reduce the risk of fraud in e-commerce transactions.

This document describes three of the 3DS flows: the Frictionless Flow (Section 2), the Challenge Flow (Section 3), and Recurring and Instalment Transactions (Section 4), along with example use cases.

The use cases presented in this document are not exhaustive and other use cases may exist. This document does not describe the practical implementation of any specific use case, and such implementations may vary by 3DS Programme.

This EMV® 3-D Secure White Paper accompanies and complements the EMV® 3-D Secure Specification (3DS Specification) and supporting documentation. Where additional relevant information on a given subject is available in any of these documents, references to specific sections in the documents are provided to avoid duplication.

For certain features, the document highlights the differences that may exist between the different specification versions active at the time of release of this document.

1.1 Audience and Structure

Structure

This EMV® 3-D Secure White Paper is structured to provide a comprehensive understanding of the 3DS Specification, presenting its key features across different perspectives.

Each key feature section begins with a business overview, which outlines the functionalities, objectives and benefits, and the ways in which they enhance 3DS transactions, their security and user experience. This is followed by a flow diagram showing how the feature can be used during a 3DS transaction, along with related data. Lastly, for certain features, a sequence of screens illustrates the user experience.

Where applicable, the White Paper also explains how the key features can be leveraged depending on which 3DS Specification version is supported (version 2.2, version 2.2 in combination with the Bridging Message Extension, or version 2.3.1).

Audience

The document is aimed at diverse groups with varying levels of expertise.

Firstly, it addresses stakeholders seeking a high-level overview of 3DS capabilities, presenting its business value and potential impact on improving user security and trust in online transactions.

It then provides information on the technical details of the 3DS Specification for experts involved in the development or implementation of 3DS applications.

Lastly, it is aimed at those interested in the user experience aspect and in learning how 3DS aims to streamline and enhance the authentication process for end users.

By addressing the needs of these distinct audiences, the document ensures comprehensive coverage of the 3DS Specification from different perspectives, and is intended for use by all participants of the 3DS ecosystem.

1.2 Notational Conventions

Abbreviations

For a list of abbreviations used in the 3DS White Paper, refer to Table 1.4 in Section 1.9 of the *EMV® 3-D Secure Protocol and Core Functions Specification*.

Terminology and Conventions

The 3DS White Paper uses the following words which have a specific meaning:

3DS Requestor – Merchant in the context of a purchase transaction.

Assumptions

Where provided, assumptions for a given use case are specific to that use case example, but not the wider use case. Different assumptions are part of the same use case but would refer to a different use case example.

Preconditions

Preconditions for a given use case are those which must occur in order for the use case to exist.

2 Improving Risk Analysis and Frictionless Flow

2.1 Business Overview

The use of risk-based authentication allows issuers to accept transactions without having to challenge cardholders, which results in a frictionless process for both cardholders and merchants. The merchants benefit from adopting the 3DS protocol by protecting against fraudulent chargebacks and ensuring that the cardholders are secure from fraudulent transactions, while the cardholders have a seamless experience using the merchants' platform as they are not being challenged. This reduction in Challenge Flow interactions may lower the drop-off rate caused by using the 3DS protocol.

In the Frictionless Flow, the Cardholder's identity is verified automatically by the Issuer without the need for additional authentication steps or Cardholder interaction.

The Frictionless Flow is achieved through real-time risk assessment that takes into account various types of information, such as:

- details of the transaction (amount, currency, Merchant, recurring or non-recurring…)
- device used by the Cardholder to perform the transaction
- the Cardholder's transaction history and relation with the Merchant
- technical information such as device location or IP address

to determine the level of risk associated with the transaction.

To enhance transaction risk assessment, the Issuer can use two 3DS features:

- **Trust List** enables the cardholder to create a list of preferred merchants. Enabling the cardholder to provide their spending habits improves the Issuer's risk assessment. For additional details, refer to *Trust List* Managed by the ACS / Issuer – Overviewin the *Technical Features* section.

- **Device Binding** enables the Cardholder to link the Device used for e-commerce transactions to their payment card (Cardholder Account Number). In return, the Issuer uses this information in transaction risk assessment as an indicator that the genuine Cardholder is performing the transaction using the same payment card on the same device. For additional details, refer to *Device Binding* in the *Technical Features* section.

The Frictionless Flow of the 3DS protocol provides a convenient and secure experience for online transactions. The automatic verification process based on real-time risk assessment helps to reduce the risk of fraud while keeping the transaction secure. The integration of the Frictionless Flow into the transaction provides a seamless shopping experience to both the Cardholder and the Merchant, making it an important aspect of online payment security.

2.2 Technical Features

2.2.1 Trust List Managed by the ACS / Issuer – Overview

The Issuer/ACS offers the Cardholder the option to add their preferred or trusted Merchant to their trust list during a 3DS challenge when in direct communication with the Cardholder. The Issuer controls the selection of merchants proposed in the Trust List (for example, only offering the Trust List service for low-risk merchants). The Issuer will consider the risk associated with the merchant type and market, as well as the Cardholder's transaction history.

The 3DS Trust List feature may be used for the trusted beneficiary exemption in countries in scope of the Revised Payment Services Directive (PSD2).

The 3DS Specification does not prevent issuers from providing alternative channels to cardholders to manage the trusted beneficiaries list (for example, e-banking).

An alternative use case is the Trust List managed by the DS as described in Section 2.2.3.

Benefits by actor

- Merchant
  - Fewer challenges
  - Faster transactions
- Issuer
  - Better knowledge of cardholder purchasing habits
  - Opportunity to pre-select "trusted" merchants
  - Reduced need to challenge
- Cardholder
  - Fewer challenges
  - Faster transactions

2.2.2 Trust List Flow and Data

Preconditions

The ACS has a Trust List Management System and can display the Trust List prompt/screen to the Cardholder during a 3DS challenge.

Optional: The ACS indicates support of the Trust List in the Card Range Data (ACS Information Indicator - 04 = Trust List Supported).

Note: The ACS uses some or all of the merchant information (Merchant Name, 3DS Requestor Name, 3DS Requestor ID) to manage the Trust List. Therefore, it is essential that the Merchant and/or the 3DS Server provide consistent merchant information across the Trust List enrolment and subsequent transactions.

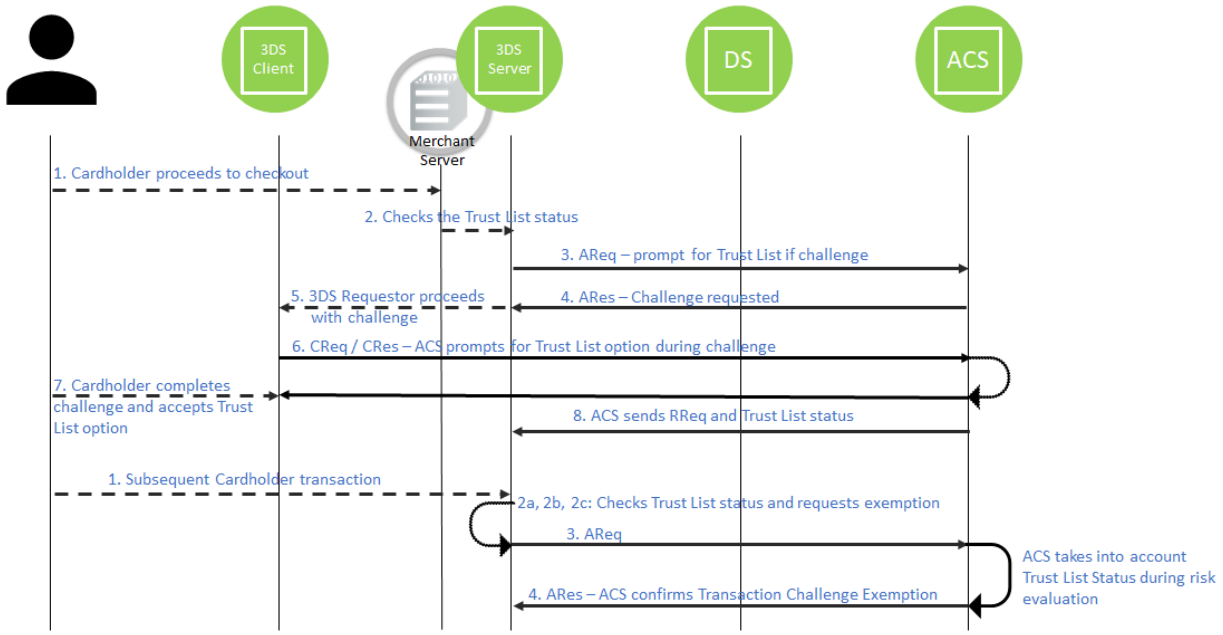
Sequence Diagram

The Cardholder enrols a Merchant on their Trust List that is managed by the Issuer/ACS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor/3DS Server may:
   a. Check if the ACS supports the Trust List by confirming that ACS Information Indicator = 04 (Trust List Supported)
   b. Set the 3DS Requestor Challenge Indicator to 09 (= Challenge requested – Trust List prompt requested if challenge required) in the Authentication Request (AReq) message to indicate to the ACS that it should prompt for the Trust List during the challenge.
3. The 3DS Server sends the AReq message.
4. The ACS responds with an Authentication Response (ARes) message requesting a challenge.
5. The 3DS Server proceeds with the challenge.
6. The ACS proceeds with the challenge and provides the prompt for the Trust List option.
7. The Cardholder completes the challenge and accepts the Trust List option (enrols the Merchant on the Trust List).
8. The ACS provides the outcome of the authentication in a Results Request (RReq) message, and optionally the Trust List Status using the Trust List Status and the Trust List Status Source.

In a subsequent transaction with the same Cardholder and Merchant:

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor/3DS Server may:
   a. Check the Trust List Status of the Cardholder.
   b. Check if the ACS supports the Trust List exemption by confirming that ACS Information Indicator = 09 (Trust List Exemption Supported)
   c. Set the 3DS Requestor Challenge Indicator to 08 (= No challenge requested – use Trust List exemption if no challenge required) in the AReq message.
3. The 3DS Server sends the AReq message.
4. As a result of the risk assessment, the ACS may apply the Trust List exemption, and may report it in the Transaction Challenge Exemption (= 08) in an ARes message.



Note: Step 6. CReq/CRes: refer to Trust List templates for the user interface.

3DS Data Elements Related to the Trust List

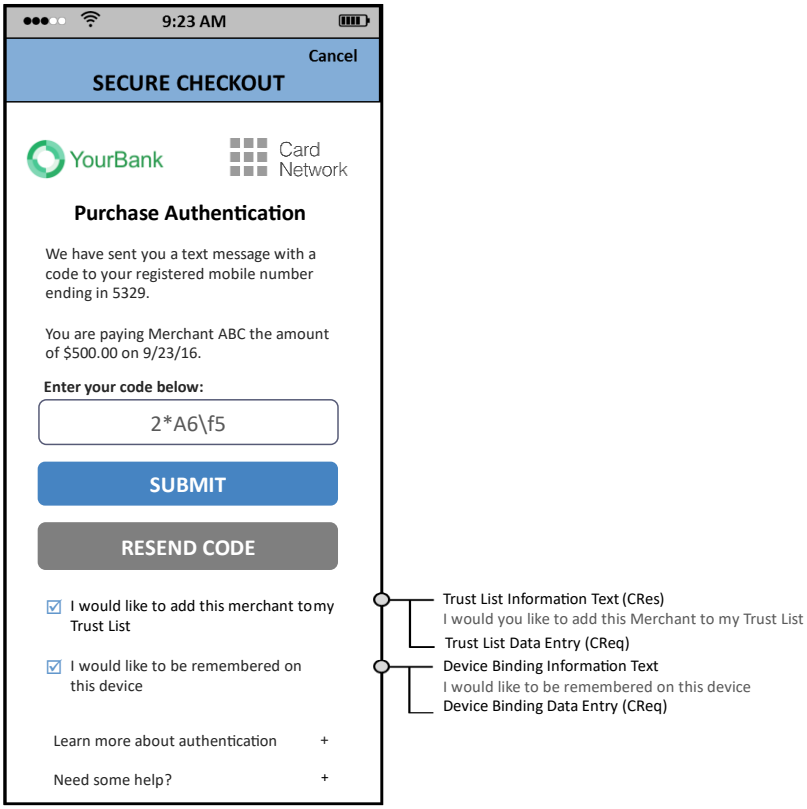
Table 2.1: 3DS Data Elements Related to the Trust List

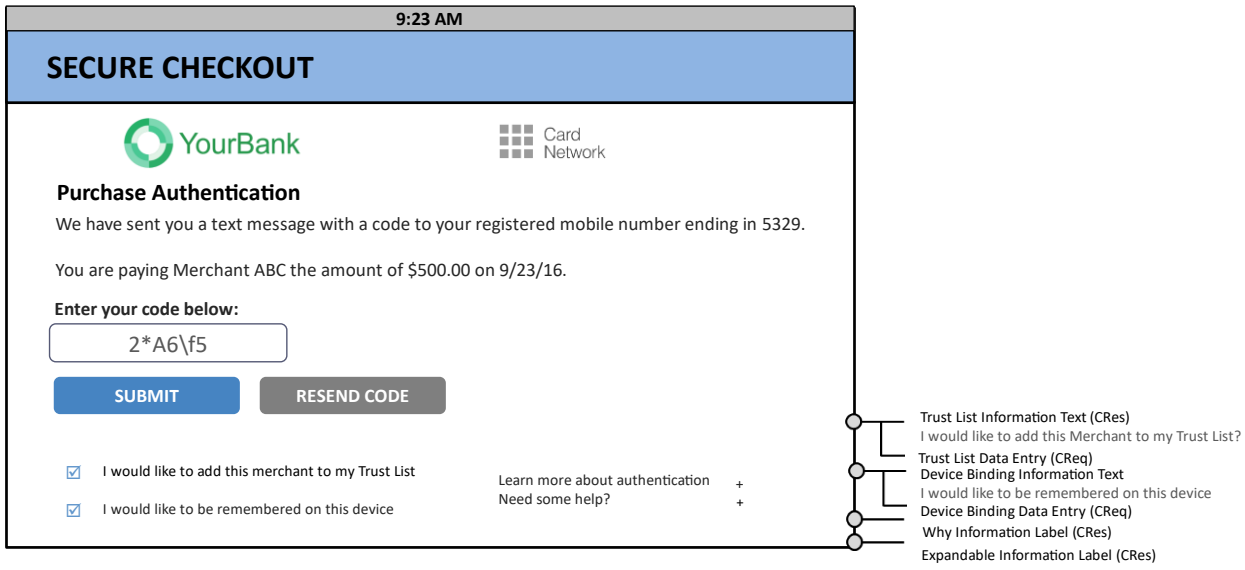
Data Element	Description	Version
3DS Requestor Challenge Indicator	Indicates whether a challenge is requested for this transaction.	2.3.1 2.2
3RI Indicator	Indicates the type of 3RI request. This data element provides additional information to the ACS to determine the best approach for handling a 3RI request. A value of 10 indicates a Trust List Status check.	2.3.1 2.2
ACS Information Indicator	Provides additional information for a particular Protocol Version to the 3DS Server. The element lists all applicable values for the card range.	2.3.1 2.2

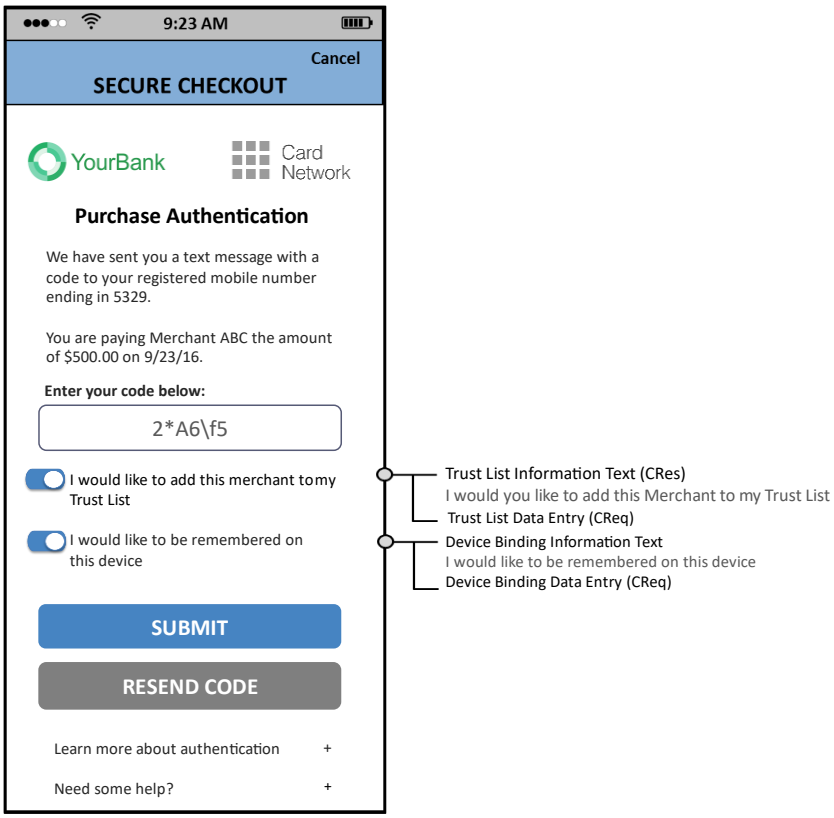
Data Element	Description	Version
Card Range Data	Card range data from the DS indicating the most recent Protocol Versions supported by the ACS, and, optionally, the DS that hosts that range, and, if configured, the ACS URL for the 3DS Method. Additionally, it identifies the 3DS features supported by the ACS in the ACS Information Indicator, such as Trust List or Decoupled Authentication. Trust List indicators are defined in the ACS Information Indicator: - 04 = Trust List Supported for v2.2 and v2.3 - 09 = Trust List Exemption Supported for v2.3	2.3.1 2.2
Toggle Position Indicator	Indicates if the Trust List and/or Device Binding prompt should be presented below or above the action buttons.	2.3.1
Transaction Challenge Exemption	Exemption applied by the ACS to authenticate the transaction without requesting a challenge.	2.3.1 2.2 + Bridging Message Extension
Trust List Data Entry	Indicator provided by the 3DS SDK to the ACS to confirm whether the Cardholder gives consent to the Trust List.	2.3.1 2.2
Trust List Information Text	Text provided by the ACS to the Cardholder during a Trust List transaction.	2.3.1 2.2
Trust List Status	Enables the communication of Trust List Status between the ACS, the DS and the 3DS Requestor.	2.3.1 2.2
Trust List Status Source	This data element will be populated by the system setting Trust List Status.	2.3.1 2.2

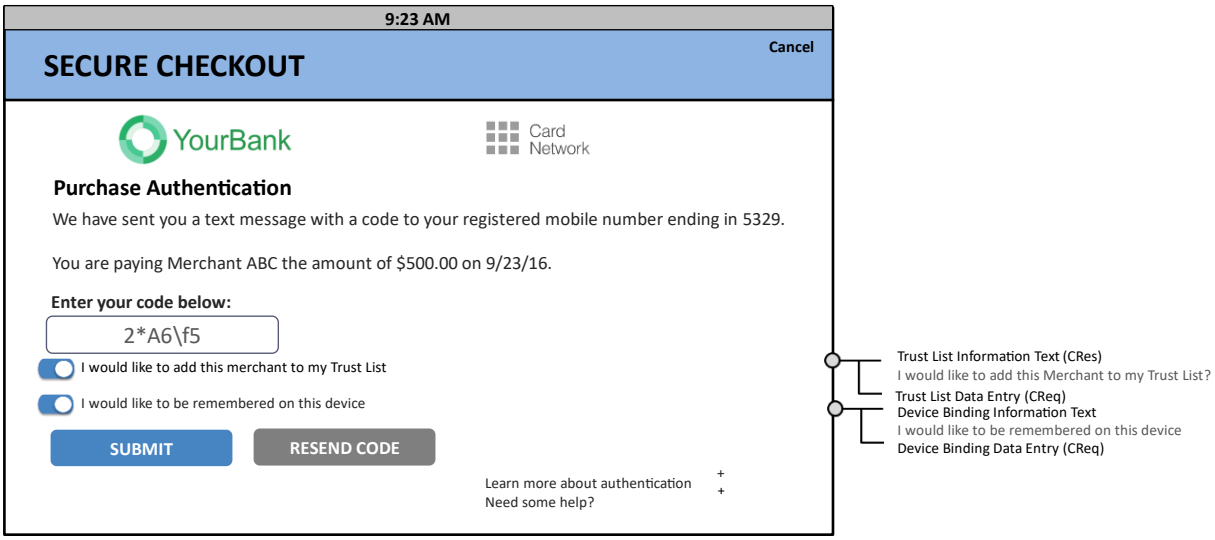
Note: The term “Trust List” is used in version 2.3.1 of the 3DS Specification, replacing the terms “Whitelist” and “Whitelisting” used in version 2.2.

App Flow – User Interface Related to the Trust List









Note: Checkbox, radio button or any relevant user interface may be used to offer the Trust List and Device Binding options.

2.2.3 Alternative Use Case – Trust List Managed by the DS

Preconditions

The DS has a Trust List Management System and an agreement with the ACS to manage the Trust List on its behalf.

The ACS is able to display the Trust List prompt/screen to the Cardholder during the 3DS challenge.

