# *EMV® Specification Bulletin No. 207*
***December 2018***

## *EMV® 3-D Secure Updates, Clarifications & Errata*

*This Specification Bulletin No. 207 provides updates, clarifications and errata incorporated into the EMV 3-D Secure Protocol and Core Functions Specification since version 2.1.0 (including SB 204v4).*

### *EMV® 3-D Secure Key Features v2.2.0*

*This Specification Bulletin No. 207 introduces new 3-D Secure features included in version 2.2.0 of the 3-D Secure Protocol and Core Functions Specification. These features include:*

- *Additional support for upcoming PSD2 Regulation (Whitelisting and Acquirer Exemptions)*
- *Support for 3RI Payments*
- *Introduction of a new Authentication Method: Decoupled Authentication*
- *Enhancements for OOB User Experiences—Note: These enhancements are only partially described in this bulletin (i.e., the addition of the 3DS Requestor App URL). As these enhancements have SDK impact, they will be fully described and reflected in the EMV 3-D Secure SDK specification version 2.2.0.*

### *Applicability*

*This Specification Bulletin applies to:*

- *EMV® 3-D Secure Protocol and Core Functions Specifications, Version 2.2.0*

*Updates are provided in the order in which they appear in the specification. Deleted text is identified using strikethrough, and red font is used to identify changed text. Unedited text is provided only for context.*

# Contents

# Chapter 1 Introduction

The 3-D Secure authentication protocol supports two Message Categories:

- **Non-Payment Authentication**—Identity verification and account confirmation.
- ~~**Confirmation of Account**—Verification of Account~~

The 3-D Secure authentication protocol can be initiated through three Device Channels:

- **3DS Requestor Initiated**—Confirmation of account information and Cardholder authentication with no direct Cardholder present. For example, a subscription-based e-commerce merchant confirming that an account is still valid or Cardholder authentication when the 3DS Requester and the ACS utilises Decoupled Authentication.

## 1.3 Normative References

**Table 1.1 Normative References**

| Reference | Publication Name | Bookmark |
|---|---|---|
| RFC 5246 | *The Transport Layer Security (TLS) Protocol Version 1.2* | https://tools.ietf.org/html/rfc5246 |
| RFC 8446 | *The Transport Layer Security (TLS) Protocol Version 1.3* | https://tools.ietf.org/html/rfc8446 |

## 1.5 Definitions

**Table 1.3 Definitions**

| Term | Definition |
|---|---|
| 3DS Requestor Initiated (3RI) | 3-D Secure transaction initiated by the 3DS Requestor for the purposes of confirming that an account is still valid or for Cardholder authentication.<br><br>The first main use case being recurrent transactions (TV subscriptions, utility bill payments, etc.) where the merchant wants to perform a payment transaction to receive authentication data for each bill or a non-payment transaction to verify that a subscription user still has a valid form of payment. The second main use case is when the 3DS Requestor requests Decoupled Authentication as a method to authenticate the Cardholder. |
| Base64URL | Encoding applied to the 3DS Method Data, Device Information and the CReq/CRes messages as defined in RFC 7515. |
| Decoupled Authentication | Decoupled Authentication is an authentication method whereby authentication can occur independent from the cardholder's experience with the 3DS Requestor. The authentication method used for Decoupled Authentication is outside the scope of this specification, however one method could be a push notification to a banking app that completes authentication and then sends the results to the ACS.<br><br>Decoupled Authentication is applicable to all Device Channels. |
| Information Only | Information Only is a Transaction Status value, whereby the ACS acknowledges the 3DS Requestor's preference to not challenge on the transaction since the data sent was only for informational purposes. |
| Whitelisting | In this specification, the process of an ACS enabling the cardholder to place the 3DS Requestor on their trusted beneficiaries list. |