Optional: The ACS or DS indicates support of the Trust List in the Card Range Data (ACS Information Indicator – 04 = Trust List Supported)

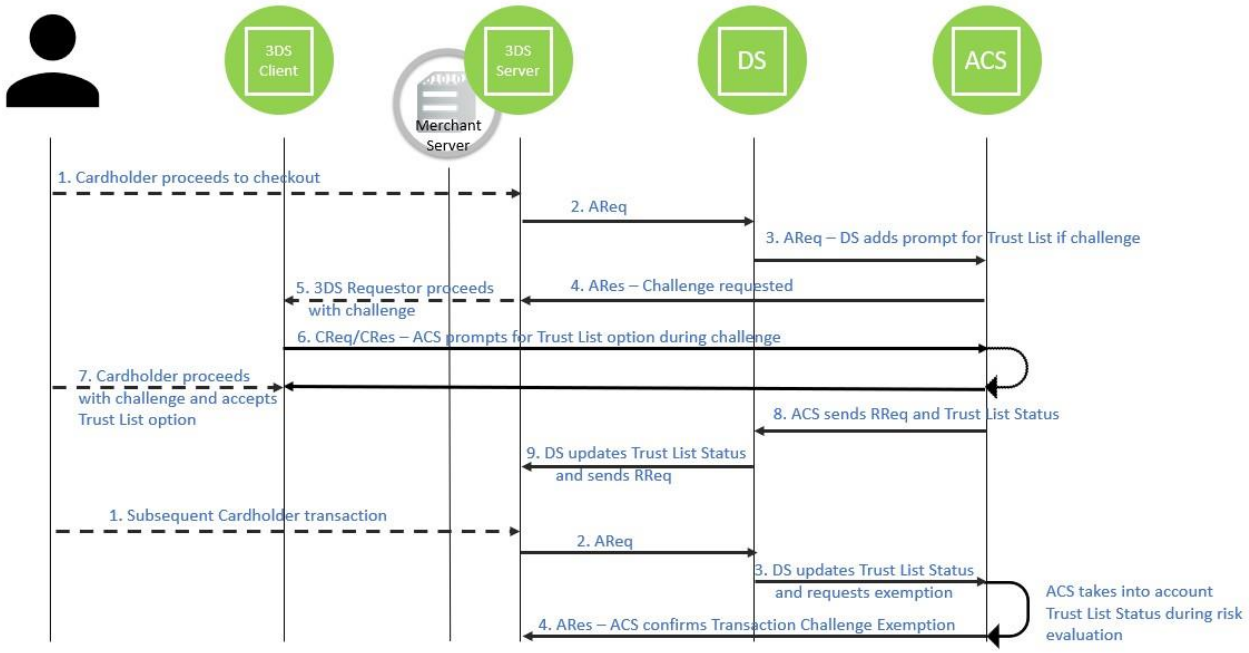
Sequence Diagram

The Cardholder enrols a Merchant on their Trust List that is managed by the DS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Server sends an AReq message.
3. The DS sets the 3DS Requestor Challenge Indicator to 09 (= Challenge requested – Trust List prompt requested if challenge required) to indicate to the ACS that it should prompt for the Trust List during the challenge.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Server proceeds with the challenge.
6. The ACS proceeds with the challenge and provides the prompt for the Trust List option.
7. The Cardholder accepts the Trust List option and completes the challenge.
8. The ACS provides the outcome of the authentication in the RReq message, and the Trust List Status to the DS using the Trust List Status and Trust List Status Source.
9. The DS updates the Trust List Status for this Cardholder account in its Trust List management system, and optionally provides the feedback to the 3DS Server using the Trust List Status and the Trust List Status Source in the RReq message.

In a subsequent transaction with the same Cardholder and Merchant:

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Server sends an AReq message.
3. The DS updates the AReq message from the 3DS Server with the Trust List Status and Trust List Status Source, and sets the 3DS Requestor Challenge Indicator to 08 (= No challenge requested – use Trust List exemption if no challenge required).
4. As a result of the risk assessment, the ACS may apply the Trust List exemption, and may report it in the Transaction Challenge Exemption (= 08) in an ARes message.



Note: Step 6. CReq/CRes: refer to Trust List templates for the user interface.

2.2.4 Device Binding

In this White Paper, Device Binding is understood to denote the process to link the Consumer Device used for a transaction to the Cardholder Account.

Device Binding may be managed by any 3DS component.

The ACS, the DS or the 3DS Server may be the source of the Device Binding Status information.

Benefits by actor

- Merchant

  Reduced need to challenge for returning cardholders
- Issuer
  - Better knowledge of cardholder purchasing habits
  - Reduced need to challenge
- Cardholder

  Feels more secure as transactions not performed on the device are more likely to be challenged

Use Case Overview

The ACS offers the Cardholder the option to link the device used for the transaction to the Cardholder Account Number during a 3DS challenge. The Device Binding Status provides to the ACS additional information that could be used for transaction risk assessment.

The 3DS Specification does not prevent issuers from providing alternative channels to cardholders to manage the Device Binding information (for example, e-banking).

The 3DS Specification does not define how the ACS identifies the Consumer Device.

Preconditions

The ACS has a Device Binding management system and is able to display the Device Binding prompt/screen to the Cardholder during the 3DS challenge.

The ACS is able to identify the Consumer Device.

Note: How the ACS identifies the Consumer Device is outside the scope of the 3DS Specification.

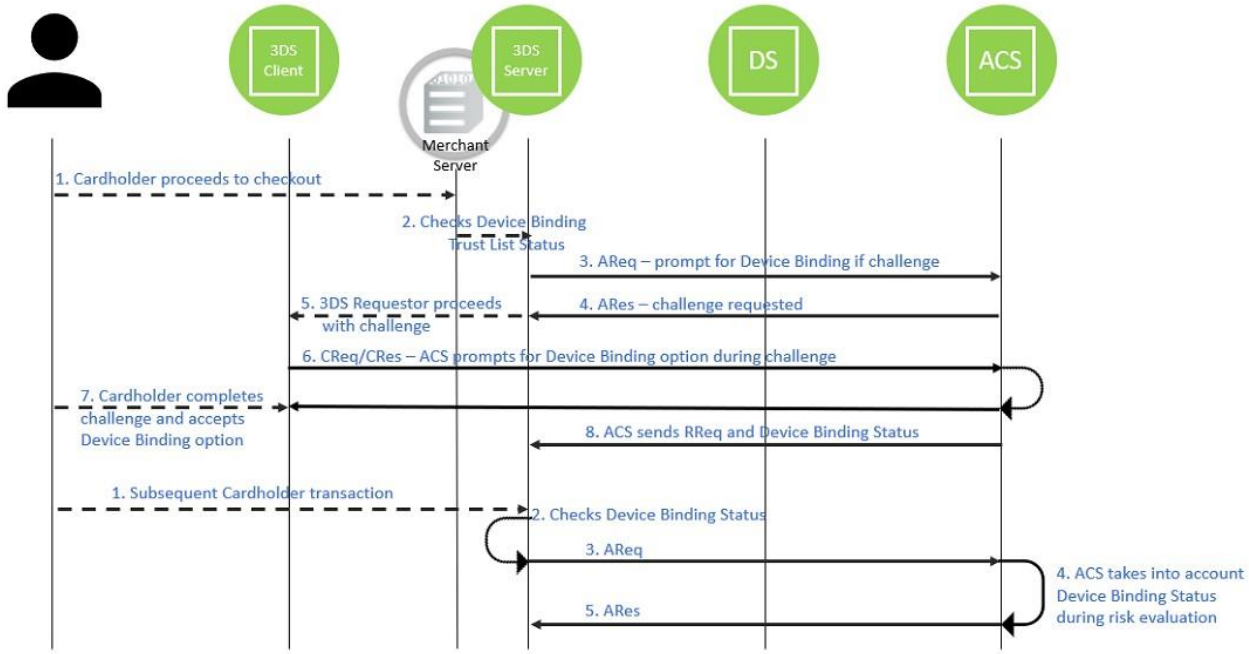
Sequence Diagram

The Cardholder accepts the Device Binding option that is managed by the ACS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. Optionally, the 3DS Requestor/3DS Server:
   a. Checks if the ACS supports Device Binding by confirming that ACS Information Indicator = 05 (Device Binding Supported).
   b. Sets the 3DS Requestor Challenge Indicator to 12 (= Challenge requested – Device Binding prompt requested if challenge required) in the AReq message to indicate to the ACS that it should prompt for Device Binding during the challenge.
   c. Initiates a 3DS authentication.
3. The 3DS Server sends the AReq message.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Server proceeds with the challenge (opens an iframe for a Browser flow or provides the relevant data to the 3DS SDK for an App flow).
6. The ACS proceeds with the challenge and provides the prompt for the Device Binding option.
7. The Cardholder completes the challenge and accepts the Device Binding option.
8. The ACS stores the Device Binding information for this Cardholder/Account, provides the outcome of the authentication in the RReq message, and optionally the Device Binding Status using the Device Binding Status and the Device Binding Status Source to the 3DS Server/3DS Requestor.

In a subsequent transaction with the same Cardholder and Merchant:

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor/3DS Server prepares the AReq message by:
   a. Checking the Device Binding Status of the Cardholder, and/or
   b. Providing the Device Binding Status and Device Binding Status Source (if known).
3. The 3DS Server sends the AReq message.
4. The ACS uses the Device Binding Status information as part of transaction risk assessment.
5. The ACS returns an ARes message.



Note: Step 6. CReq/CRes: refer to Device Binding templates for the user interface.

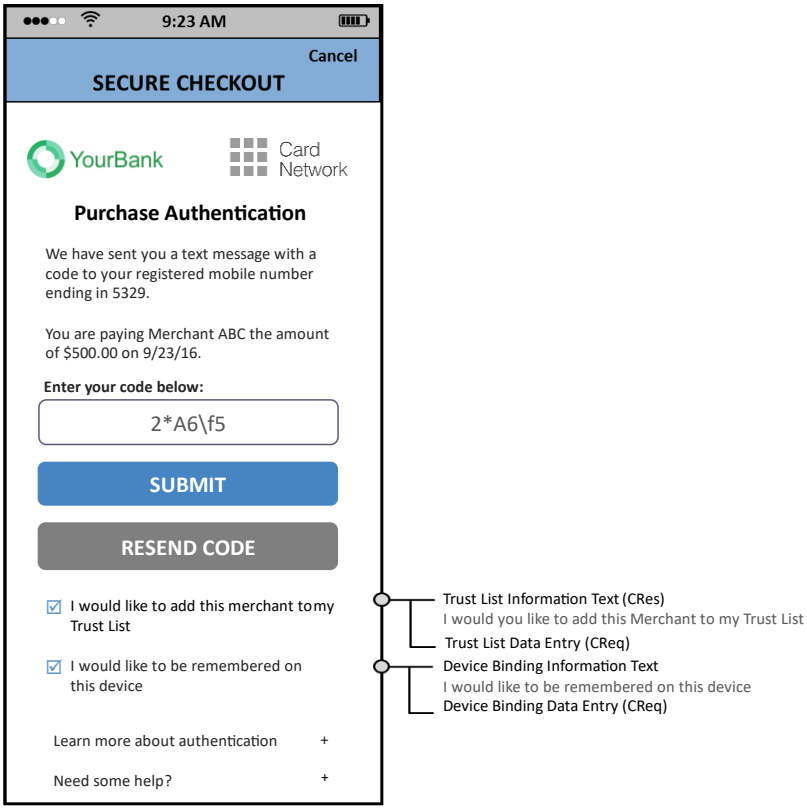
3DS Data Elements Related to Device Binding

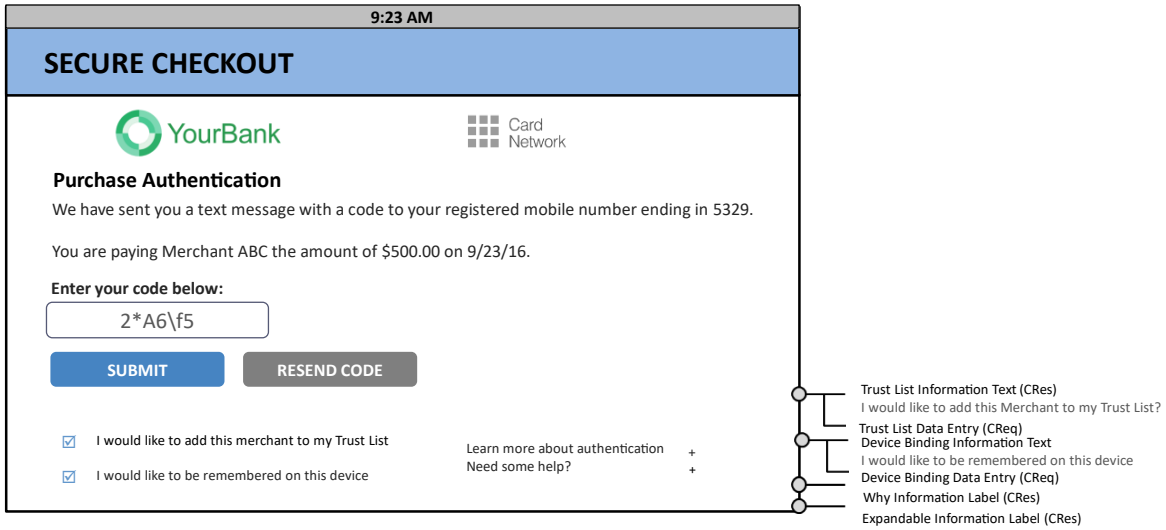
Table 2.2: 3DS Data Elements Related to Device Binding

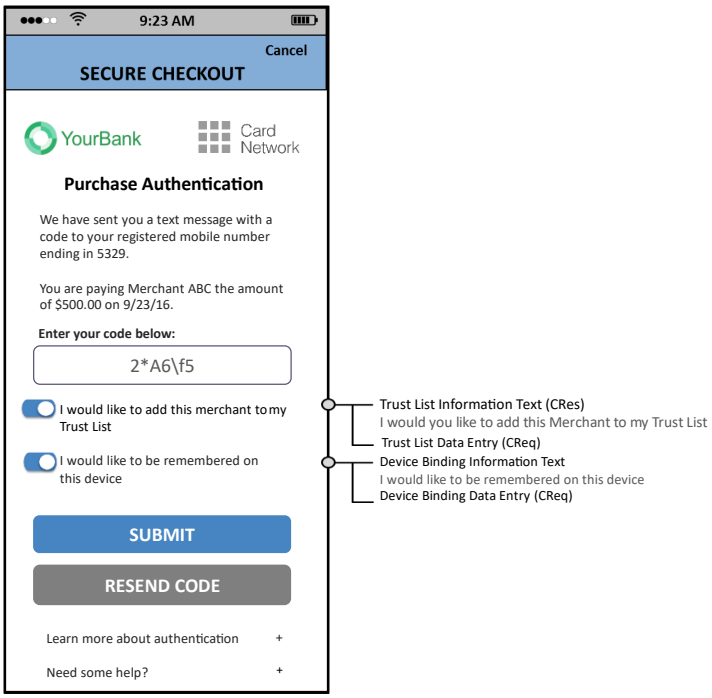
Data Element	Description	Version
3DS Requestor Challenge Indicator	Indicates whether a challenge is requested for this transaction.	2.3.1
3RI Indicator	Indicates the type of 3RI request. This data element provides additional information to the ACS to determine the best approach for handling a 3RI request. A value of 10 indicates a Trust List Status check.	2.3.1
ACS Information Indicator	Provides additional information for a particular Protocol Version to the 3DS Server. The element lists all applicable values for the card range.	2.3.1

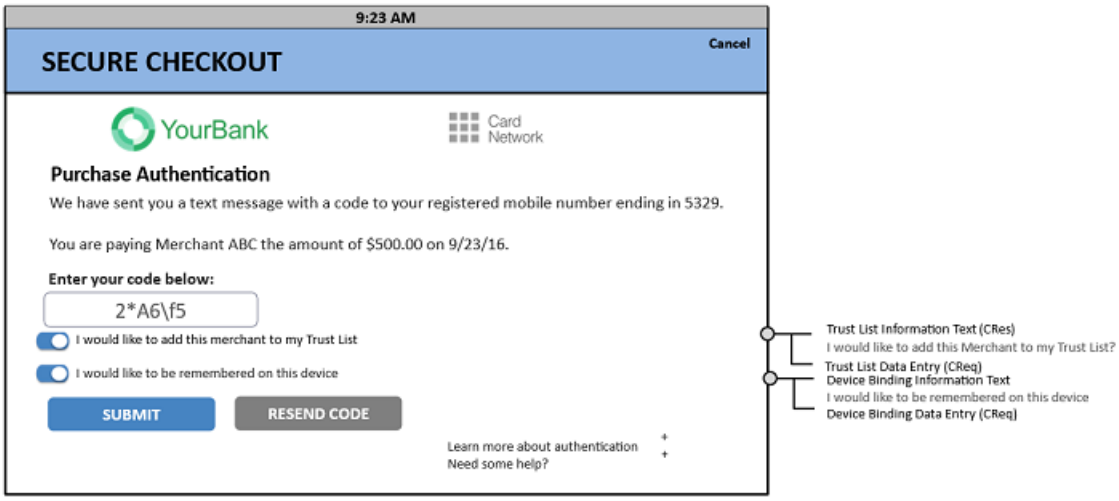
Data Element	Description	Version
Card Range Data	Card range data from the DS indicating the most recent Protocol Versions supported by the ACS, and, optionally, the DS that hosts that range, and, if configured, the ACS URL for the 3DS Method. Additionally, it identifies the 3DS features supported by the ACS, such as Trust List or Decoupled Authentication. The Device Binding indicator is defined in the ACS Information Indicator: - 05 = Device Binding Supported	2.3.1
Device Binding Data Entry	Indicator provided by the 3DS SDK to the ACS to confirm whether the Cardholder gives consent to bind the device.	2.3.1
Device Binding Information Text	Text provided by the ACS to the Cardholder during the Device Binding process.	2.3.1
Device Binding Status	Enables the communication of Device Binding Status between the ACS, the DS and the 3DS Requestor. For bound devices (value = 11–14), Device Binding Status also conveys the type of binding that was performed.	2.3.1
Device Binding Status Source	This data element will be populated by the system setting Device Binding Status.	2.3.1
Toggle Position Indicator	Indicates if the Trust List and/or Device Binding prompt should be presented below or above the action buttons.	2.3.1

User Interface Related to Device Binding









Note: Checkbox, radio button or any relevant user interface may be used to offer the Trust List and Device Binding options.

2.2.5 Alternative Use Case – Device Binding Managed by the 3DS Server/3DS Requestor

Preconditions

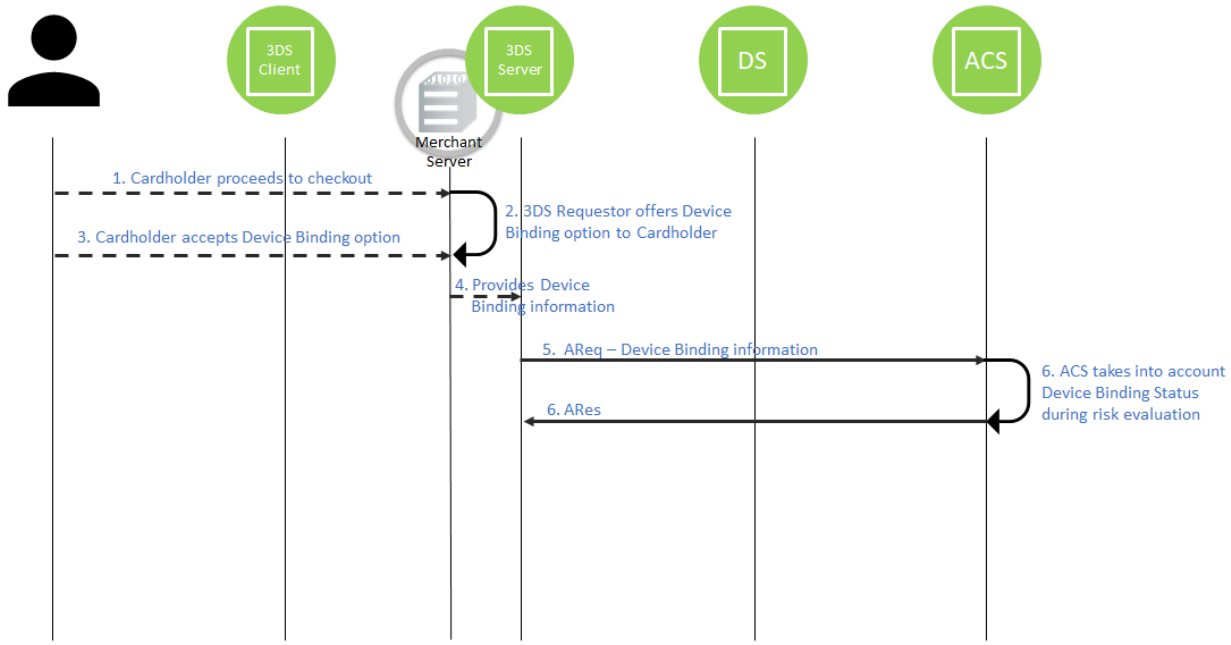
The 3DS Server (and/or 3DS Requestor) has a Device Binding management system.

The 3DS Server (and/or 3DS Requestor) is able to identify the Device used by the Cardholder.

Sequence Diagram

The Cardholder accepts the Device Binding option that is managed by the 3DS Server/3DS Requestor.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor offers the Cardholder the option to link their Cardholder Account Number with the Device used for this transaction during the checkout process.
3. The Cardholder accepts the Device Binding option.
4. The 3DS Requestor provides the transaction information to the 3DS Server with the Device Binding information.
5. The 3DS Server sends an AReq message and the Device Binding information, using the Device Binding Status and Device Binding Status Source.
6. The ACS uses the Device Binding Status information as part of transaction risk assessment.
7. The ACS returns an ARes message.



2.2.6 Alternative Use Case – Device Binding Managed by the DS

Preconditions

The DS has a Device Binding management system, and is able to identify the Consumer Device.

Note: How the DS identifies the Consumer Device is outside the scope of the 3DS Specification.

The DS and ACS have an agreement for the management of the Device Binding information.

The ACS is able to display the Device Binding prompt/screen to the Cardholder during the 3DS challenge.

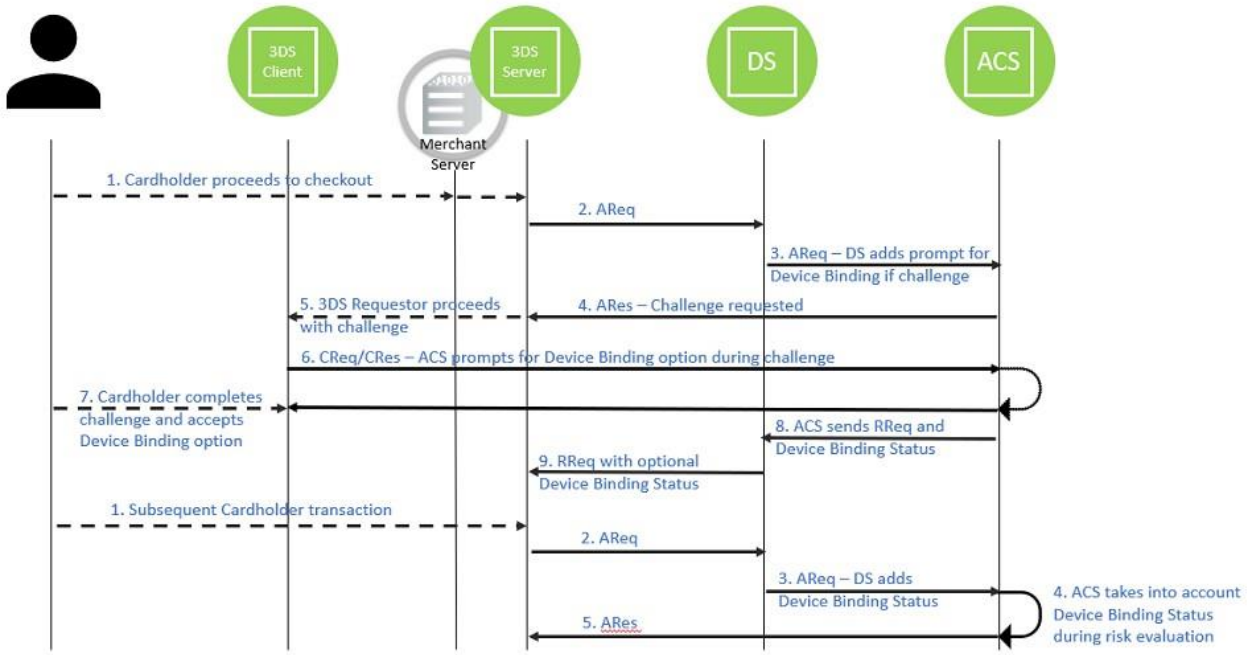
Sequence Diagram

The Cardholder accepts the Device Binding option that is managed by the DS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Server sends an AReq message.
3. The DS receives the AReq message, sets the 3DS Requestor Challenge Indicator to 12 (= Challenge requested – Device Binding prompt requested if challenge required) to indicate to the ACS that it should prompt for Device Binding during the challenge, and sends the AReq message to the ACS.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Server proceeds with the challenge (opens an iframe for a Browser flow or provides the relevant data to the 3DS SDK for an App flow).
6. The ACS proceeds with the challenge and provides the prompt for the Device Binding option.
7. The Cardholder accepts the Device Binding option and completes the challenge.
8. The ACS provides the Device Binding information for this Cardholder/Account, the outcome of the authentication in the RReq message to the DS.
9. The DS optionally provides the Device Binding status in the RReq message to the 3DS Server.

In a subsequent transaction with the same Cardholder and Merchant:

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor/3DS Server prepares the AReq message and sends it to the DS.
3. The DS updates the AReq message with the Device Binding Status and Device Binding Status Source.
4. The ACS uses the Device Binding Status information as part of transaction risk assessment.
5. The ACS returns an ARes message.



3 Out-of-Band (OOB) Authentication

3.1 Business Overview

Out-of-band (OOB) authentication adds an extra layer of security to the authentication process by requiring the Cardholder to authenticate with their bank through a separate channel. The use of a different channel makes the authentication process more resistant to attacks such as man-in-the-middle attacks, where an attacker intercepts and modifies the communication between the Cardholder and the authentication server.

In the context of 3DS, OOB authentication can be used to verify the identity of the Cardholder during a transaction. For example, the Cardholder initiates a payment, and the Issuer decides that a challenge is needed to confirm the transaction. Instead of conducting the challenge in the Merchant environment (App or Browser), the Issuer instructs the Cardholder to use a separate authentication app to verify their identity using an OOB channel. In the authentication app, the Issuer can request to the Cardholder any preferred authentication process. Issuers typically use their banking website or mobile banking apps that they fully control and trust. Once the Cardholder has been authenticated using the OOB channel, the Issuer can notify the Merchant that the authentication was successful.

Overall, the use of OOB authentication in 3DS can help reduce the risk of fraud and improve the security of online transactions, providing greater protection for both Cardholders and Merchants.

OOB authentication is an effective authentication mechanism that involves two signals from two separate channels. This method is used to block fraudulent users who have access to only one of the channels. OOB authentication is known to be effective in preventing fraudulent attacks, especially in e-commerce. The key benefit of 3DS OOB authentication is that it gives the Issuer full control over the selection of Cardholder authentication methods, which include biometric authentication, tokens, and one-time password via SMS or email. OOB authentication is an ideal choice to protect Cardholders while enabling Issuers to customise services according to their preferences.

The 3DS Specification supports OOB authentication for both Browser- and App-based transactions by providing a specific user interface template, and automation of the transition from the Merchant app to the OOB App in the context of mobile devices. Another key benefit is the ability to leverage consistent authentication methods across 3DS and other channels, e.g., online banking.

3.2 OOB – Introduction

OOB authentication is a challenge activity that is completed outside of, but in parallel to, the 3DS flow. OOB authentication methods or implementations are not in scope of the 3DS Specification.

Benefits by actor

- Merchant
  - Cardholder is used to the authentication process defined by the ACS, so there is less abandonment or failure
  - Automated App-to-App transfer between merchant and OOB apps when on the same device (App flow in 3DS version 2.3)
- Issuer
  - Consistent authentication methods for cardholders
  - Simpler customer education and support
- Cardholder

  Similar user experience across all Merchants

Use Case Overview

During a challenge, the ACS directs the Cardholder to use a specific channel and application to authenticate the transaction, instead of using the 3DS challenge window to authenticate the Cardholder. For example, the Issuer requests the use of the mobile banking app to authenticate and validate the transaction.

The OOB flow depends on:

- the 3DS Specification version;
- the channel used by the Cardholder for the transaction and the channel used by the ACS for the authentication;
- whether the OOB Authentication App is on the same device as the transaction – for an App-based transaction;
- whether the transition from the 3DS Requestor checkout page to the OOB Authentication App, and the return, is manual or automated.

Table 3.1 below shows all the possible options and indicates whether automation of the transition between the merchant app and the OOB Authentication App is possible.

Table 3.1: OOB Authentication per Channel and Automation

Merchant Channel	OOB App Channel	Same Device	OOB App Transition Automation
Browser	Browser	Yes	No
Browser	App	Yes	No
App	Browser	Yes	No
App	App	Yes	2.2, 2.2 + Bridging Message Extension and 2.3.1
App/Browser	App/Browser	No	No

Note: This table assumes an implementation fully compliant with the 3DS Specification – in particular, the setting of the iframe for the challenge in the Browser flow, and the use of Universal App Link for the App flow.

3.3 OOB Flow for Browser Channel

For a Browser-based transaction and all versions of the 3DS Specification, during the challenge, the ACS instructs the Cardholder to manually switch from the payment/checkout page to the OOB Authentication App. The OOB Authentication App may be accessible using a Browser or an app on the same or different device. When the Cardholder has completed the authentication, the Cardholder returns to the challenge window in the payment/checkout page and must select the completion button.

Note: Unlike in the App-based flow, in the Browser-based flow it is not possible to automate the switch between the Browser – 3DS Requestor page and the OOB Authentication App.

Preconditions

The ACS has defined, deployed, and communicated an OOB authentication process to the Cardholder.

The Issuer has a pre-established authentication process with the Cardholder using the OOB Authentication App, available as a web service or a mobile app, and accessed on any device or a specific device at the ACS's preference.

Assumptions

The 3DS Requestor Website and the OOB Authentication App do not need to be on the same device.

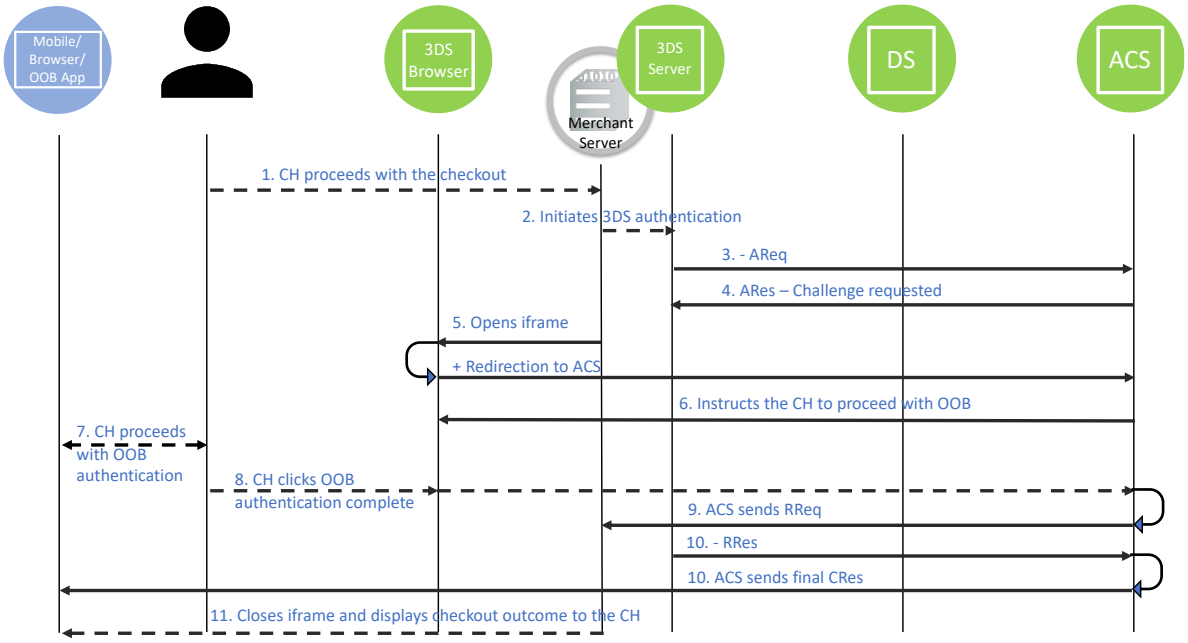
Sequence Diagram

The Cardholder authenticates the transaction using an OOB Authentication App provided by the ACS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor initiates a 3DS authentication.
3. The 3DS Server sends an AReq message.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Requestor proceeds with the challenge, opens an iframe in its checkout page and makes the redirection to the ACS.
6. The ACS provides the UI in the iframe and instructs the Cardholder to proceed with an OOB authentication.
7. The Cardholder switches to the OOB App, which may be available on a Browser or as a mobile app, on the same or different device. The Cardholder completes the authentication with the OOB App as instructed by the ACS or authentication system provider. The OOB authentication is defined and controlled by the ACS, and thus falls outside the scope of the 3DS Specification.
8. The Cardholder manually switches to the 3DS Requestor checkout page and selects the "Complete" button.

9. The ACS sends the result of the authentication in the RReq message to the 3DS Server.
10. After receiving the RRes message from the 3DS Server, the ACS sends a Final Challenge Response (CRes) message through the iframe to the 3DS Requestor to indicate the end of the challenge and the outcome of the authentication.
11. The 3DS Requestor closes the iframe and updates the UI according to the outcome of the authentication and/or authorisation.

Note: In Step 9, the ACS may continue the challenge if the OOB authentication was not performed or if it failed, before sending the Final CRes message.



Note: Automation (URLs to and from the OOB Authentication App) of the OOB flow in the Browser channel is not possible.

3.3.1 Browser Channel – Alternative OOB Flow

In this alternative OOB flow, the ACS directly accesses the result of the OOB authentication and sends the RReq and Final CRes messages before the Cardholder manually switches back to the 3DS Requestor checkout page and selects the “Complete” button.

Note: This flow is recommended as the Cardholder does not need to click the “Complete” button for the challenge to complete.

Preconditions

The ACS has defined, deployed, and communicated an OOB authentication process to the Cardholder. The OOB Authentication App may be available as a web service or as a mobile app, and may be accessed on any device, or on a specific device at the ACS’s preference.

The ACS receives or knows the result of the OOB authentication (pass or fail) before the Cardholder confirms completion (selects the “Complete” button) and does not perform additional challenges after the OOB authentication.

Benefits

The main benefits are as follows:

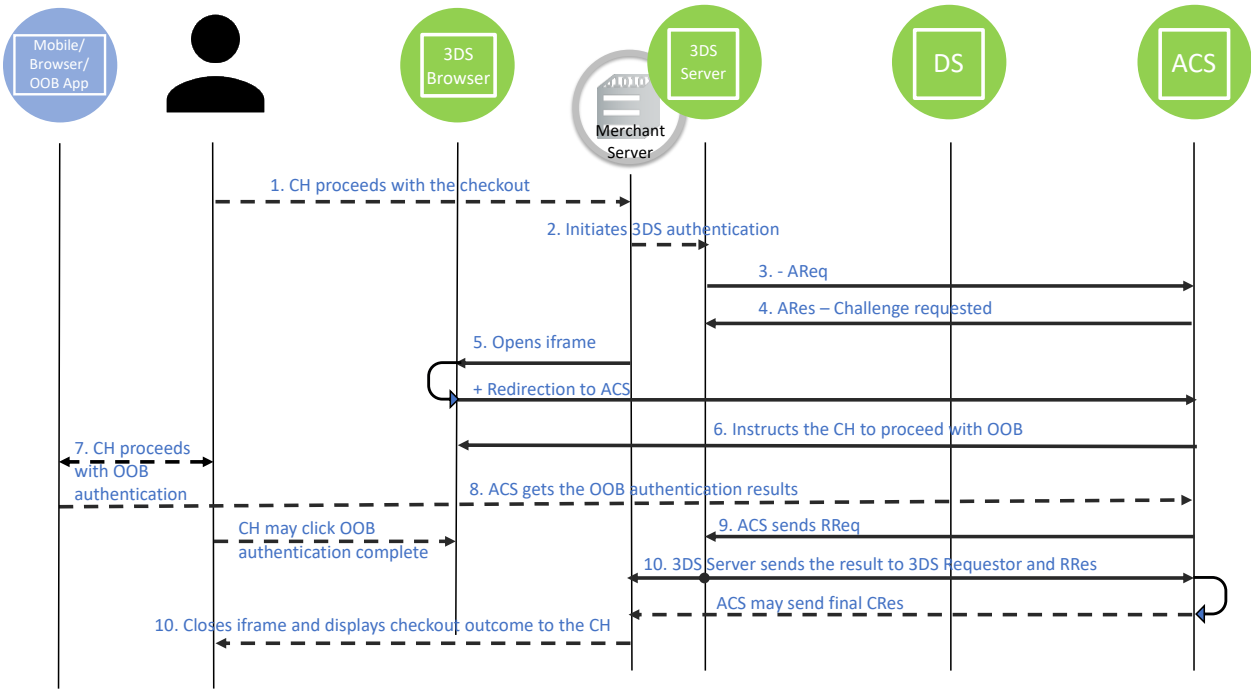
- The 3DS Requestor receives the completion information from the ACS, and can close the iframe and update the UI according to the outcome of the authentication and/or authorisation, without the Cardholder having to click the “Complete” button in the iframe.
- If the iframe is still open, the Cardholder may select the “Complete” button – this does not impact the outcome of the transaction.
- This alternative flow prevents the Authentication from failing after the 10-minute timeout due to lack of Cardholder interaction.

Sequence Diagram

The Cardholder authenticates the transaction using an OOB Authentication App provided by the ACS.

1. The Cardholder makes a purchase and proceeds to checkout.
2. The 3DS Requestor initiates a 3DS authentication.
3. The 3DS Server sends an AReq message.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Requestor proceeds with the challenge, opens an iframe in its checkout page and makes the redirection to the ACS.
6. The ACS provides the UI in the iframe and instructs the Cardholder to proceed with an OOB authentication.
7. The Cardholder switches to the OOB App, which may be available on a Browser or as a mobile app, on the same or different device. The Cardholder completes the authentication with the OOB App as instructed by the ACS or authentication system provider. The OOB authentication is defined and controlled by the ACS, and thus falls outside the scope of the 3DS Specification.
8. The ACS receives the result of the OOB authentication and does not need to wait for the authentication completion information from the Cardholder (“Complete” button).
9. The ACS sends the results of the authentication in the RReq message through the DS to the 3DS Server.
10. The 3DS Server provides the authentication result to the 3DS Requestor and sends the RRes message to the ACS. The 3DS Requestor closes the iframe and updates the UI according to the outcome of the authentication and/or authorisation.

Note: In parallel to Step 8 and 10, and if the iframe is still open, the Cardholder may manually switch to the 3DS Requestor checkout page and select the “Complete” button. After receiving the RRes message from the 3DS Server, the ACS may send the Final CRes message through the iframe.



3.4 OOB Flow: App Channel – Manual Switching

During the challenge, the ACS instructs the Cardholder to manually switch from the payment/checkout page to the OOB Authentication App. The OOB Authentication App may be on the same or different device. When the Cardholder has completed the authentication, the Cardholder returns to the challenge window in the payment/checkout page and must select the completion button.

This flow is applicable to all versions of the 3DS Specification.

Preconditions

The ACS has defined, deployed, and communicated an OOB authentication process to the Cardholder.

The ACS and the 3DS Requestor do not use the 3DS Requestor App URL and the OOB App URL (version 2.2 and 2.3.1).

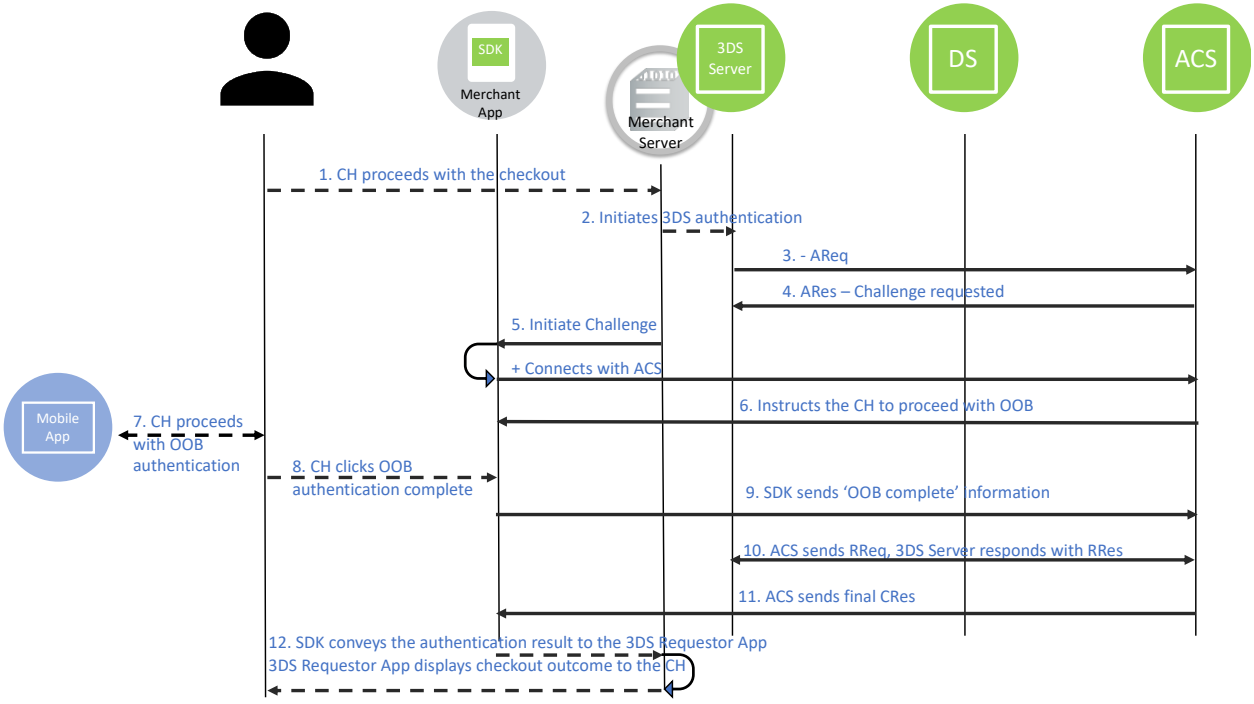
Assumptions

The 3DS Requestor App and the OOB Authentication App do not need to be on the same device.

Sequence Diagram

1. The Cardholder makes a purchase on the 3DS Requestor App and proceeds to checkout.
2. The 3DS Requestor initiates a 3DS authentication.
3. The 3DS Server sends an AReq message.
4. The ACS responds with an ARes message requesting a challenge.

5. The 3DS Requestor triggers the 3DS SDK to proceed with a challenge. The 3DS SDK connects to the ACS.
6. The ACS provides the UI to the 3DS SDK and instructs the Cardholder to proceed with the OOB authentication.
7. The Cardholder switches to the OOB App, which may be available on a Browser or as a mobile app, on the same or different device. The Cardholder completes the authentication with the OOB App as instructed by the ACS or authentication system provider. The OOB authentication is defined and controlled by the ACS, and thus falls outside the scope of the 3DS Specification.
8. The Cardholder manually switches to the 3DS Requestor App and selects the “Complete” button displayed by the 3DS SDK.
   If the OOB App and the 3DS Requestor App are on the same device, the 3DS SDK will automatically send a CReq message when the 3DS Requestor App is moved to the foreground.
9. The 3DS SDK sends the “OOB complete” information to the ACS.
10. The ACS sends the results of the authentication in an RReq message through the DS to the 3DS Server, and the 3DS Server acknowledges it by sending the RRes message.
11. The ACS sends a Final CRes message to the 3DS SDK, the 3DS SDK conveys the information to the 3DS Requestor App.
12. The 3DS Requestor App updates the UI according to the outcome of the authentication and/or authorisation.