## 1.7 3-D Secure Protocol Version Number

**Table 1.5 Protocol Version Numbers**

| Reference | Publication Name |
|---|---|
| 2.2.0 | Active |

# Chapter 2 EMV 3-D Secure Overview

### 2.3.4 Access Control Server

The ACS contains the authentication rules and is controlled by the Issuer. ACS functions include:

- ~~Authenticating the Cardholder for a specific transaction~~
- Authenticating the Cardholder or confirming account information ~~for a 3RI transaction~~

### 2.4.5 Results Request Message (RReq)

The RReq message communicates the results of the authentication or verification. The message is sent by the ACS through the DS to the 3DS Server. There is only one RReq message per ~~authentication~~AReq message. The RReq message is not present ~~only~~ in ~~an~~ a ~~authentication requiring a Cardholder challenge~~Frictionless transaction.

### 2.4.6 Results Response Message (RRes)

There is only one RRes message per RReq message~~authentication. The RRes message is present only in an authentication requiring a Cardholder challenge~~.

### 2.4.7 Preparation Request Message (PReq)

The PReq message is sent from the 3DS Server to the DS to request information about the ~~Protocol Version Number(s) supported by available~~ ACSs and the DS ~~and if one exists, any corresponding 3DS Method URL. This message is not part of the 3-D Secure authentication message flow~~.

### 2.4.8 Preparation Response Message (PRes)

~~The PRes message is the DS response to the PReq message.~~ The 3DS Server can utilise the PRes message to cache information about the ~~Protocol Version(s) supported by available~~ ACSs and the DS, (for example, about which Protocol Version(s) are supported).~~and if one exists, about the corresponding 3DS Method URL. This message is not part of the 3-D Secure authentication message flow~~.

### 2.5.2 Challenge Flow

In addition to the AReq and ARes messages that comprise the Frictionless flow, the Challenge flow ~~consists of~~ completes with the ~~CReq, CRes,~~ RReq, and RRes messages. The Challenge flow also includes CReq and CRes messages except in the case of Decoupled Authentication.

## 2.7 Challenge Flow Outline

**6. ACS to 3DS Client**

**Note: For Decoupled Authentication, instead of utilising the CReq and CRes messages, the ACS authenticates the cardholder outside of the EMV 3DS protocol.**

# Chapter 3 EMV 3-D Secure Authentication Flow Requirements

## 3.1 App-based Requirements

*Added Note following Figure 3.1:*

**Note: For a Decoupled Authentication challenge, instead of utilising the CReq and CRes messages (Steps 10 through 17 and Step 23), the ACS authenticates the cardholder outside of the EMV 3DS protocol. The Decoupled Authentication flow is portrayed in Figure 3.4 and outlined below.**

### Step 5 The 3DS Server

*Updated Note following Req. 14:*

**Note: In addition, the 3DS Server can use the ACS Information Indicator to identify the features that the Account Range supports (for example, Decoupled Authentication and/or Whitelisting).**

### Step 7 The ACS

### [Req 26]

Check whether the Consumer Device is supported unless transaction will be processed as a Decoupled Authentication.

If device not supported, the ACS returns to the DS an ARes message with a Transaction Status = U and Transaction Status Reason code = 03 and ends processing.

*Updated Note following Req 26:*

**Note: The ACS uses the Device Information received in the AReq message to recognise the device, assess transaction risk, and determine if it can complete the authentication ~~with this device~~.**

*Added Note following Req 26:*

**Note: When Decoupled Authentication is utilised, the consumer device that initiated the transaction does not need to be supported when the ACS has alternative approaches to authenticating the Cardholder.**

### [Req 29]

Use the values of the 3DS Requestor Challenge Indicator, the 3DS Requestor Authentication Indicator and the 3DS Requestor Decoupled Requestor Indicator received in the AReq message when evaluating the transaction disposition as defined in ***[Req 30]***.