Note: In Step 9, the ACS may continue the challenge if the OOB authentication was not performed or if it failed, before sending the Final CRes message.

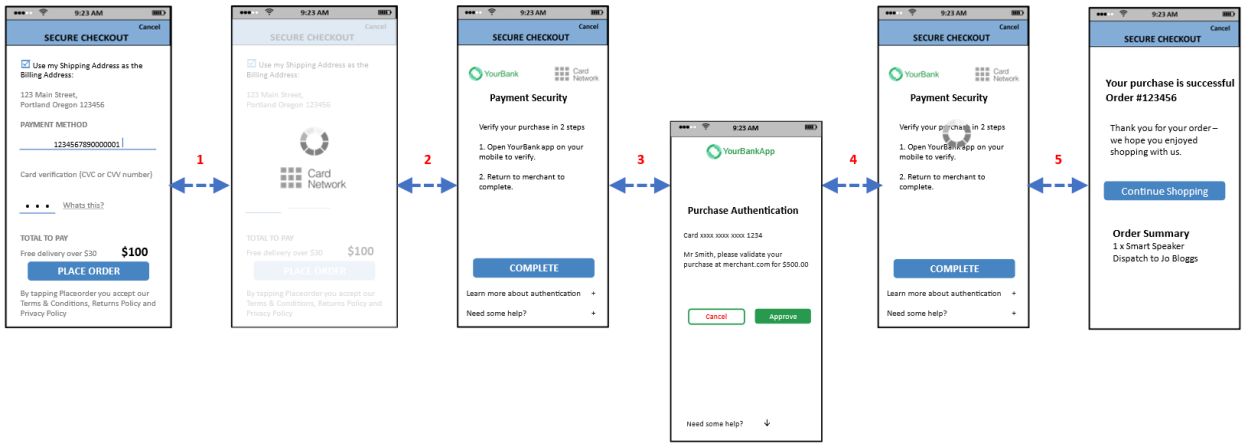
Note: If the ACS receives or knows the result of the OOB authentication (pass or fail) before the Cardholder confirms completion, it may send an RReq message before receiving the “OOB complete” information from the 3DS SDK.

User Experience

The Cardholder authenticates the transaction using an OOB Authentication App provided by the ACS.

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS’s response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.
3. The Cardholder manually switches to the OOB App.
4. When the OOB authentication is completed, the Cardholder manually switches back to the 3DS Requestor App.
5. The Cardholder selects the “Complete” button.
   If the OOB App and the 3DS Requestor App are on the same device, the 3DS SDK will automatically send a CReq message when the 3DS Requestor App is moved to the foreground, and the Cardholder will not need to select the “Complete” button.
6. The 3DS Requestor App displays the purchase completion information.

Note: After Step 4, the ACS may continue the challenge if the OOB authentication was not performed or if it failed OR send the Final CRes message as shown.



3.4.1 3DS Version 2.2 and 2.3.1 Data Elements

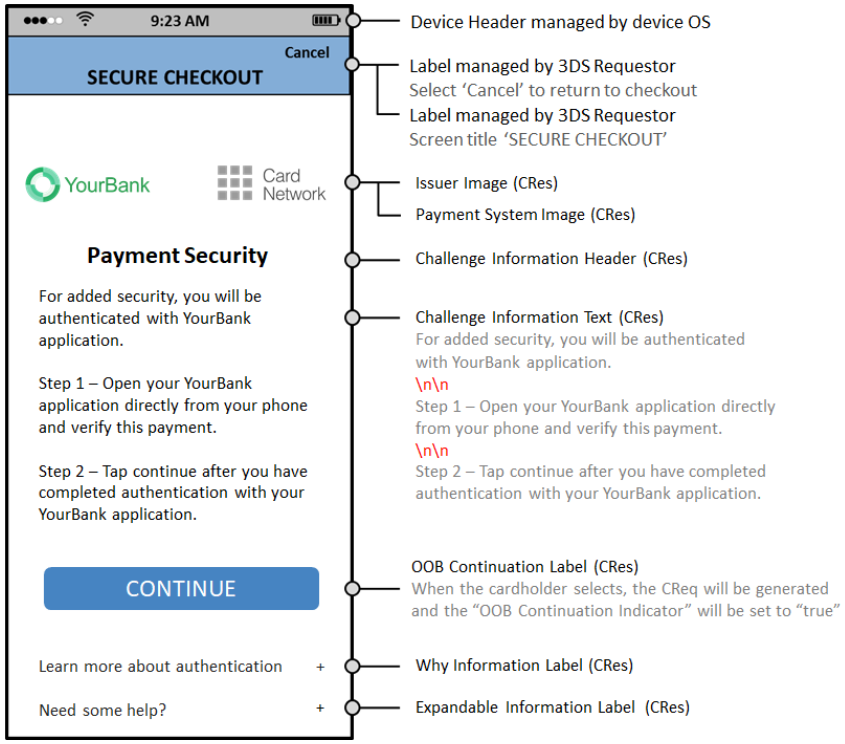
Table 3.2: 3DS Data Elements Related to OOB – Manual Switching

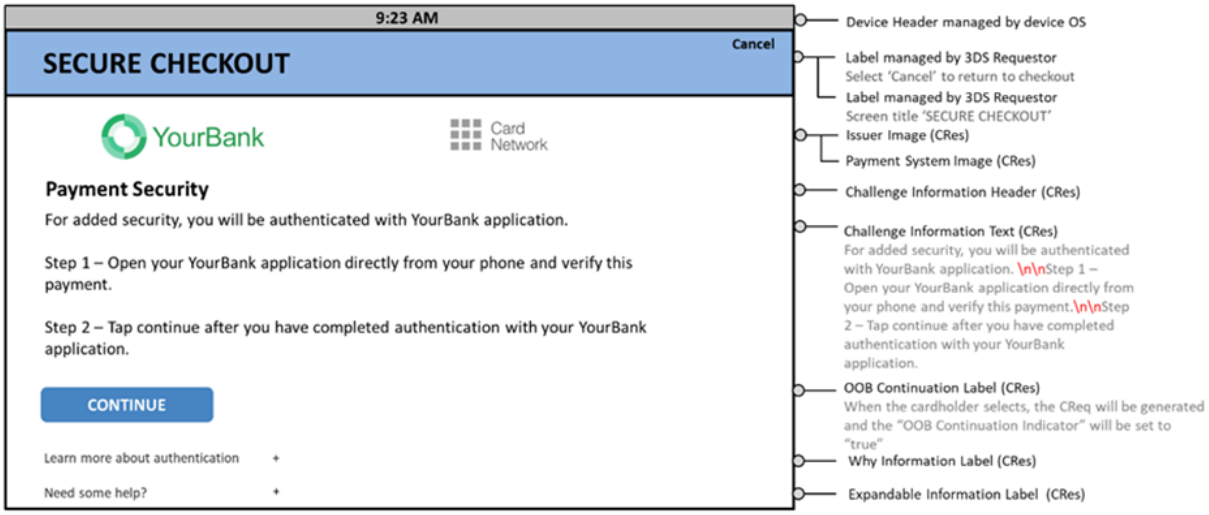
Data Element	Description	Version
ACS Interface	The interface that the challenge presents to the cardholder.	2.3.1 2.2

Data Element	Description	Version
ACS UI Template	Identifies the UI Template format that the ACS first presents to the Cardholder.	2.3.1 2.2
ACS UI Type	User interface type that the 3DS SDK will render, which includes the specific data mapping and requirements.	2.3.1 2.2
Authentication Method	Indicates the list of authentication types the Issuer will use to challenge the Cardholder, when in the ARes message or used by the ACS in the RReq message. The authentication approach that the ACS used to authenticate the Cardholder for this specific transaction.	2.3.1 2.2
Authentication Type	Indicates the type of authentication method the Issuer will use to challenge the Cardholder, whether in the ARes message or used by the ACS in the RReq message.	2.2
OOB Continuation Label	Label to be used in the UI for the button that the Cardholder selects when they have completed the OOB authentication.	2.3.1 2.2
SDK UI Type	Lists all UI types supported by the device for displaying specific challenge user interfaces within the 3DS SDK.	2.3.1 2.2

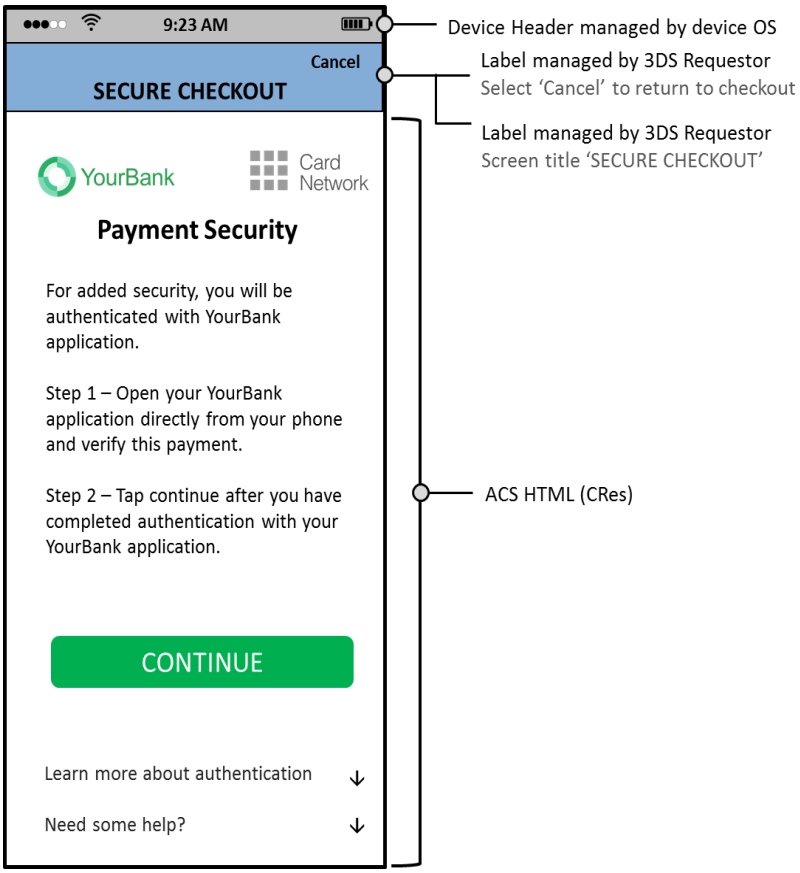
3.4.2 OOB User Interface for 3DS Version 2.2 and 2.3.1

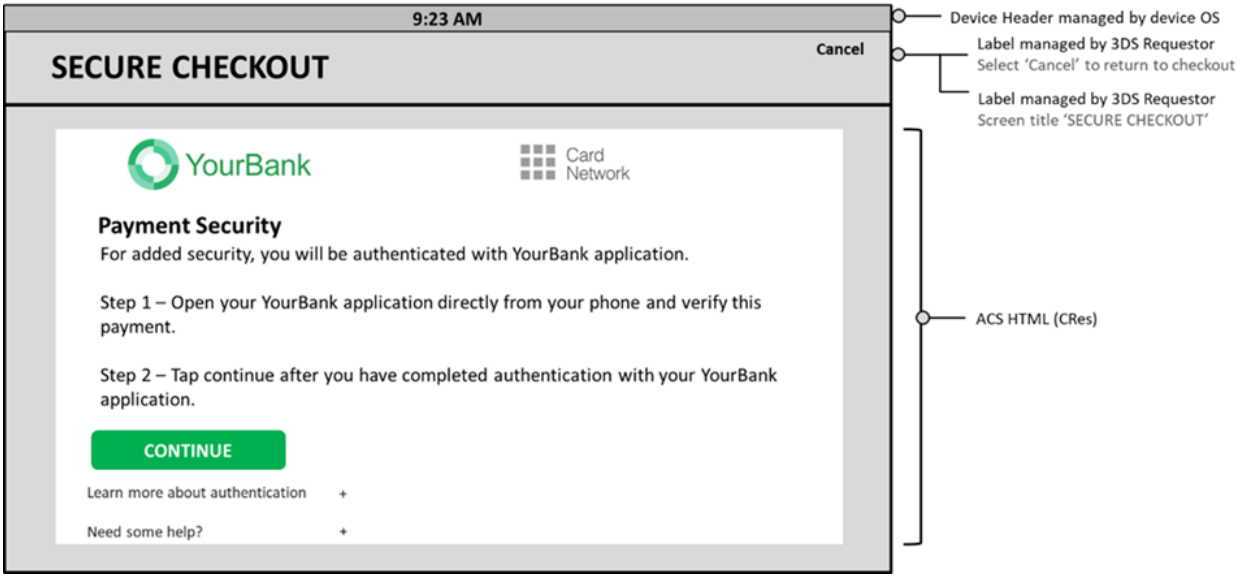
Native User Interface





HTML User Interface





3.5 OOB Flow App Channel – Automatic Switching to the 3DS Requestor App

For version 2.2 and above of the 3DS Specification, it is possible to automate the switching from the OOB Authentication App to the 3DS Requestor App.

During the challenge, the ACS instructs the Cardholder to manually switch from the payment/checkout page to the OOB Authentication App. When the Cardholder has completed the authentication, the Authentication App will automatically return to the Challenge screen on the 3DS Requestor App, assuming that the two apps are on the same device.

Preconditions

The ACS has defined, deployed, and communicated an OOB authentication process to the Cardholder.

The OOB Authentication App can handle the 3DS Requestor App URL.

The 3DS Requestor provides the 3DS Requestor App URL to the 3DS SDK.

The ACS provides the 3DS Requestor App URL to the OOB Authentication App.

The 3DS Requestor App and the OOB Authentication App are on the same device.

The 3DS Requestor App URL is a Universal App Link (refer to Table 1.3 in version 2.2 of the 3DS Specification).

Sequence Diagram

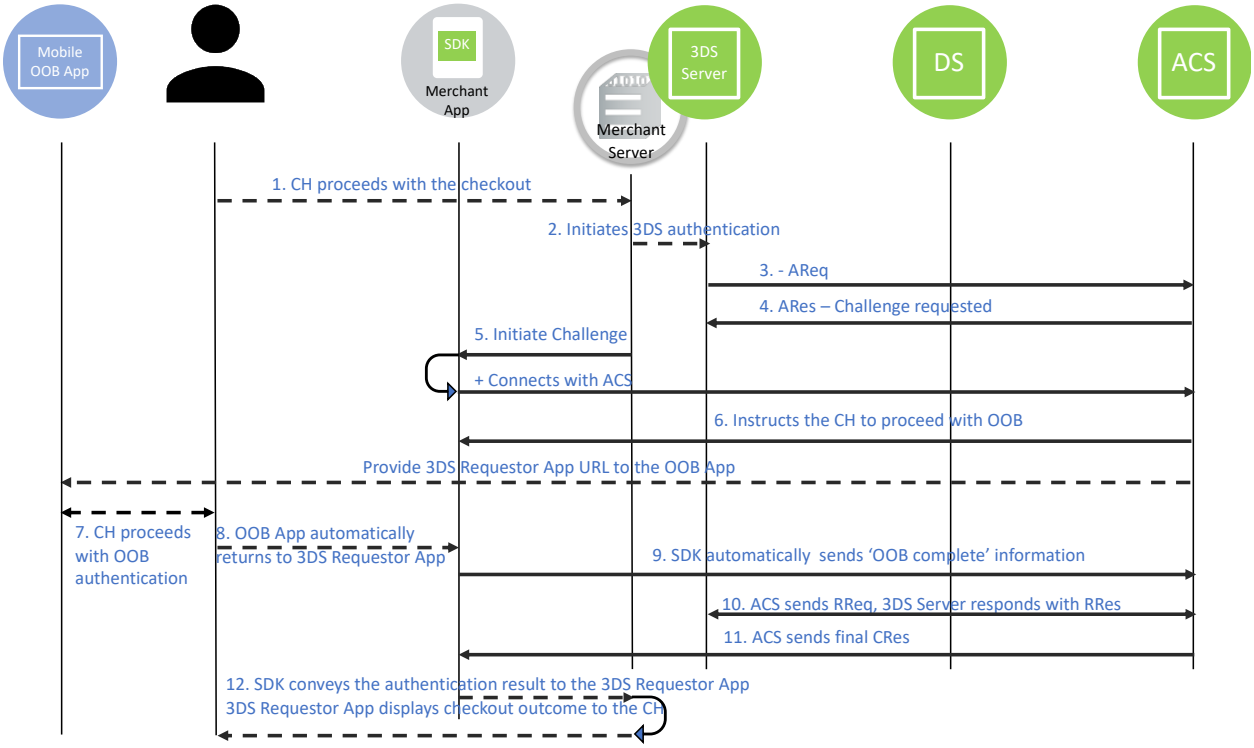
The Cardholder authenticates the transaction using an OOB Authentication App that is on the Device used for the purchase.

1. The Cardholder makes a purchase on the 3DS Requestor App and proceeds to checkout.
2. The 3DS Requestor initiates a 3DS authentication.
3. The 3DS Server sends an AReq message.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Requestor triggers the 3DS SDK to proceed with a challenge. The 3DS SDK connects to the ACS and provides the 3DS Requestor App URL to the ACS.
6. The ACS provides the UI to the 3DS SDK and instructs the Cardholder to proceed with an OOB authentication.
   The ACS conveys the 3DS Requestor App URL to the OOB Authentication App.
   Note: The ACS also displays the “Complete” button if the OOB Authentication App is on a different device.
7. The Cardholder switches to the OOB App on the same device, and completes the authentication as instructed by the ACS or authentication system provider.
   The OOB authentication is defined and controlled by the ACS, and thus falls outside the scope of the 3DS Specification.
8. The OOB Authentication App uses the 3DS Requestor App URL (Universal App Link) to automatically return the Cardholder to the 3DS Requestor App.

9. The Cardholder does not need to select the “Complete” button, the 3DS SDK detects that the 3DS Requestor App is back in the foreground and sends a Challenge Request (CReq) message to the ACS (Automatic CReq). The 3DS SDK sends the “OOB complete” information to the ACS.
10. The ACS sends the results of the authentication in an RReq message through the DS to the 3DS Server, and the 3DS Server acknowledges it by sending an RRes message.
11. The ACS sends a Final CRes message to the 3DS SDK, the 3DS SDK conveys the information to the 3DS Requestor App.
12. The 3DS Requestor App updates the UI according to the outcome of the authentication and/or authorisation.

Note: In Step 9, the ACS may continue the challenge if the OOB authentication was not performed or if it failed, before sending the Final CRes message.

Note: If the ACS receives or knows the result of the OOB authentication (pass or fail) before the Cardholder confirms completion, it may send the RReq before receiving the “OOB complete” information from the 3DS SDK.

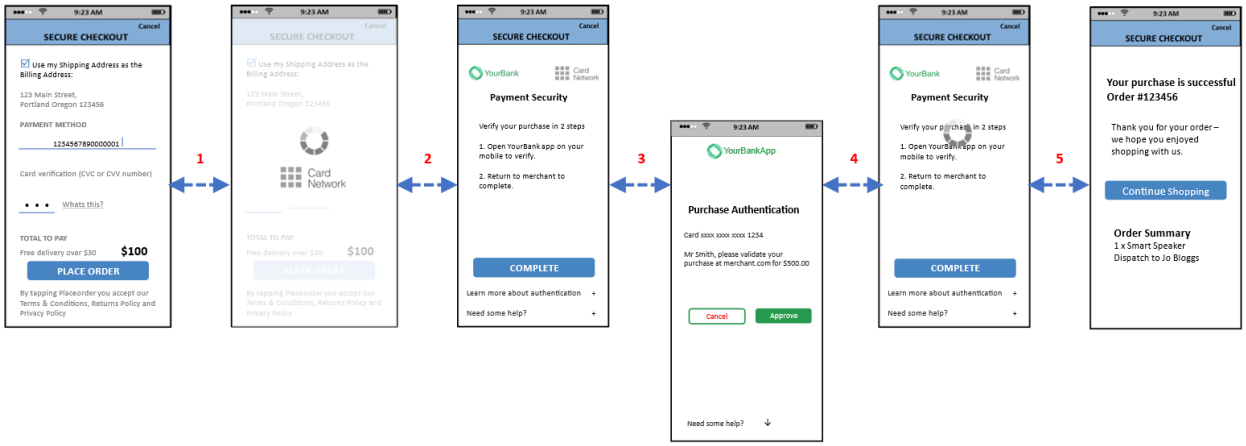


User Experience

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS’s response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.
3. The Cardholder manually switches to the OOB App.
4. When the OOB authentication is completed, the OOB App invokes the 3DS Requestor App URL, and the Cardholder is automatically taken back to the 3DS Requestor App.

5. The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information. The Cardholder does not need to select the “Complete” button.
6. The 3DS Requestor App displays the purchase completion information.

Note: After Step 4, the ACS may continue the challenge if the OOB authentication was not performed or if it failed, OR send the Final CRes message as shown.



3.5.1 Technical Variant: the Device Operating System Cannot Match the 3DS Requestor App URL to an Installed App

User Experience

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS’s response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.

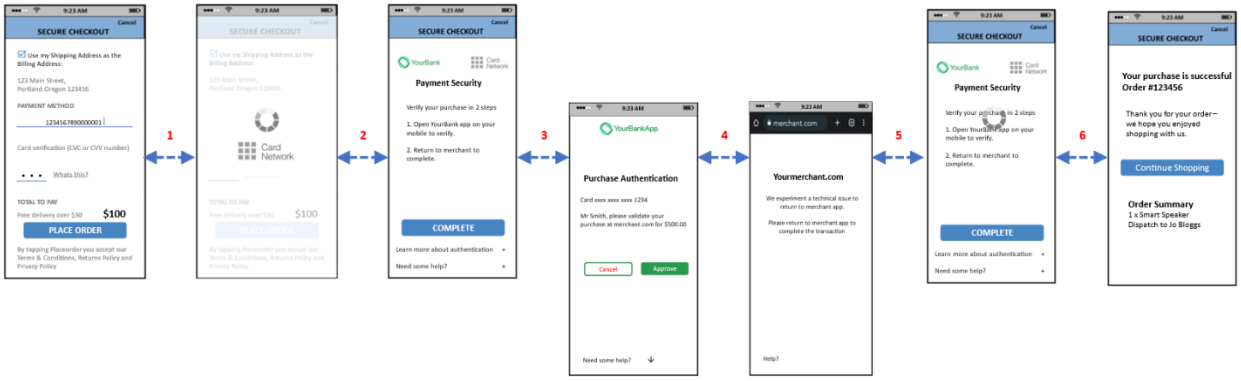
Note: The ACS also displays the “Complete” button in case the OOB Authentication App is on a different device.

3. The Cardholder manually switches to the OOB App.
4. When the OOB authentication is completed, the OOB Authentication App invokes the 3DS Requestor App URL (Universal App Link) to return to the 3DS Requestor App, but the Device Operating System cannot resolve the URL and opens the default Device Browser.

Note: The 3DS Requestor would need to provide a landing page to instruct the Cardholder to manually switch to the 3DS Requestor App.

5. The Cardholder manually switches to the 3DS Requestor App.
6. The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information to the ACS. The Cardholder does not need to select the “Complete” button.
7. The 3DS Requestor App displays the purchase completion information.

Note: After Step 4, the ACS may continue the challenge if the OOB authentication was not performed or if it failed OR send the Final CRes message as shown.



3.5.2 Technical Variant: the 3DS Requestor App URL Is Invalid or Is Based on a Custom Device Operating System

User Experience

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS's response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.

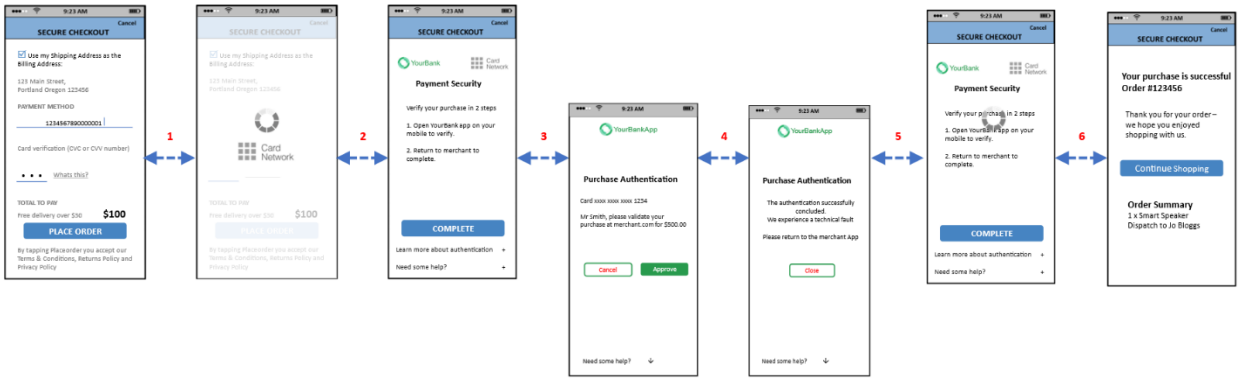
Note: The ACS also displays the "Complete" button in case the OOB authentication App is on a different device.

3. The Cardholder manually switches to the OOB App.
4. When the OOB authentication is completed, the OOB App invokes the 3DS Requestor App URL to return to the 3DS Requestor App, but the Device Operating System cannot resolve the URL and returns an error to the OOB Authentication App. The OOB Authentication App displays a page to instruct the Cardholder to manually switch to the 3DS Requestor App.

Note: The OOB Authentication App needs to interpret the error returned by the Device Operating System and be able to display the instructions to the Cardholder.

5. The Cardholder manually switches to the 3DS Requestor App.
6. The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information to the ACS. The Cardholder does not need to select the "Complete" button.
7. The 3DS Requestor App displays the purchase completion information.

Note: After Step 4, the ACS may continue the challenge if the OOB authentication was not performed or if it failed OR send the Final CRes message as shown.



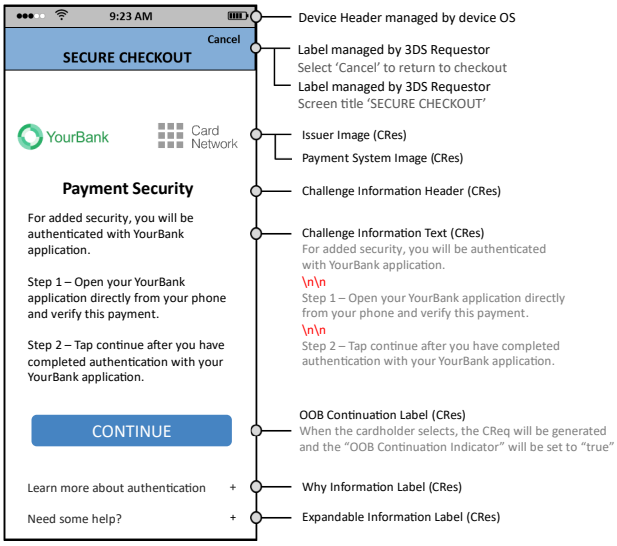
3.5.3 3DS Version 2.2 and Above Data Elements

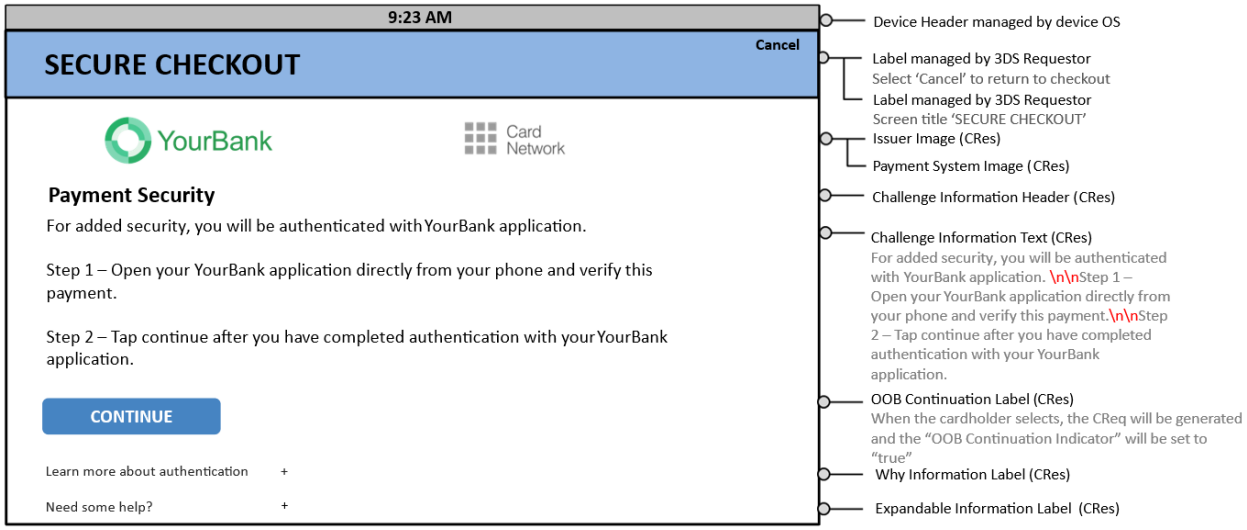
Table 3.3: 3DS Data Elements Related to OOB – Automatic Switching to the 3DS Requestor App

Data Element	Description	Version
3DS Requestor App URL	3DS Requestor App declaring its URL within the CReq message so that the Authentication App can call the 3DS Requestor App after OOB authentication has occurred. Each transaction would require a unique Transaction ID by using the SDK Transaction ID.	2.3.1 2.2
ACS UI Template	Identifies the UI Template format that the ACS first presents to the consumer.	2.3.1 2.2
ACS UI Type	User interface type that the 3DS SDK will render, which includes the specific data mapping and requirements.	2.3.1 2.2
Authentication Method	Authentication approach that the ACS used to authenticate the Cardholder for this specific transaction.	2.3.1 2.2
Authentication Type	Indicates the type of authentication method the Issuer will use to challenge the Cardholder, whether in the ARes message or what was used by the ACS when in the RReq message.	2.3.1 2.2
OOB Continuation Label	Label to be used in the UI for the button that the Cardholder selects when they have completed the OOB authentication.	2.3.1 2.2
SDK UI Type	Lists all UI types that the device supports for displaying specific challenge user interfaces within the 3DS SDK.	2.3.1 2.2

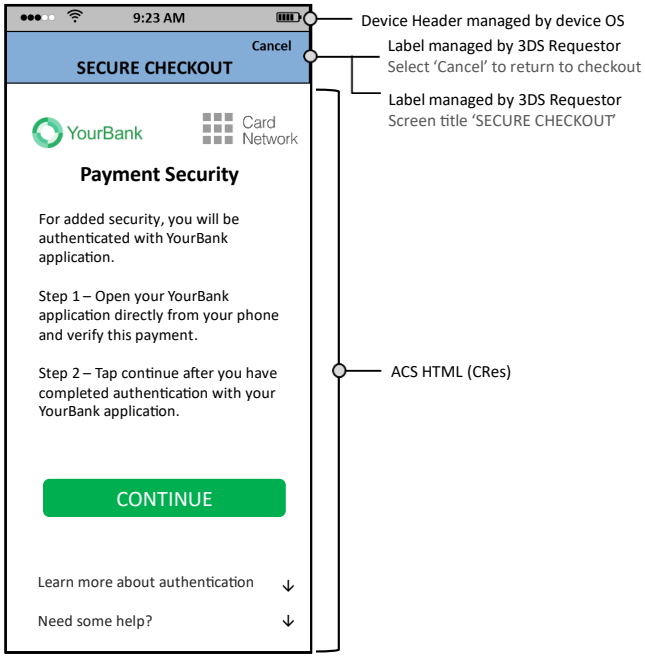
3.5.4 OOB User Interface for 3DS Version 2.2 and Above

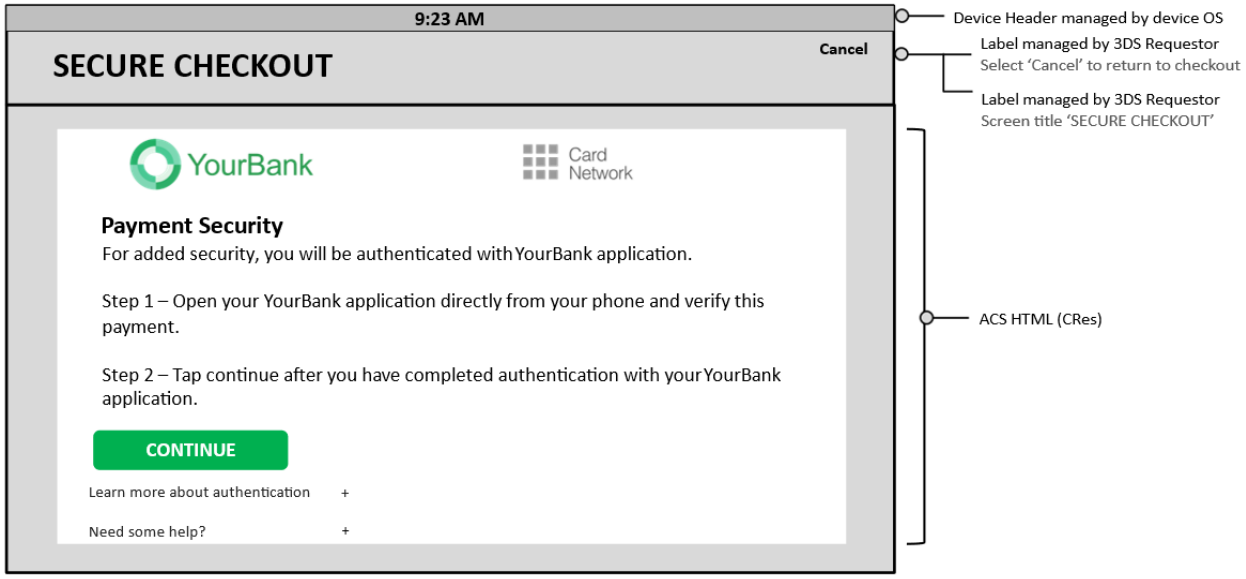
Native User Interface





HTML User Interface





3.6 OOB Flow: App Channel – Automatic Switching to the OOB App

For version 2.3.1 of the 3DS Specification, it is possible to automate the switching from the 3DS Requestor App to the OOB Authentication App. This flow is also possible with version 2.2 of the 3DS Specification if the Bridging Message Extension with the Challenge Data object is present and supported by the ACS and the 3DS SDK.

During the challenge, the ACS instructs the Cardholder to switch from the payment/checkout page to the Authentication App using the provided button on the screen. When the Cardholder has completed the authentication, the OOB Authentication App will automatically return the Cardholder to the Challenge screen on the 3DS Requestor App.

Refer to Section 3.5 for details on automatic switching from the OOB Authentication App to the 3DS Requestor App.

Preconditions

The ACS has defined, deployed, and communicated an OOB authentication process to the Cardholder.

The ACS provides the OOB App URL to the 3DS SDK.

The OOB Authentication App can handle the 3DS Requestor App URL.

The 3DS Requestor provides the 3DS Requestor App URL to the 3DS SDK.

The 3DS Requestor App and the OOB Authentication App are on the same device.

The 3DS SDK and ACS communicate via the 3DS Requestor App URL Indicator and OOB App URL Indicator that they support the URLs for automatic switching.

Sequence Diagram

The Cardholder authenticates the transaction using an OOB Authentication App that is on the Device used for the purchase. The switching between the 3DS Requestor and the OOB Authentication App is automated.

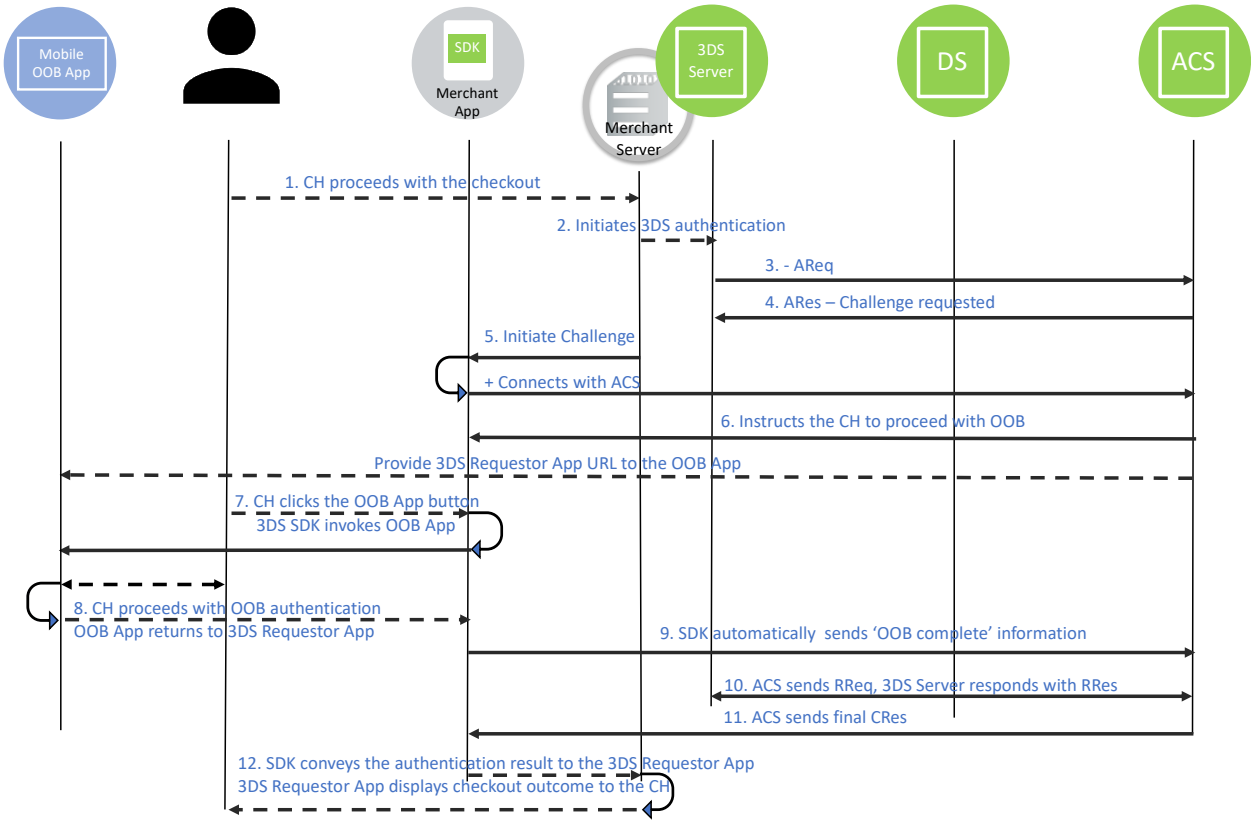
1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS's response.
2. The 3DS Requestor initiates a 3DS authentication.
3. The 3DS Server sends an AReq message.
4. The ACS responds with an ARes message requesting a challenge.
5. The 3DS Requestor triggers the 3DS SDK to proceed with a challenge. The 3DS SDK connects to the ACS.
6. The ACS provides the UI to the 3DS SDK and instructs the Cardholder to proceed with an OOB authentication. In particular, the ACS provides the OOB App URL (Universal App Link) and OOB App Label that the 3DS SDK uses to display a button to automatically switch to the OOB App.
   The ACS conveys the 3DS Requestor App URL to the OOB Authentication App.

7. The Cardholder selects the “OOB App” button, and the 3DS SDK invokes the OOB App URL that opens the OOB App. The Cardholder is automatically taken to the OOB App.
8. The Cardholder proceeds with the OOB authentication. When completed, the OOB App invokes the 3DS Requestor App URL (Universal App Link) to automatically return to the 3DS Requestor App.
9. The Cardholder does not need to select the “Complete” button, the 3DS SDK detects that the 3DS Requestor App is back in the foreground and sends a CReq message to the ACS (Automatic CReq). The 3DS SDK sends the “OOB complete” information to the ACS.
10. The ACS sends the results of the authentication in an RReq message through the DS to the 3DS Server, and the 3DS Server acknowledges it by sending an RRes message.
11. The ACS sends a Final CRes message to the 3DS SDK, the 3DS SDK conveys the information to the 3DS Requestor App.
12. The 3DS Requestor App displays the purchase completion information.

Note: After Step 9, the ACS may continue the challenge if the OOB authentication was not performed or failed, OR send the Final CRes message as shown.

Note: If the ACS receives or knows the result of the OOB authentication (pass or fail) before the Cardholder confirms completion, it may send the RReq before receiving the “OOB complete” information from the 3DS SDK.

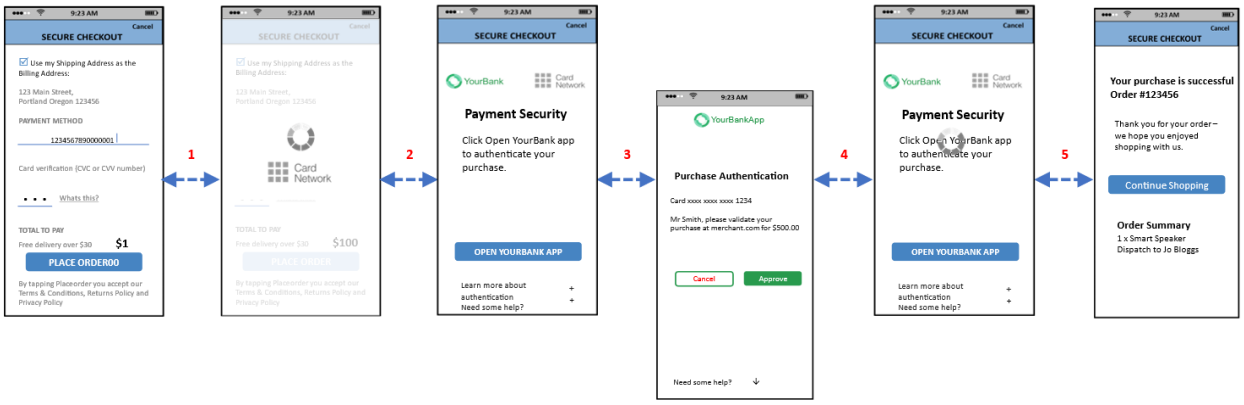
Note: It is recommended for the ACS to display the “Complete” button (refer to the OOB Continuation Label) if the OOB Authentication App is on a different device or if there is a technical issue when the 3DS Requestor App URL and OOB App URL are invoked.



User Experience

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS's response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.
3. The Cardholder selects the "Open yourbank app" button, the OOB App automatically opens and comes to the foreground.
4. When the OOB authentication is completed, the OOB App invokes the 3DS Requestor App URL, the Cardholder is automatically taken back to the 3DS Requestor App.
5. The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information.
6. The 3DS Requestor App displays the purchase completion information.

Note: After Step 4, the ACS may continue the challenge if the OOB authentication was not performed or if it failed, OR send the Final CRes message as shown.