### [Req 30]

Evaluate the values received in the AReq message and determine whether the transaction is:

- requiring a Cardholder challenge using Decoupled Authentication (Transaction Status = D)
- authentication not requested by the 3DS Server for data sent for informational purposes only (Transaction Status = I)

### [Req 321]

If a Decoupled Authentication challenge is deemed necessary (Transaction Status = D), the ACS determines whether an acceptable challenge method is supported by the ACS based in part on the following data element received in the AReq message: 3DS Requestor Decoupled Max Time. The ACS performs the following:

a. Sets the Transaction Status = D for Decoupled Authentication.

b. Sets the ACS Decoupled Confirmation Indicator = Y.

c. Stores the 3DS Server Transaction ID and DS Transaction ID (for subsequent RReq processing).

**[Req 322]**

For a Decoupled Authentication transaction, (Transaction Status = D), do the following asynchronous process:

a. Start timer against the 3DS Requestor Decoupled Max Time.

b. Authenticate the cardholder. How an authentication decision is made is outside the scope of this specification, however the ACS objective is to complete the Cardholder authentication before the 3DS Requestor Decoupled Max Time expires.

### Step 8: The DS

**[Req 37]**

Send the ARes message to the 3DS Server ~~as~~ received from the ACS using the secure link established in [Req 12].

### Step 9: The 3DS Server

**[Req 323]**

For a Decoupled Authentication transaction (Transaction Status = D), send necessary information (as defined in Table B.2) from the ARes message to the 3DS Requestor Environment.

**[Req 355]**

If the Cardholder Information Text has been provided by the ACS for this transaction the 3DS Server shall ensure the Cardholder Information Text is displayed on the 3DS Requestor website.

*New and updated Notes at the end of Step.*

**Note: The next step for:**

- **Decoupled Authentication transaction, the next step is Step 18**
- **Challenge Flow is Step 10 (Step 10 through Step 23 and the first requirement of Step 24 are applicable only for a Challenge Flow [Transaction Status = C]).**

**Note: For a Decoupled Authentication transaction, as defined in *[Req 345],* the 3DS Server is now expected to wait for the ACS to authenticate the Cardholder at which time the ACS will send an RReq message.**

### Step 11: The 3DS Requestor Environment

**[Req 45]**

If the content protection fails, the SDK reports the error to the 3DS Requestor App and **ends 3-D Secure processing**.

### Step 13: The ACS

**[Req 52]**

If the content protection fails the ACS **ends 3-D Secure processing**.

### Step 16: The 3DS SDK

**[Req 57]**

If the content protection fails, the SDK reports the error to the 3DS Requestor App and **ends 3-D Secure processing**.

### Step 18: The ACS

*Updated Step introduction (applicable to all requirements in step):*

The ACS shall for all Challenge flow transactions (ARes Transaction Status = C) and for Decoupled Authentication transactions (ARes Transaction Status = D) once the authentication as defined in [Req 322].b has completed or the timer as defined in [Req 322].a has expired do the following:

### [Req 66]

Ensure that one RReq message is sent to the DS for each ARes message with a Transaction Status = C or D.

### [Req 345]

Ensure for a Decoupled Authentication transaction that:

- An RReq message is sent immediately upon obtaining an authentication result (whether successful or not).
- An RReq message without an authentication result is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

### Step 20 The 3DS Server

### [Req 346]

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 30 seconds for the RReq message. If an RReq message is never received, further processing is outside the scope of 3- Secure processing.

**Note: If the RReq message is not received, then the 3DS Server should assume that the Decoupled Authentication is not successful.**

### Step 22 The ACS

*New Note following [Req 75]:*

**Note: 3-D Secure processing completes for Decoupled Authentication transactions.**

### Step 23: The ACS

*Updated Step introduction (applicable to all requirements in Step):*

The ACS shall for a Challenge flow transaction (ARes Transaction Status = C) ~~(~~as a continuation of receiving the CReq message in Step 17~~)~~, do the following:

### [Req 76]

If the content protection fails the ACS **ends 3-D Secure processing**.