3.6.1 Technical Variant – the Device Operating System Cannot Match the OOB App URL to an Installed App

User Experience

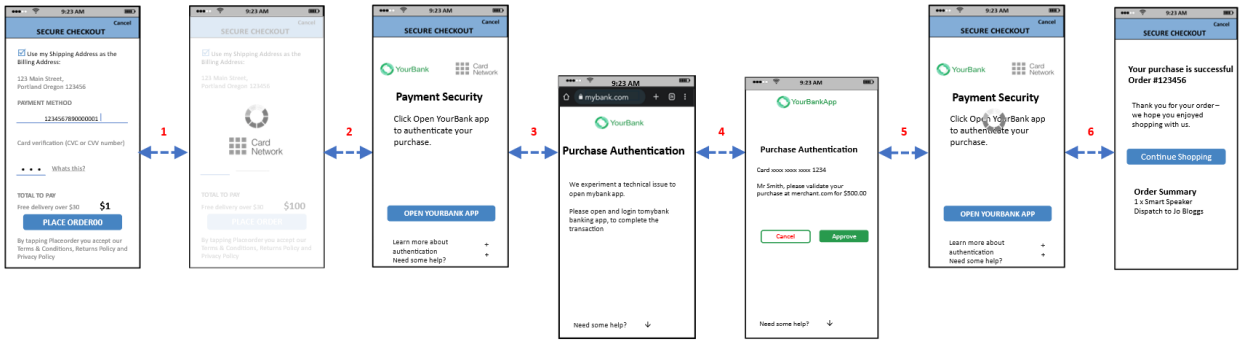
1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS's response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.
3. The Cardholder selects the "Open yourbank app" button.
   The 3DS SDK invokes the OOB App URL (Universal App Link), but the Device Operating System cannot resolve the URL and opens the default Device Browser.

Note: The ACS would need to provide a landing page to instruct the Cardholder to manually switch to the OOB Authentication App.

4. The Cardholder manually switches to the OOB App.
5. When the OOB authentication is completed, the OOB App invokes the 3DS Requestor App URL, the Cardholder is automatically taken back to the 3DS Requestor App.

6. The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information.
7. The 3DS Requestor App displays the purchase completion information.

Note: The ACS may also display the “Complete” button if the OOB Authentication App is on a different device.



3.6.2 Technical Variant – the OOB App URL Is Invalid or Is Based on a Custom Device Operating System

User Experience

1. The Cardholder makes a purchase and proceeds to checkout. The 3DS Requestor App displays the processing screen while waiting for the ACS’s response.
2. The 3DS SDK displays the UI provided by the ACS to proceed with an OOB authentication.
3. The Cardholder selects the “Open yourbank app” button.
   The 3DS SDK invokes the OOB App URL (Universal App Link), but the Device Operating System cannot resolve the URL and returns an error to the 3DS SDK. The 3DS SDK indicates the error to the ACS in a CReq message using OOB App Status (01) and OOB Continuation Indicator (02). The ACS provides a new UI with instructions to the Cardholder to manually switch to the OOB Authentication App.

Note: This error scenario also occurs if the OOB Authentication App is on a different device.

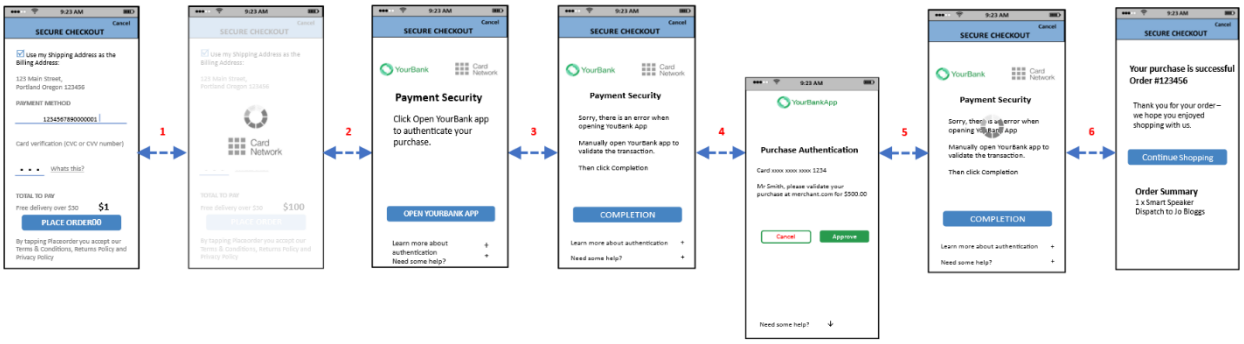
Note: The 3DS SDK needs to interpret the error returned by the Device Operating System in order to indicate the error to the ACS in the CReq message.

4. The Cardholder manually switches to the OOB App.
5. When the OOB authentication is completed, the OOB App invokes the 3DS Requestor App URL, the Cardholder is automatically taken back to the 3DS Requestor App.

The 3DS SDK detects that it is in the UI foreground and automatically sends the OOB complete information.

6. The 3DS Requestor App displays the purchase completion information.

Note: The ACS should display the “Complete” button if the OOB Authentication App is on a different device.



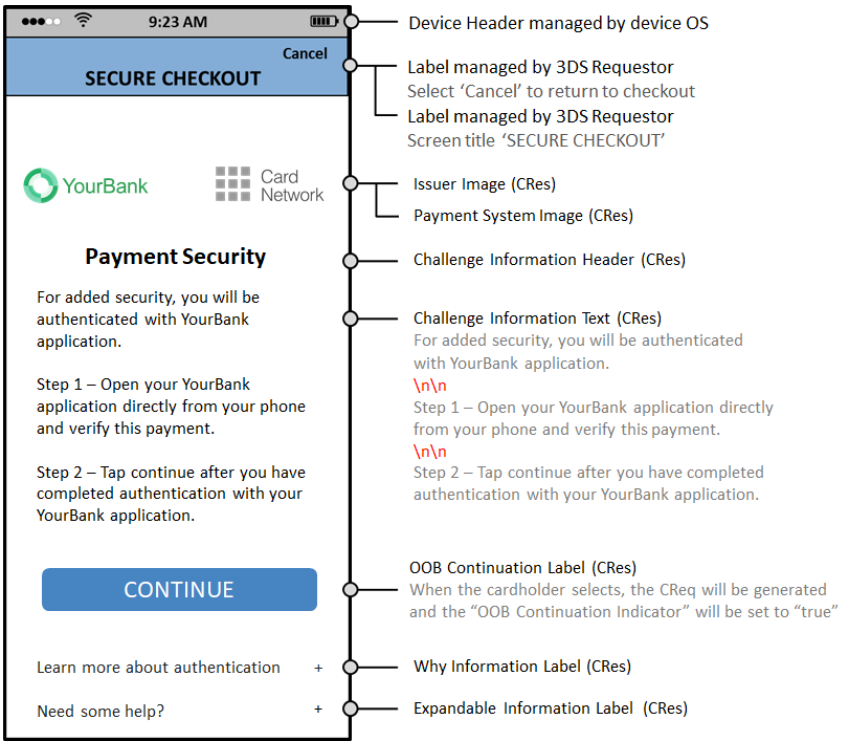
3.6.3 3DS Version 2.3.1 Data Elements

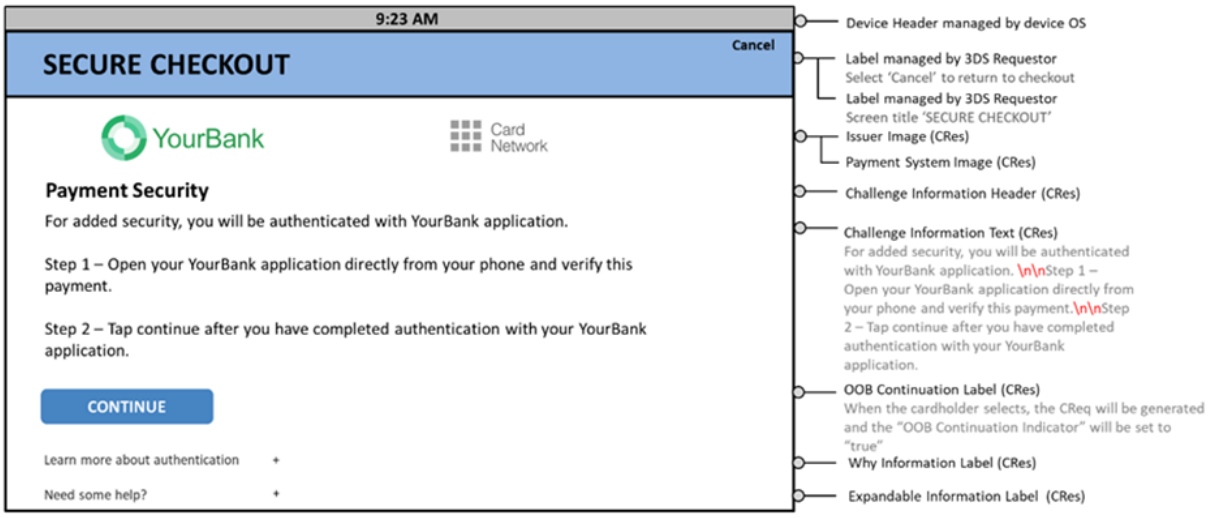
Table 3.4: 3DS Data Elements Related to OOB – Automatic Switching to and from the OOB App

Data Element	Description	Version
3DS Requestor App URL	3DS Requestor App declaring its URL within the CReq message so that the Authentication App can call the 3DS Requestor App after OOB authentication has occurred. Each transaction would require a unique Transaction ID by using the SDK Transaction ID.	2.3.1
3DS Requestor App URL Indicator	Indicates whether the OOB Authentication App used by the ACS during a challenge supports the 3DS Requestor App URL.	2.3.1 2.2 + Bridging Message Extension
ACS Interface	The ACS interface that the challenge presents to the Cardholder.	2.3.1
ACS UI Template	Identifies the UI Template format that the ACS first presents to the Cardholder.	2.3.1
ACS UI Type	User interface type that the 3DS SDK will render, which includes the specific data mapping and requirements.	2.3.1
Authentication Method	Authentication approach that the ACS used to authenticate the Cardholder for this specific transaction.	2.3.1

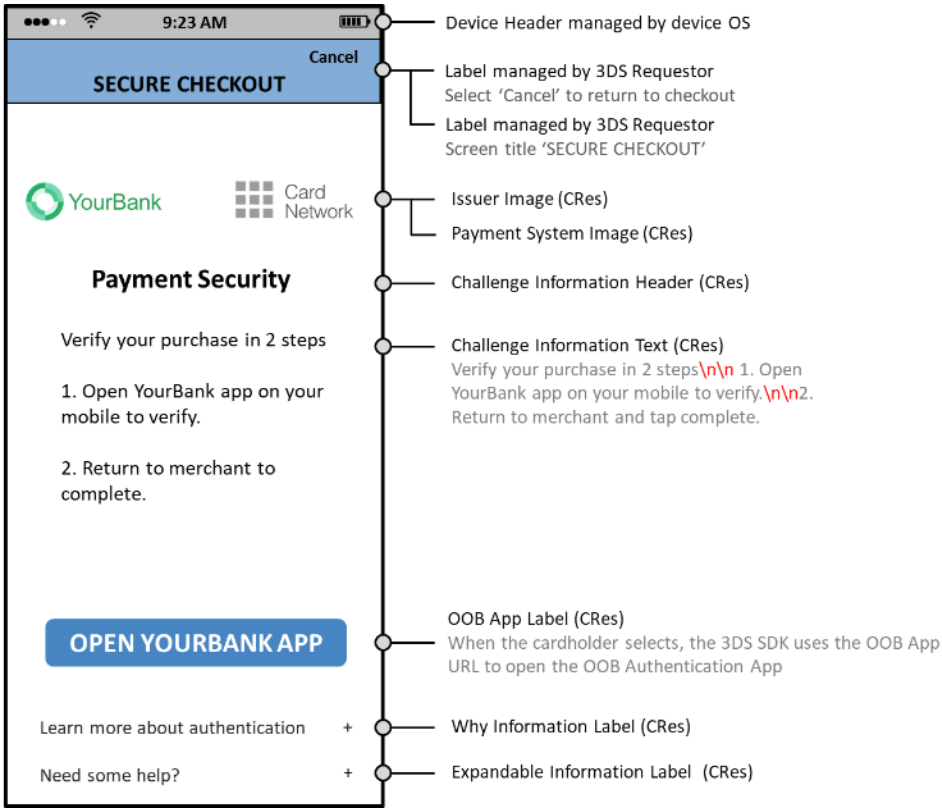
Data Element	Description	Version
OOB App Label	Label to be displayed for the link to the OOB App URL.	2.3.1 2.2 + Bridging Message Extension
OOB App Status	Status code indicating the type of problem encountered when using the OOB App URL (fail to open).	2.3.1 2.2 + Bridging Message Extension
OOB App URL	Universal App Link to an Authentication App used in the OOB authentication. The OOB App URL will open the appropriate location within the OOB Authentication App.	2.3.1 2.2 + Bridging Message Extension
OOB App URL Indicator	Indicates if the 3DS SDK supports the OOB App URL.	2.3.1 2.2 + Bridging Message Extension
OOB Continuation Indicator	Indicator notifying the ACS that the Cardholder has selected the OOB Continuation button in an OOB authentication method, or that the 3DS SDK automatically completes without any Cardholder interaction.	2.3.1 2.2 + Bridging Message Extension
OOB Continuation Label	Label to be used in the UI for the button that the Cardholder selects when they have completed the OOB authentication.	2.3.1
SDK Authentication Type	Authentication methods preferred by the 3DS SDK in order of preference.	2.3.1
SDK UI Type	Lists all UI types that the device supports for displaying specific challenge user interfaces within the 3DS SDK.	2.3.1

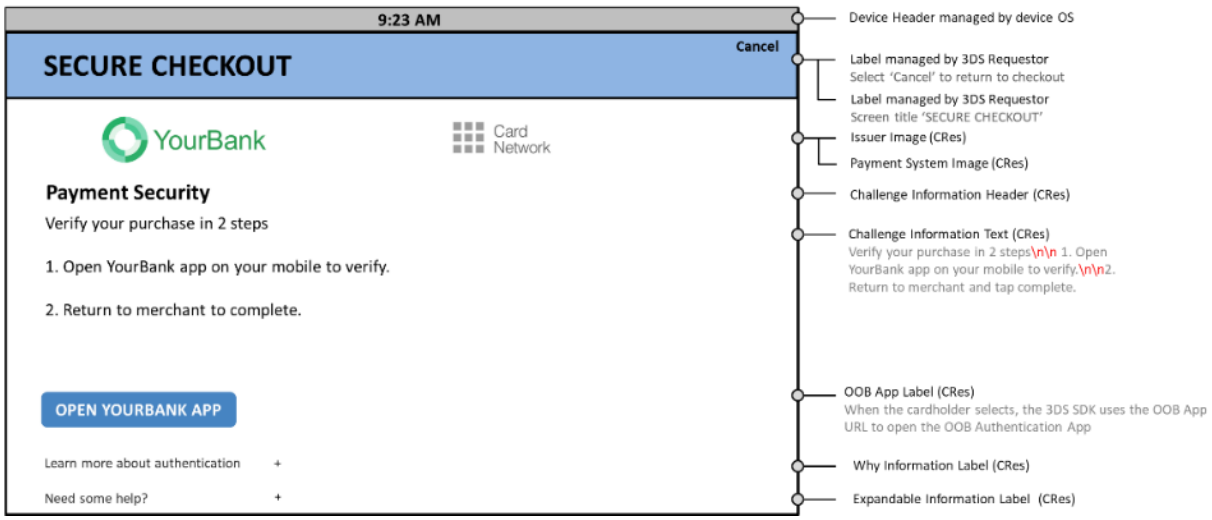
3.6.4 OOB User Interface for Version 2.3.1



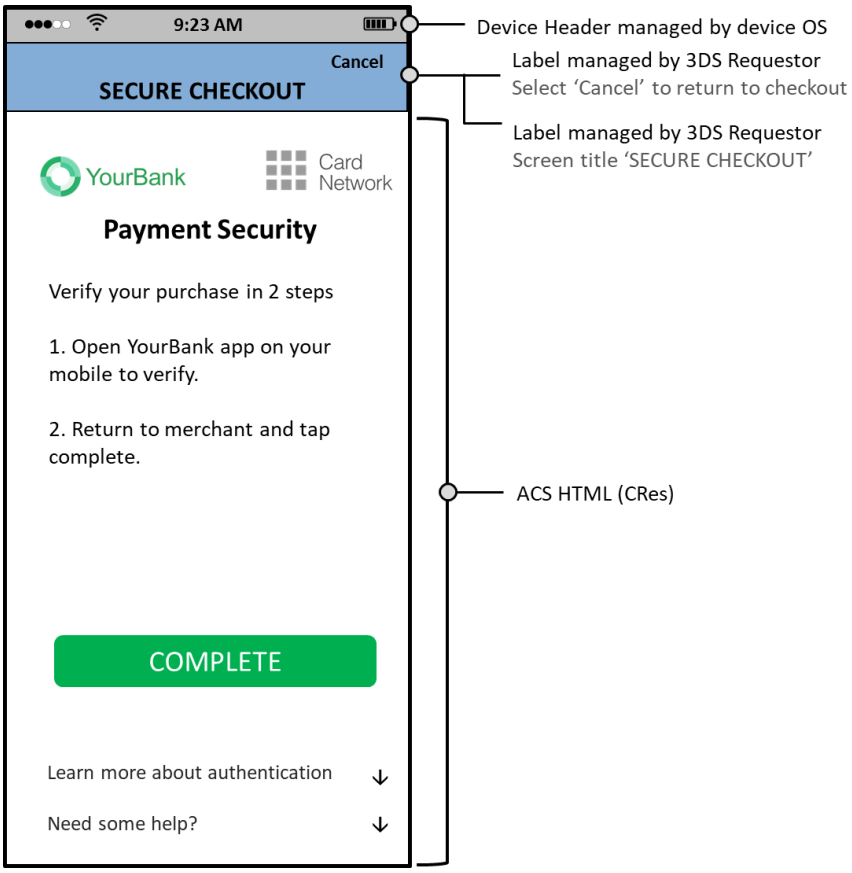


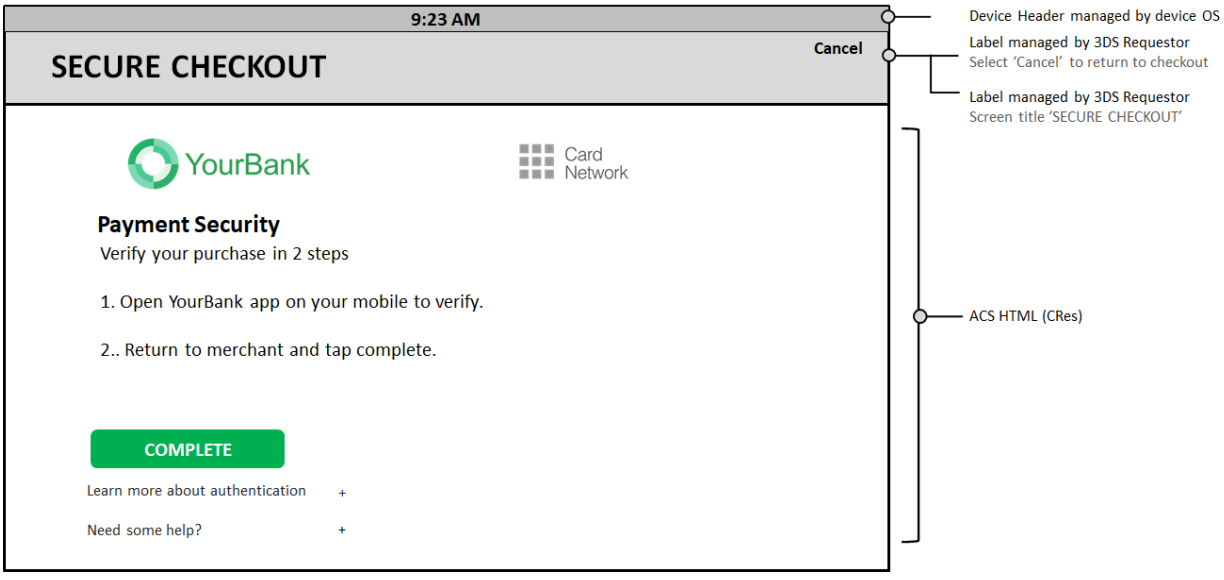
Sample OOB Native UI Template with Automatic OOB App URL Link—Portrait + Landscape



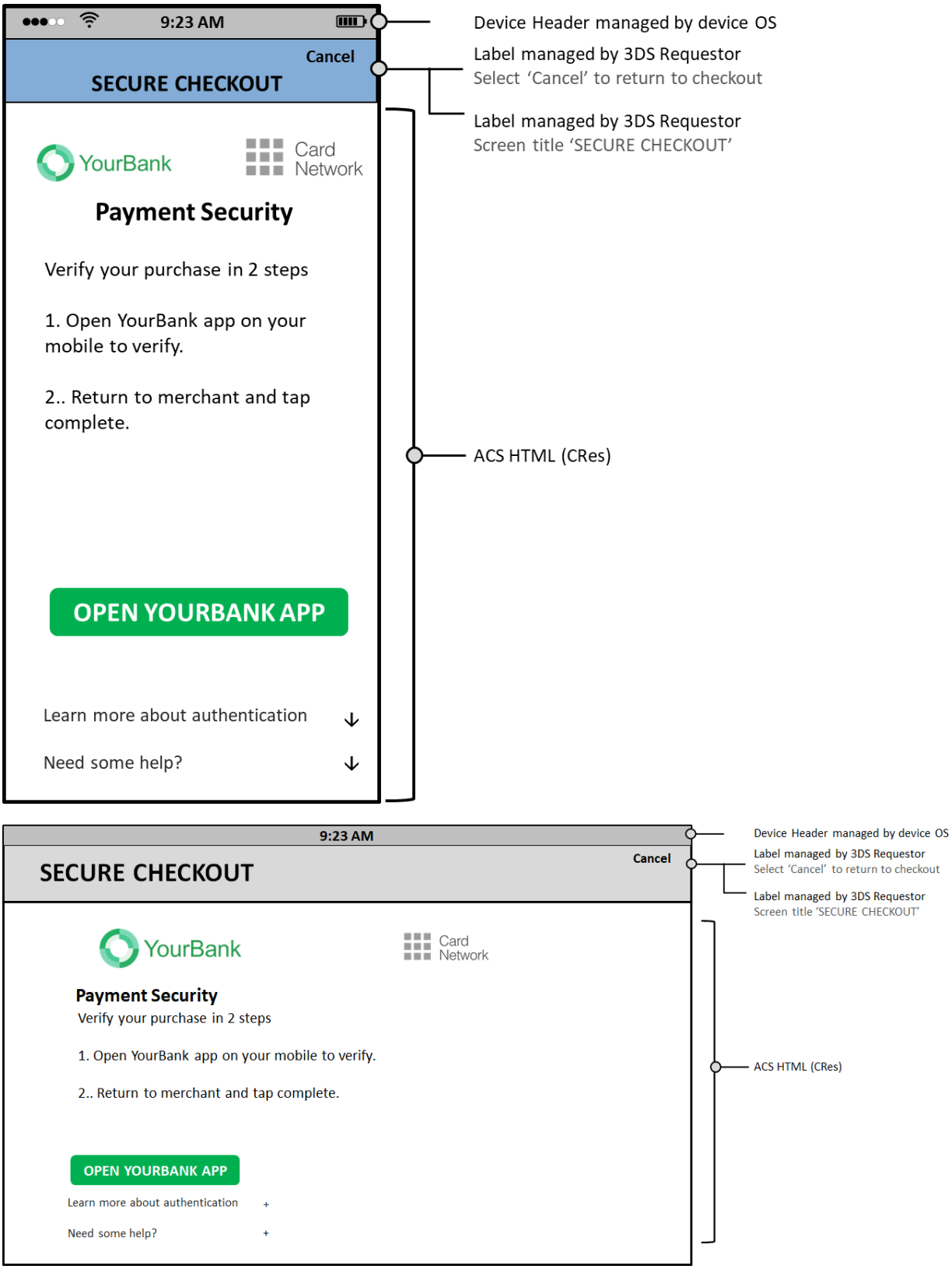


Sample OOB HTML UI Template with Complete Button—PA—Portrait + Landscape





Sample OOB HTML UI Template with OOB App URL Button—PA—Portrait + Landscape



4 Recurring and Instalment Transactions

4.1 Business Overview

Recurring payments involve Cardholders granting permission for Merchants to automatically charge their payment cards to cover subscription-type agreements, providing peace of mind for Cardholders and an easier collection process for Merchants. There are many types of recurring payments, depending on whether the amount and the frequency are fixed. For example, the frequency can be predefined, such as each week, month or year or can be non-fixed and triggered by a specific usage event (for example, when the balance on a prepaid card falls below $5, reload with $20. The amount can also be fixed (for example, "reload by $20" in the previous example) or variable – when the amount itself is dependent on usage (for example, a utility bill). Fixed amount does not necessarily mean fixed frequency, and vice versa. The use case determines the parameters of the recurring or instalment payment.