### Step 24 The 3DS Requestor Environment

*Updated Step introduction (applicable to all requirements in Step):*

The 3DS SDK shall for a Challenge flow transaction (ARes Transaction Status = C):

## 3.2 Challenge Flow with OOB Authentication Requirements

### Step 17: *(2nd paragraph)*

When a Cardholder returns to the 3DS Requestor App from ~~another~~ an OOB app on the same device, further Cardholder action will not be required to complete the authentication~~the ACS can also utilise the Challenge Additional Info Text element (for the Native UI) or the ACS HTML Refresh element (for the HTML UI) to improve the UI experience~~. In this scenario, the SDK will automatically ~~display these data elements~~post a CReq message when the 3DS Requestor App is moved to the foreground.

**Note: OOB authentication as defined in this section is a sperate authentication flow from the Decoupled Authentication flow.**

## 3.3 Browser-based Requirements

*Added after Figure 3.3:*

**Note: For a Decoupled Authentication challenge, instead of utilising the CReq and CRes messages (Steps 11 through 15 and Step 21), the ACS authenticates the cardholder outside of the EMV 3DS protocol. The Decoupled Authentication flow is portrayed in Figure 3.4 and outlined below.**

### Step 6: The 3DS Server

*Added Note after Req 92:*

**Note: The 3DS Server can use the ACS Start Protocol Version, ACS End Protocol Version, DS Start Protocol Version and DS End Protocol Version obtained from the PRes message to verify that the ACS and DS support the protocol version used by the 3DS Server. In addition, the 3DS Server can use the ACS Information Indicator to identify the features that the Account Range supports (for example, Decoupled Authentication and/or Whitelisting).**

### Step 8 The ACS

*Added Note after Req 103:*

**Note: The ACS uses the Device Information received in the AReq message and the 3DS Method to recognise the device, assess transaction risk, and determine if it can complete the authentication. When Decoupled Authentication is utilised, the consumer's device that initiated the transaction does not need to be supported when the ACS has alternative approaches to authenticating the Cardholder.**

**[Req 106]**

Use the values of the 3DS Requestor Challenge Indicator, the 3DS Requestor Authentication Indicator and the 3DS Requestor Decoupled Requestor Indicator received in the AReq message when evaluating the transaction disposition as defined in [Req 107].

**[Req 107]**

Evaluate the values received in the AReq message and determine whether the transaction is:

- requiring a Cardholder challenge using Decoupled Authentication (Transaction Status = D)
- authentication not requested by the 3DS Server for data sent for informational purposes only (Transaction Status = I)

**[Req 325]**

If a Decoupled Authentication challenge is deemed necessary (Transaction Status = D), the ACS determines whether an acceptable challenge method is supported by the ACS based in part on the following data element received in the AReq message: 3DS Requestor Decoupled Max Time. The ACS performs the following:

a. Sets the Transaction Status = D for Decoupled Authentication.

b. Sets the ACS Decoupled Confirmation Indicator = Y.

c. Stores the 3DS Server Transaction ID and DS Transaction ID (for subsequent RReq processing).

**[Req 326]**

For a Decoupled Authentication transaction, (Transaction Status = D), do the following asynchronous process:

a. Start timer against the 3DS Requestor Decoupled Max Time.

b. Authenticate the cardholder. How an authentication decision is made is outside the scope of this specification, however the ACS objective is to complete the Cardholder authentication before the 3DS Requestor Decoupled Max Time expires.

### Step 9: The DS

**[Req 114]**

Send the ARes message to the 3DS Server ~~as~~ received from the ACS using the secure link established in [Req 100].

### Step 10 The 3DS Server

**[Req 327]**

For a Decoupled Authentication transaction (Transaction Status = D), send necessary information (as defined in Table B.2) from the ARes message to the 3DS Requestor Environment.

**[Req 356]**

If the Cardholder Information Text has been provided by the ACS for this transaction the 3DS Server shall ensure the Cardholder Information Text is displayed on the 3DS Requestor website.

**Note: The next step for:**

- **Decoupled Authentication transaction is Step 16.**

**Note: For a Decoupled Authentication transaction, as defined in [Req 347], the 3DS Server is now expected to wait for the ACS to authenticate the Cardholder at which point in time the ACS will send an RReq message.**

### Step 16 The ACS

*Updated Step introduction (applicable to all requirements in Step):*

The ACS shall for all Challenge Flow transactions (ARes Transaction Status = C) and for a Decoupled Authentication transaction (ARes Transaction Status = D) once the authentication as defined in [Req 326].b has completed or the timer as defined in [Req 326].a has expired, do the following:

**[Req 128]**

Ensure that one RReq message is sent to the DS for each ARes message with a Transaction Status = C or D.~~Send one RReq message to the DS for each ARes message with an ARes Transaction Status = C.~~

**[Req 347]**

Ensure that or a Decoupled Authentication transaction that:

- An RReq message is sent immediately upon obtaining an authentication result (whether successful or not).
- An RReq message without an authentication result is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

### Step 18 The 3DS Server

**[Req 348]**

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 30 seconds for the RReq, If an RReq message is never received, further processing is outside the scope of 3-D Secure processing.

**Note: If the RReq message is not received, then the 3DS Server should assume that the Decoupled Authentication is not successful.**

### Step 20 The ACS

**Note: 3-D Secure processing completes for Decoupled Authentication transactions.**

### Step 21 The ACS

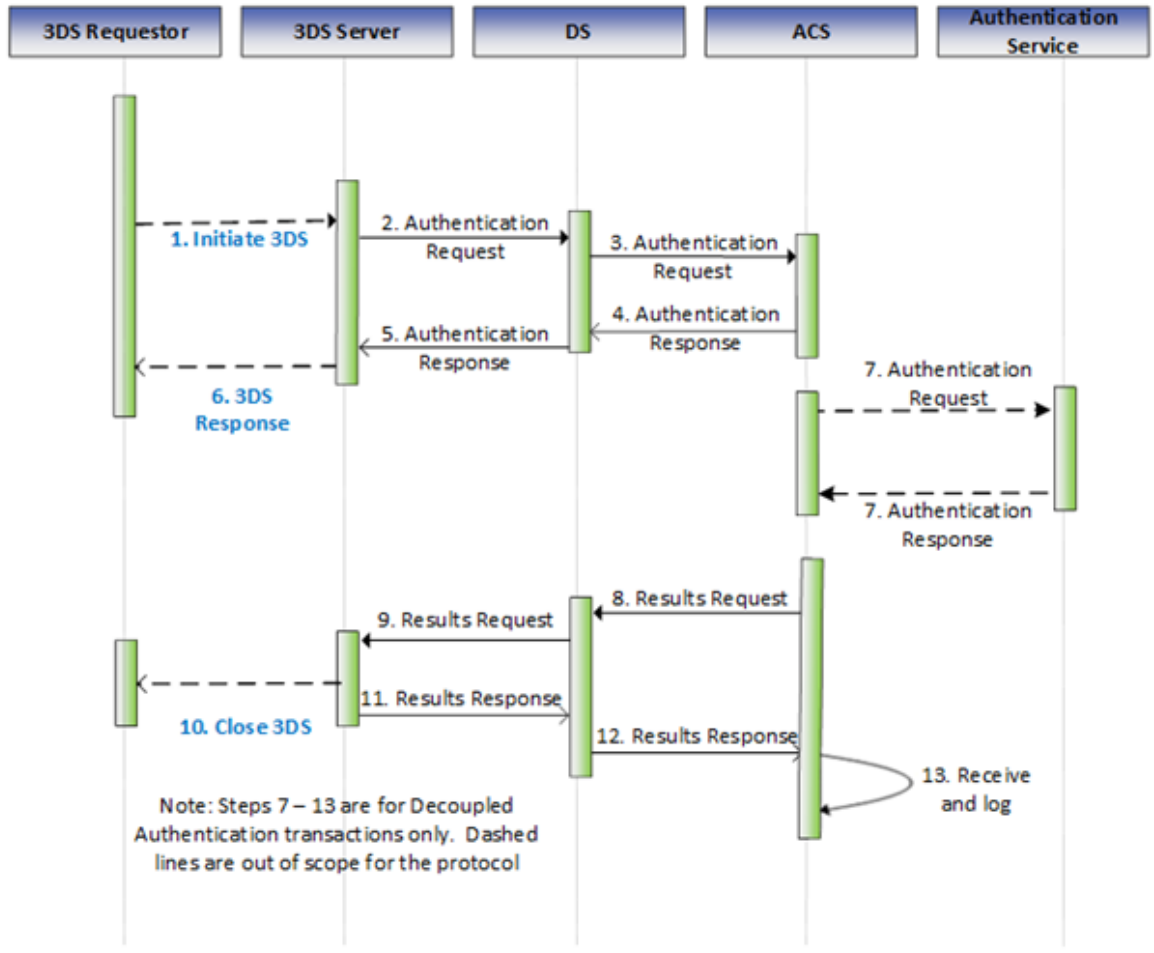
Updated Step introduction (applicable to all requirements in Step):