An instalment payment is a payment made over time according to a pre-agreed schedule for goods and services that have been fully delivered or performed. Instalment transactions are explained in more detail in Use Case 7: Instalment Payment below.

Merchants enjoy several advantages with recurring and instalment payments. They experience fewer late payments, as the automated system ensures that payments are collected on time. This contributes to consistent cash flow and peace of mind. Recurring and instalment payments also save time and resources for Merchants, as they eliminate the need for manual invoicing and payment collection. Additionally, Merchants can build better customer relationships by offering the convenience of recurring and instalment payments. Cardholders appreciate not having to remember to make additional payments or re-enter payment information, which results in greater satisfaction and loyalty.

Good communication between the Merchant, the Cardholder and the ACS/Issuer is essential during the set-up of a recurring and instalment transactions to prevent dispute or declined transactions. The 3DS Specification enables the Merchant to provide detailed information on recurring and instalment transactions using the data elements available in the 3DS protocol.

Benefits by actor

- Merchant
  - May help in solving disputes with Cardholders as to whether the recurring or instalment payment was put in place.
  - Leverage a single authentication to set up a recurring or instalment transaction at the same time as a purchase.
- Issuer

  Receive detailed information about the recurring or instalment transaction to make it clear an agreement is entered into.

- Cardholder
  - Enjoy the convenience of using a recurring or instalment transaction rather than initiating multiple transactions.
  - Receive detailed information about the recurring or instalment transaction before proceeding with the transaction.

4.2 Technical Features

Preconditions

Depending on the use case, the appropriate 3DS Specification version or the Bridging Message Extension will need to be supported.

Additionally, to initiate 3RI payment authentications for subsequent payments in a recurring or instalment transaction, EMV 3DS version 2.2 or 2.3.1 is required. The DS Transaction ID and/or the ACS Transaction ID, which was received in the initial authentication, is kept and used in each associated 3RI transaction.

3DS Data Elements Related to Recurring and Instalment Transactions

The following data elements may be provided by 3DS Servers to support recurring and instalment transactions.

For additional information, refer to Table A.1 in the *EMV 3-D Secure Protocol and Core Functions Specification* and the *EMV 3-D Secure Bridging Message Extension*.

Table 4.1: 3DS Data Elements Related to Recurring and Instalment Transactions

Data Element	Description	Version
3DS Requestor Authentication Indicator	Indicates the type of Authentication request. This data element provides additional information to the ACS to determine the best approach for handling an authentication request. A value of 02 indicates that this authentication is requested for a recurring transaction. A value of 03 indicates that this authentication is requested for an instalment transaction.	2.3.1 2.2
3DS Requestor Prior DS Transaction ID	This data element is within the 3DS Requestor Prior Transaction Authentication Information object and contains a DS Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the Cardholder).	2.3.1

Data Element	Description	Version
3DS Requestor Prior Transaction Reference	This data element is within the 3DS Requestor Prior Transaction Authentication Information object and contains an ACS Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the Cardholder).	2.3.1 2.2
3RI Indicator	Indicates the type of 3RI request. This data element provides additional information to the ACS to determine the best approach for handling a 3RI request. A value of 01 indicates that this authentication is requested for a recurring transaction (PA). A value of 02 indicates that this authentication is requested for an instalment transaction (PA). A value of 05 indicates that this authentication is requested for an account verification with recurring payment data for information (NPA). 3RI requests are used when the Merchant decides to authenticate subsequent transactions.	2.3.1 2.2
Instalment Payment Data	Indicates the maximum number of authorisations permitted for instalment payments.	2.3.1 2.2
Purchase Amount	Purchase amount in minor units of currency with all punctuation removed. The purchase amount is the amount payable at the time of purchase, which includes both: • the amount of the one-time purchase (when there is one) and • the amount of the recurring transaction also payable that day (if there is one). The amount payable at the set-up of a recurring payment can be the recurring amount itself, a promotional amount (i.e. a percentage of the recurring amount) or even zero if no amount is due at the time of purchase.	2.3.1 2.2

Data Element	Description	Version
Purchase Currency	Currency in which the Purchase Amount is expressed.	2.3.1 2.2
Purchase Currency Exponent	Minor units of currency as specified in the ISO 4217 currency exponent. Examples: • USD = 2 • JPY = 0	2.3.1 2.2
Purchase Date & Time	Date and time of the authentication converted into UTC.	2.3.1 2.2
Recurring Amount	Recurring amount in minor units of currency with all punctuation removed. Recurring amount is specified if the recurring payment is a fixed amount. In the case of instalment payments, the instalment amount is included in this Recurring Amount field.	2.3.1 2.2 + Bridging Message Extension
Recurring Currency	Currency in which the Recurring (or instalment) Amount is expressed.	2.3.1 2.2 + Bridging Message Extension
Recurring Currency Exponent	Minor units of currency as specified in the ISO 4217 currency exponent. Examples: • USD = 2 • JPY = 0	2.3.1 2.2 + Bridging Message Extension
Recurring Date	Effective date of the new authorised amount following the first/promotional payment in a recurring or instalment transaction. Recurring date is specified if the date is fixed.	2.3.1 2.2 + Bridging Message Extension
Recurring Expiry	Date after which no further authorisations are performed. This applies to both recurring and instalment payments. Recurring expiry is often not specified for a recurring payment in cases where there is no known expiry date.	2.3.1 2.2 + Bridging Message Extension 2.2

Data Element	Description	Version
Recurring Frequency	Indicates the minimum number of days between authorisations for a recurring or instalment transaction.	2.3.1 2.2 + Bridging Message Extension 2.2
Recurring Indicator	Indicates whether the recurring or instalment payment has a fixed or variable amount and frequency. The Recurring Indicator object contains: • the Amount Indicator • the Frequency Indicator	2.3.1 2.2 + Bridging Message Extension 2.2

4.2.1 Cardholder-Initiated Flow (App-Based or Browser-Based Device Channels)

Overview

For the initial set-up of a recurring transaction agreement, the Cardholder is present (i.e. the Cardholder is initiating the payment transaction). 3DS Servers should provide the relevant recurring transaction data elements to allow the ACS to determine the appropriate authentication action (i.e., Frictionless Flow or Cardholder challenge). If the transaction is challenged, the recurring transaction data elements are used to determine the information to display to the Cardholder. Upon a successful authentication, a DS Transaction ID and an ACS Transaction ID are provided by the ACS and returned to the 3DS Server in an ARes message (or RReq message, in the case of a Cardholder challenge). The DS Transaction ID and/or ACS Transaction ID should be provided in future authentication requests directly related to the recurring transaction to help the ACS reference the details of the initial authentication.

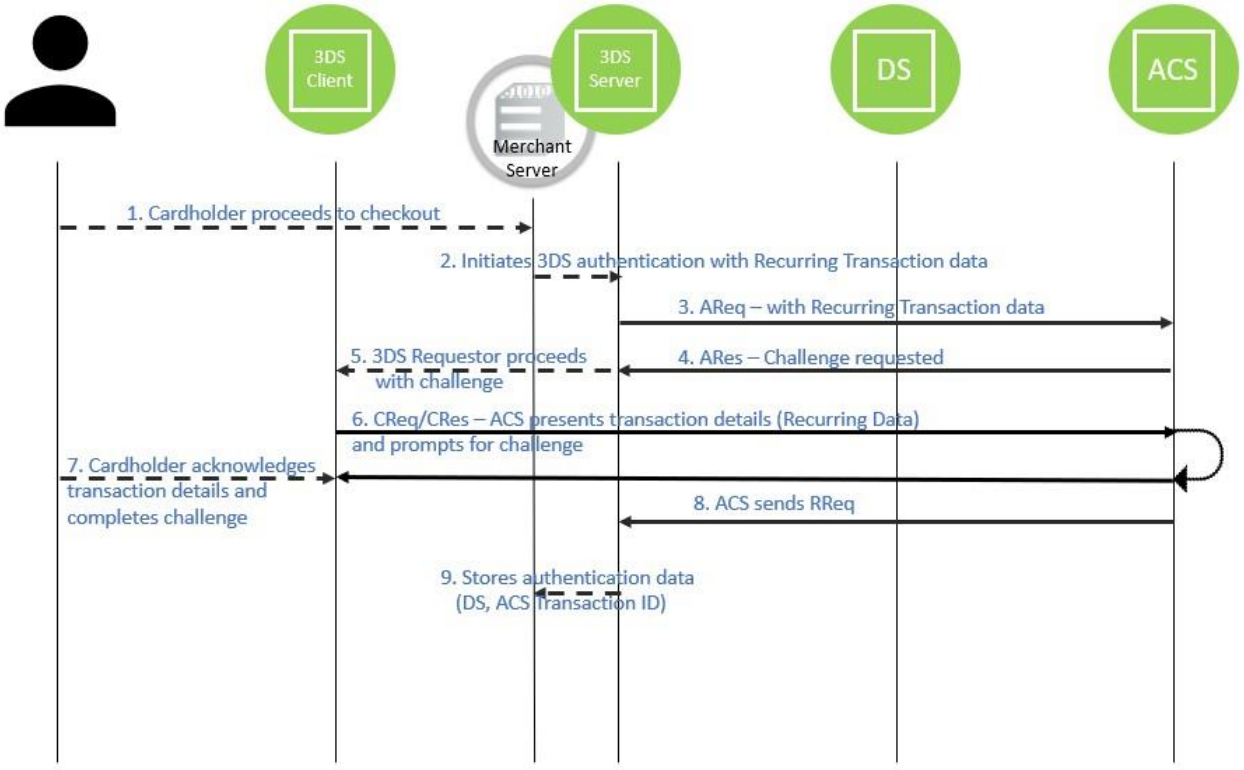
Sequence Diagram

The Cardholder and the Merchant agree on the set-up of a recurring or instalment transaction.

1. The Cardholder makes a purchase that includes a recurring or instalment payment.
2. The 3DS Requestor initiates a 3DS authentication and provides the details of the purchase, in particular the recurring transaction data elements.
3. The 3DS Server sends an AReq message.
4. The ACS responds with a challenge (ARes).
5. The 3DS Server proceeds with the challenge (opens an iframe for a Browser flow or provides the relevant data to the 3DS SDK for an App flow).
6. The ACS proceeds with the challenge and provides the UI that includes the transaction information. The ACS uses the transaction data from the AReq to provide the recurring transaction details to the Cardholder (amount, frequency, expiry date…).
7. The Cardholder acknowledges the transaction details and completes the challenge.

Note: How the Cardholder acknowledges the transaction details is an implementation decision from the ACS.

8. The ACS may store the details of the authentication for future 3RI processing, and provides the outcome of the authentication in the RReq message to the DS and 3DS Server.
9. The 3DS Requestor stores the details of the authentication (DS Transaction ID and/or ACS Transaction ID, Authentication Value) for future authentication.



4.2.2 Merchant-Initiated Flow (3RI Device Channel)

Overview

For subsequent payments in a recurring transaction, 3DS Requestors should use the 3RI Indicator to indicate that this is a recurring transaction (01 = Recurring transaction) or instalment transaction (02 = instalment). Additionally, 3DS Requestors should provide the DS Transaction ID and/or the ACS Transaction ID, which was received in the initial authentication, in the 3DS Requestor Prior Transaction Authentication Information object of the AReq message as it allows the ACS to reference the authentication from the initial set-up.

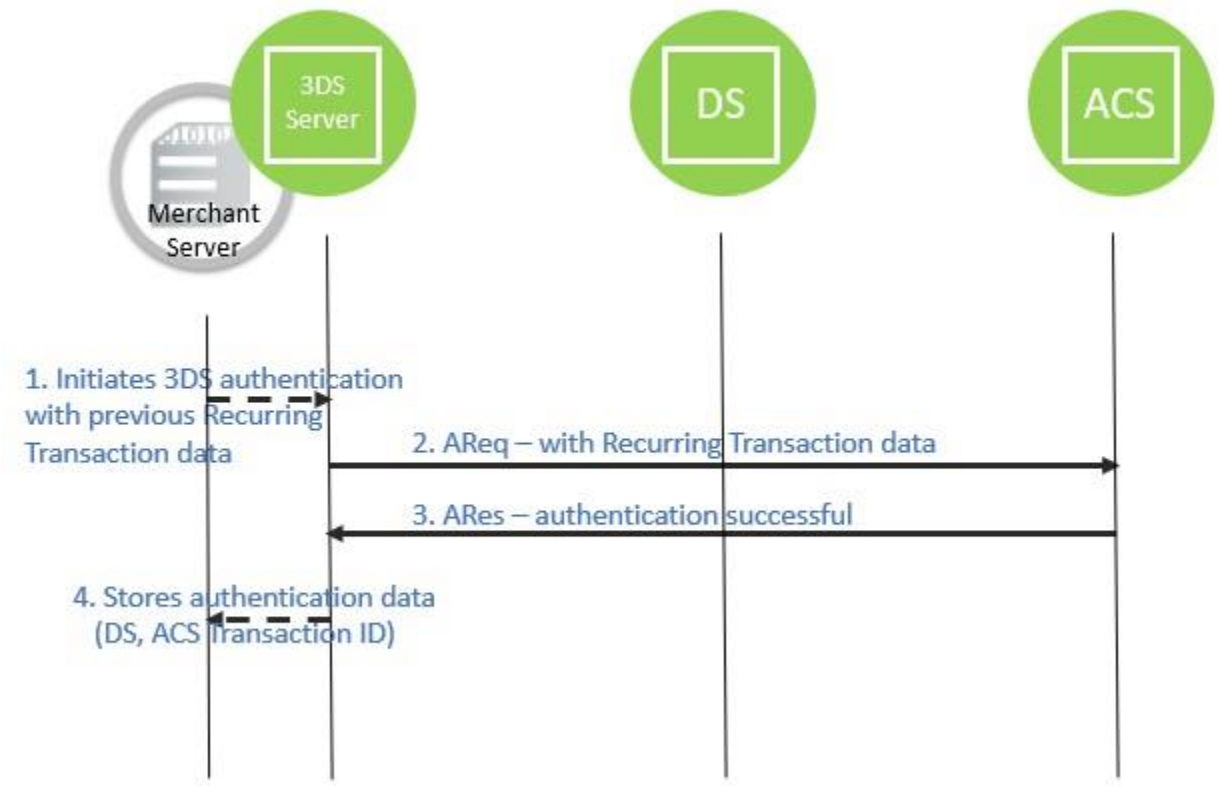
Note: 3RI payment authentications are supported in EMV 3DS version 2.2 and above.

Sequence Diagram

In a subsequent transaction with the same Merchant:

1. The Merchant needs to renew the recurring transaction before it expires (assuming the Merchant uses 3RI transactions to authenticate on an ongoing basis).
   The 3DS Requestor initiates a 3DS authentication and provides the details of the previous transaction (DS Transaction ID and/or ACS Transaction ID) in the 3DS Requestor Prior Transaction Reference.

2. The 3DS Server sends a 3RI Authentication Request (AReq).
3. The ACS matches the references provided in the 3DS Requestor Prior Transaction Reference to the initial Cardholder-initiated transaction, responds with an approval (ARes) to the DS and 3DS Server.
4. The 3DS Requestor stores the details of the authentication (DS Transaction ID and/or ACS Transaction ID, Authentication Value) for future authentication.



4.3 Use Cases

The following use cases illustrate the technical capabilities of 3DS with recurring data elements and cover the most common types of recurring or instalment transactions. Payment systems may impose additional requirements on the use of recurring data, including for the purposes of ensuring compliance with market regulations.

4.3.1 Use Cases for Version 2.2

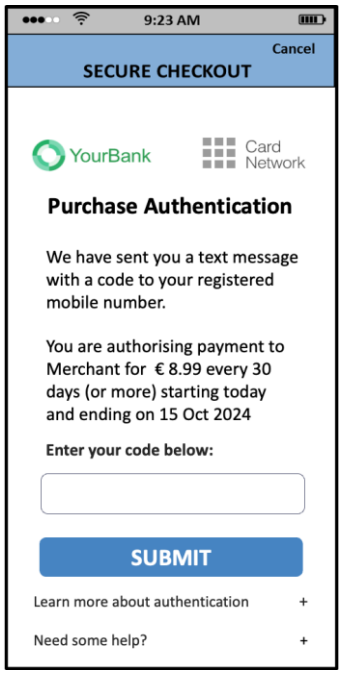
With version 2.2 of the 3DS Specification, the Merchant has a limited set of data available to provide to the ACS about a recurring or instalment transaction. For example, the Merchant cannot indicate if the recurring transaction has a variable amount, or if the instalment amount is different from the initial amount (purchase amount).

Presented below are example use cases for recurring or instalment transactions in version 2.2:

1. Recurring payment with a fixed frequency
2. Instalment payment

4.3.1.1 Use Case 1: Recurring Payment with a Fixed Frequency

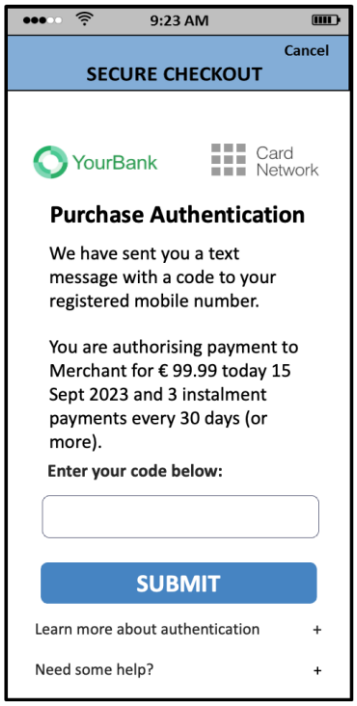
In this use case, the amount due at recurring payment set-up is the same amount that will be due on a recurring basis. In the example below, the Cardholder is committing to pay €8.99 monthly, starting on the day of the purchase and ending on 15 October 2024.

Merchant/Acquirer	Issuer	Cardholder
Existing recurring data elements • Purchase Amount = 899 • Purchase Currency = 978 (€) • Purchase Currency Exponent = 2 • Purchase Date & Time = 20230915120000 • Recurring Expiry = 20241015 • Recurring Frequency = 30 • 3DS Requestor Authentication Indicator = 02	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information. Message is displayed to the Cardholder in the 3DS challenge window.	

4.3.1.2 Use Case 2: Instalment Payment

An instalment payment is a payment made over time according to a pre-agreed schedule for goods and services that have been fully delivered or performed.

One example is the purchase for a total of €999.99, to be paid in 4 instalments (i.e., 3 times €300.00 each month after the first payment of €99.99), with the first payment occurring on the day of the purchase. The merchant cannot provide information on the different amounts between the first payment and the 3 successive instalment payments. Similarly, if anything else is purchased at the same time as the instalment set up, the amount of that purchase would be added to the purchase amount with the first installment payment

Merchant/Acquirer	Issuer	Cardholder
Existing recurring data elements • Purchase Amount = 9999 • Purchase Currency = 978 (€) • Purchase Currency Exponent = 2 • Purchase Date & Time = 20230915120000 • Recurring Frequency = 30 • Instalment Payment Data = 04 • 3DS Requestor Authentication Indicator = 03	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information. Message is displayed to the Cardholder in the 3DS challenge window.	

4.3.2 Use Cases for Version 2.3.1

With version 2.3.1 of the 3DS Specification, the Merchant has a large set of data available to provide to the ACS about a recurring or instalment transaction. For example, the Merchant can indicate if the recurring transaction has a variable amount, or if the recurring amount is different from the initial amount (purchase amount).

The use cases are also possible with version 2.2 of the 3DS Specification if the Bridging Message Extension with a Recurring Data object is present and supported by the ACS and the 3DS Server:

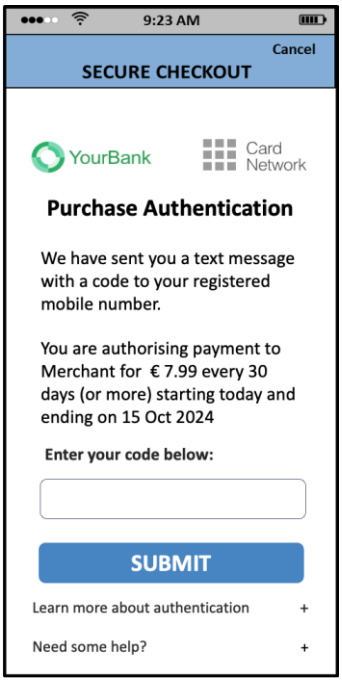
1. Recurring payment with a fixed amount and a fixed frequency.
2. Recurring payment with a fixed amount, fixed frequency, and a promotional rate.
3. Recurring payment with a variable amount and a fixed frequency.
4. Recurring payment with a variable amount and a variable frequency.
5. Recurring payment with a fixed amount and a variable frequency.
6. Recurring payment combined with one-time purchase.
7. Instalment payments.

4.3.2.1 Use Case 1: Recurring Payment with a Fixed Amount and a Fixed Frequency

In this scenario, the amount due at recurring payment set-up is the amount that will be due on a recurring basis. Use Case 2 covers the scenario when the two amounts differ.

In the example below, the Cardholder is committing to pay €7.99 monthly, starting on the day of the purchase and ending on 15 October 2024.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 799
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• Recurring Expiry = 20241015
• Recurring Frequency = 30
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Amount = 799
• Recurring Indicator
  ○ Amount Indicator = 01
  ○ Frequency Indicator = 01
• Recurring Currency = 978 (€)
• Recurring Currency Exponent = 2
• Recurring Date = 20231015
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.2.2 Use Case 2: Recurring Payment with a Fixed Amount, Fixed Frequency, and a Promotional Rate

A rate is considered promotional when the amount to be paid at set-up is not the same as the amount to be paid on an ongoing basis. In the case of an ongoing subscription of €7.99/month, the data listed below need to be provided.

If the first month is free:

- The purchase amount will be zero.
- The recurring amount will be €7.99.

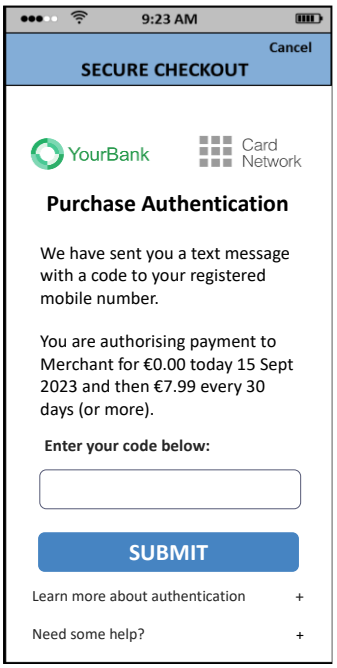
If there is a 50% discount:

- The purchase amount will be €3.99.
- The recurring amount will be €7.99.

If there is no promotional rate and the €7.99 is also due on the day of the purchase, refer to Use Case 1: Recurring Payment with a Fixed Amount and a Fixed Frequency.

In the example below, the first month is free, the recurring amount is €7.99, and there is no end date provided. When there is no end date, there is no need to (and it is recommended not to) convey this information.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 0
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• Recurring Frequency = 30
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 01
  ○ Frequency Indicator = 01
• Recurring Amount = 799
• Recurring Currency = 978 (€)
• Recurring Currency Exponent = 2
• Recurring Date = 20231015
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

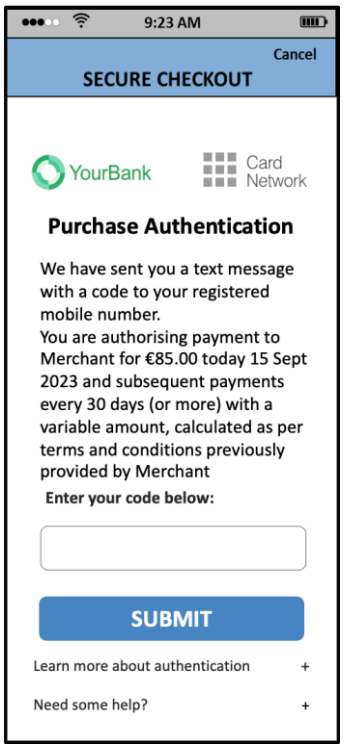
4.3.2.3 Use Case 3: Recurring Payment with a Variable Amount and a Fixed Frequency

In the case of a recurring payment with a variable amount, the method of calculating the amount is typically communicated in the Merchant's terms and conditions of the recurring payment set-up. For example, in the case of an electricity bill, a Merchant will typically inform the Cardholder that the amount to be charged will depend on usage and will be calculated on display €x per kW of usage.

It is recommended that Issuers find a generic way to convey the meaning of "variable amount" by using terms such as "of an amount calculated as per the terms and conditions previously displayed by the merchant". When there is no end date, there is no need to (and it is recommended not to) convey this information.

The example below shows data provided when the Merchant has required a payment of €85 on the day of the purchase (considered the average monthly payment) and payment on usage every month starting one month after that date.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 8500
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• Recurring Frequency = 30
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 02
  ○ Frequency Indicator = 01
• Recurring Date = 20231015
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.2.4 Use Case 4: Recurring Payment with a Variable Amount and a Variable Frequency

In the case of a recurring payment with a:

- variable amount – the method of calculating the amount is typically communicated as part of the Merchant's terms and conditions of the recurring payment set-up;
- variable frequency – the event that will trigger a charge/payment is typically described to the Cardholder in the Merchant's terms and conditions of the recurring payment set-up.

For example, in the case of a payment to be collected by a highway operator when the Cardholder's transponder is used on a highway, the operator informs the Cardholder that a payment will be charged at the end of the day, every time the highway is used on that day, for an amount based on the distance driven.

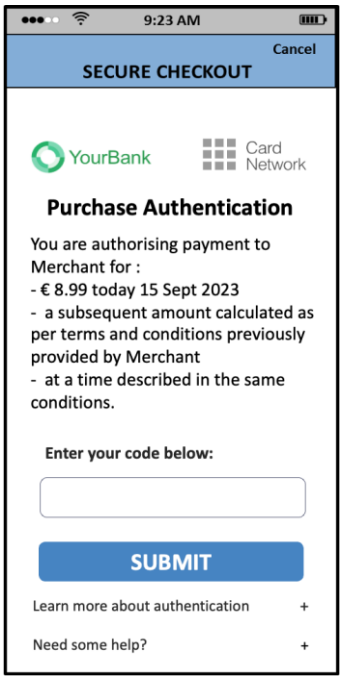
It is recommended that Issuers find a generic way to convey the meaning of "variable amount" and "variable frequency" to Cardholders by using terms such as:

- for amount – "of an amount calculated as per the terms and conditions previously displayed by the merchant";
- for frequency – "at a time described in the terms and conditions previously displayed by the merchant".

When both amount and frequency are variable, Issuers should try to avoid displaying the wording “described in the terms and conditions previously described by the merchant” twice, for example, as per the image below.

Note: Payment systems may impose additional requirements on the use of recurring data or may set limits such as a maximum amount.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 899
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 02
  ○ Frequency Indicator = 02
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.2.5 Use Case 5: Recurring Payment with a Fixed Amount and a Variable Frequency

In the case of payments with a variable frequency, the event that will trigger a charge/payment is typically described to the Cardholder in the Merchant’s terms and conditions of the recurring payment set-up.

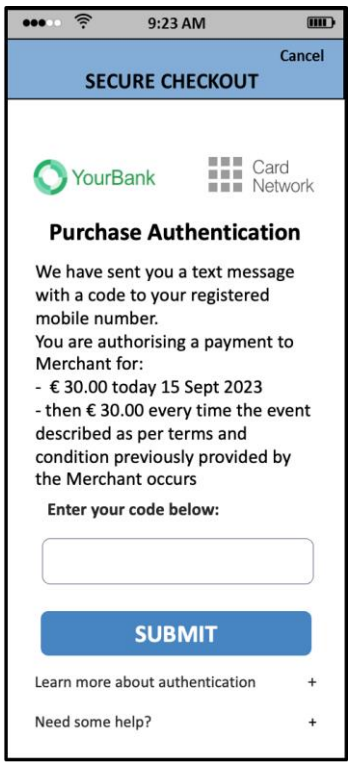
For example, in the case of a payment to be collected by a transit operator that provides prepaid transit cards, the triggering event could be the transit card balance falling below an amount set by the Cardholder or set by the operator and communicated to the Cardholder.

The terms and conditions set forth by the operator may state, for example, that a reload of €30.00 will occur when the transit card balance falls below €15.00.

In the example below, at set-up, the card is loaded with €30 and a reload of €30 will occur when the balance falls below €15.00.

Note: Payment systems may impose additional requirements on the use of these data or may set limits such as a maximum transaction per recurring period.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 3000
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 01
  ○ Frequency Indicator = 02
• Recurring Amount = 3000
• Recurring Currency = 978 (€)
• Recurring Currency Exponent = 2
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.2.6 Use Case 6: Recurring Payment, Combined with a One-Time Purchase

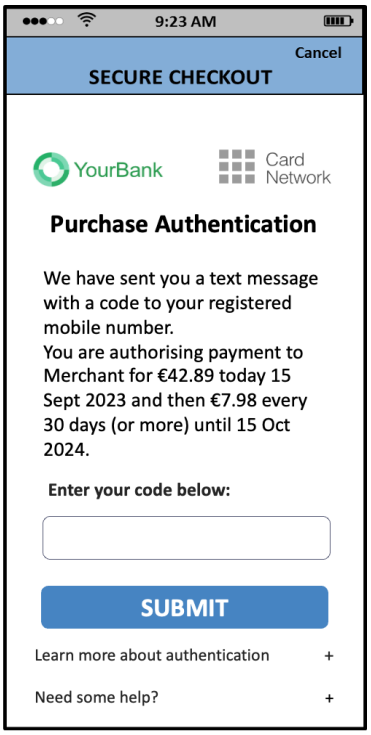
In every use case, the amount to be sent in the purchase amount is the amount the Cardholder must pay on the day of the authentication. This will include:

- the amount of the one-time purchase when there is one
- the amount of the recurring agreement also payable that day:
  - if there is a promotion and no amount is payable that day, this amount is zero, but if any amount is payable that day, this amount must be added to the amount of the one-time purchase;
  - if both the amount of the one-time purchase and a recurring amount is to be paid that day, it is not possible to indicate the individual amount for each.

The amounts and frequency to be provided in the recurring data amount and frequency should follow the principles set forth in Use Cases 1–5.

For example, if the one-time purchase has a value of €42.89 and the fixed recurring payment is free for the first month and payable only in the second month (see example below), then the purchase amount should be sent as €42.89. If 50% of the recurring amount is due on the day of the purchase (€3.99), in addition to the purchase of €42.89, the amount to be sent in the purchase amount would be €46.88 (sum of €42.89 and €3.99).

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 4289
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• Recurring Expiry = 20241015
• Recurring Frequency = 30
• 3DS Requestor Authentication Indicator = 02
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 01
  ○ Frequency Indicator = 01
• Recurring Amount = 798
• Recurring Currency = 978 (€)
• Recurring Currency Exponent = 2
• Recurring Date = 20231015
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.2.7 Use Case 7: Instalment Payment

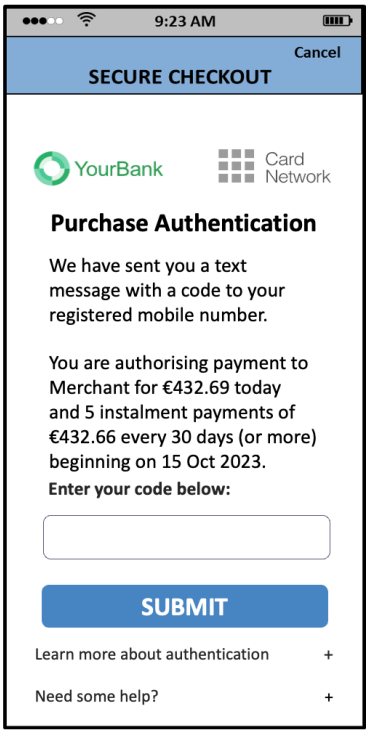
An instalment payment is a payment made over time according to a pre-agreed schedule for goods and services that have been fully delivered or performed.

One example is the purchase of a sofa for a total of €2595.99, to be paid in 6 instalments (i.e. €432.66 each after the first payment of €432.69), with the first payment occurring on the day of the purchase. As the first instalment is paid on the day of the purchase, only 5 instalments remain. The value provided in the Instalment Payment Data corresponds to the maximum number of authorisations permitted for instalment payments (6 in this example).

If any other purchase was made at the same time as the instalment set-up, the amount of that purchase would be added to the purchase amount with the first instalment payment, following the principles set forth in Use Case 6 above.

Note: Payment systems may impose different requirements on the use of these data. For example, they may require that the total amount (€2595.99) be provided in the Purchase Amount.

Merchant/Acquirer	Issuer	Cardholder

Existing recurring data elements
• Purchase Amount = 43269
• Purchase Currency = 978 (€)
• Purchase Currency Exponent = 2
• Purchase Date & Time = 20230915120000
• Recurring Frequency = 30
• Instalment Payment Data = 06
• 3DS Requestor Authentication Indicator = 03
 	
Additional elements
• Recurring Indicator
  ○ Amount Indicator = 01
  ○ Frequency Indicator = 01
• Recurring Amount = 43266
• Recurring Currency = 978 (€)
• Recurring Currency Exponent = 2
• Recurring Date = 20231015
	Determines that a Cardholder challenge is necessary and builds the message with the recurring payment information.
	
	Message is displayed to the Cardholder in the 3DS challenge window.
		

4.3.3 Best Practices for Defining Recurring Frequency Values

The Recurring Frequency data element defines the minimum number of days between authorisations. This is a limitation, as Merchants often charge on a fixed interval basis – not necessarily based on the number of days but on a calendar interval (week, month, quarter…). It is recommended that Merchants use the Recurring Frequency values indicated in Table 4.2: to ensure that the Issuer's message is expressed as a calendar interval rather than a number of days. Issuers receiving those Recurring Frequency values should use the corresponding calendar intervals to display recurring transaction information to Cardholders.

Table 4.2: Recommended Issuer Messaging for Recurring Frequency Values

Recurring Frequency value	Issuer messaging
7	Every week
14	Biweekly
28	Every month
59	Bimonthly
89	Quarterly
181	Twice a year
365	Annually

For example, for a Recurring Frequency of 28 days, the ACS should interpret the frequency as a monthly payment and provide the following message to the Cardholder:
“You are authorising payment to *[Merchant abc]* every **month**”.

If the ACS does not interpret the 28 days as a monthly payment, it may provide the following message to the Cardholder:
“You are authorising payment to *[Merchant abc]* every **28 days (or more)**”.

5 3-D Secure Documentation

The 3DS documentation consists of several key documents that define the three-domain model and overall architecture and provide the technical requirements, as well as a range of supporting documents to help the understanding and implementation of the 3DS protocol.

There are four key types of 3DS documentation:

- Specifications – define the 3DS architecture and requirements
- Specification bulletins – update or complement the specifications
- Message extensions – enable the transport of additional data
- Supporting documents such as guides, white papers or FAQ – provide additional information and guidance.

The 3DS Specification consists of five key documents listed below.

- EMV 3-D Secure Protocol and Core Functions Specification (the main 3-D Secure specification) – defines the three-domain model, the messages, their data, and the channels for performing a 3DS authentication.
- EMV 3-D Secure SDK Specification – defines the device-side component of 3DS. 3DS Requestors such as Merchants integrate this SDK with their mobile device app and make the app available to end users.
- EMV 3-D Secure Split-SDK Specification – defines a variant of the 3DS SDK for which some of the client functionalities do not run on the device, but on a server component, thus implementing a 3DS SDK with functionalities split between a Split-SDK Client (client side) and a Split-SDK Server (server side).
- EMV 3-D Secure SDK Device Information – defines the device information provided by the 3DS SDK when an authentication is initiated from an app.
- EMV 3-D Secure Specification Bulletin No. 255 Specification Version Configuration – defines the status of the EMV® 3-D Secure Protocol and Core Functions Specification, the EMV 3-D Secure SDK—Device Information versions, and the EMV® 3-D Secure Message Extensions.

The SDK Specification and the Split-SDK Specification are only applicable to mobile device applications or the Split-SDK architecture.

There are currently four EMV 3-D Secure message extensions:

- EMV 3-D Secure Bridging Message Extension – defines how existing 3DS v2.1.0 and v2.2.0 components can provide or consume additional data related to EMV® 3-D Secure Protocol and Core Functions Specification v2.3.1.
- EMV 3-D Secure Device Acknowledgement Message Extension – defines how the 3DS Server can provide the Split-SDK-related data to the ACS and the ACS can acknowledge data received in EMV® 3-D Secure Device Information.
- EMV 3-D Secure Payment Token Message Extension – defines how 3DS components can provide or receive token-related information.

- EMV 3-D Secure Travel Industry Message Extension – defines how 3DS Servers can provide travel-related data to the ACS.

5.1 3-D Secure Specification v2.2.0

The following documents are applicable to 3DS Specification v2.2.0:

- EMV 3-D Secure Protocol and Core Functions Specification v2.2.0, as amended by EMV 3-D Secure Specification Bulletin No. 214 v3 (June 2023)
- EMV 3-D Secure SDK Specification v2.2.0, as amended by EMV® 3-D Secure Specification Bulletin No. 211 – EMV® 3-D Secure SDK Key Features for version 2.2.0 (December 2018)
- EMV 3-D Secure Specification Bulletin No. 255 v3 – Specification Version Configuration (December 2023)

For this version, the updates to the specifications are contained in the applicable specification bulletins.

5.2 3-D Secure Specification v2.3.1

The following documents are applicable to 3DS Specification v2.3.1:

- EMV 3-D Secure Protocol and Core Functions Specification v2.3.1.1
  - EMV 3-D Secure Specification Bulletin No. 294 – updates, clarifications and errata incorporated since version 2.3.1.0 (May 2023)
  - EMV 3-D Secure Specification Bulletin No. 279 – updates, clarifications and errata incorporated since version 2.2.0 as amended by EMV® 3-D Secure Specification Bulletin No. 214 v3 (August 2023)
- EMV 3-D Secure SDK Specification v2.3.1.1
  - EMV 3-D Secure Specification Bulletin No. 296 – updates, clarifications and errata incorporated since version 2.3.1.0 (May 2023)
  - EMV 3-D Secure Specification Bulletin No. 280 – updates, clarifications and errata incorporated since version 2.2.0 (August 2023)
- EMV 3-D Secure Split-SDK Specification v2.3.1.0
  - EMV 3-D Secure Specification Bulletin No. 271 Split-SDK Specification for version 2.3.1.0 (August 2022)
- EMV 3-D Secure Specification Bulletin No. 255 v3 – Specification Version Configuration (December 2023)

For this version, the specifications include all the latest revisions, and specification bulletins are provided (where applicable) solely as resources reflecting the changes.

5.3 3-D Secure SDK — Device Information

The EMV 3-D Secure SDK – Device Information is applicable to the ACS for all specification versions (refer to EMV 3-D Secure Specification Bulletin 255).

- Data Version 1.0:
  - EMV 3-D Secure SDK – Device Information Version 2.0.0
  - EMV 3-D Secure Specification Bulletin No. 205 v1 (August 2018)
- Data Version 1.1:
  - EMV 3-D Secure SDK – Device Information Version 2.1.0
  - EMV 3-D Secure Specification Bulletin No. 213 v1 (May 2019)
- Data Version 1.3: EMV 3-D Secure Specification Bulletin No. 222 v1 (August 2019)
- Data Version 1.4: EMV 3-D Secure Specification Bulletin No. 223 v1 (October 2019)
- Data Version 1.5
  - EMV 3-D Secure SDK – Device Information Data Version 1.5
  - EMV 3-D Secure Specification Bulletin No. 225 – SDK Device Information Data Version 1.5 Updates, clarifications, and errata (September 2021)
- Data Version 1.6
  - EMV 3-D Secure SDK – Device Information Data Version 1.6
  - EMV 3-D Secure Specification Bulletin No. 285 – SDK Device Information Data Version 1.6 (May 2023)

All the specifications and specification bulletins listed in this section are available on the EMVCo website.

5.4 Other Supporting Documentation

- EMV 3-D Secure Specifications Frequently Asked Questions – Technical Questions (January 2024)
- EMV 3-D Secure Frequently Asked Questions – General Questions (December 2020)
- EMV 3-D Secure SDK Technical Guide Version 2.1.0 (October 2017)
- EMV 3-D Secure App-based Cryptographic Worked Samples Version 3.0.0 (October 2019)
- EMV 3-D Secure JSON Message Samples Version 2.1.0 (April 2018)
- EMV 3-D Secure White Paper Version 2.0 – Use of FIDO® Data in 3-D Secure Messages to Support Issuer Validation of FIDO® Authentication Data (November 2023)
- EMV 3-D Secure Browser Flow Best Practices (September 2021)
- EMV 3-D Secure and PSD2 Requirements for Strong Customer Authentication (December 2020)

- EMV 3-D Secure UI/UX Design Guidelines
- EMV General Bulletin No. 50 – New EMV 3-D Secure UI Design Guidelines (August 2021)

All the documents listed in this section are available on the EMVCo website.