The ACS shall for a Challenge Flow transaction (ARes Transaction Status = C) ~~(~~as a continuation of receiving the CReq message in Step 11~~)~~: do the following:

## 3.4 3RI-based Requirements

~~3RI-based implementations shall support only Non-Payment Authentication (NPA) transactions.~~The 3RI flow supports two primary main use cases: confirmation of account information (accomplished through Steps 1–6) and Cardholder authentication (accomplished through Steps 1–13).

**Figure 3.4: 3-D Secure Processing Flow Steps—3RI-based (Updated)**




**Note:** Dashed arrows are not part of the 3-D Secure 2.0 protocol but are shown for clarity.

### Step 2: The 3DS Server

*Added Note at end of Step:*

**Note: The 3DS Server can use the ACS Start Protocol Version, ACS End Protocol Version, DS Start Protocol Version and DS End Protocol Version obtained from the PRes message to verify that the ACS and DS support the protocol version used by the 3DS Server. In addition, the 3DS Server can use the ACS Information Indicator to identify the features that the Account Range supports (for example, Decoupled Authentication and/or Whitelisting).**

### Step 4 The ACS

**[Req 290]**

Use the values of the 3RI Indicator, the 3DS Requestor Decoupled Requestor Indicator and the 3DS Requestor Prior Transaction Authentication Information received in the AReq message when evaluating the transaction disposition as defined in [Req 291].

**[Req 291]**

Evaluate the values received in the AReq message and determine whether the 3RI transaction is:

- requiring a Cardholder challenge using Decoupled Authentication (Transaction Status = D)
- authentication not requested by the 3DS Server for data sent for informational purposes only (Transaction Status = I)

**[Req 292]**

If a transaction is deemed authenticated (Transaction Status is = Y or A) then the ACS performs the following:

- For a Payment Authentication (Message Category = 01-PA), the ACS shall:
  - Generate the ECI value and Authentication Value and include in the ARes message as defined by the specific Payment System.

**[Req 328]**

If a Decoupled Authentication challenge is deemed necessary (Transaction Status = D), the ACS determines whether an acceptable challenge method is supported by the ACS based in part on the following data element received in the AReq message: 3DS Requestor Decoupled Max Time. The ACS performs the following:

a. Sets the Transaction Status = D (Decoupled Authentication)

b. Sets the ACS Decoupled Confirmation Indicator = Y

c. Stores the 3DS Server Transaction ID and DS Transaction ID (for subsequent RReq message processing).

### Step 5: The DS

**[Req 297]**

Send the ARes message to the 3DS Server ~~as~~ received from the ACS using the secure link established in [Req 275].

### Step 6 The 3DS Server

**[Req 357]**

If the Cardholder Information Text has been provided by the ACS for this transaction the 3DS Server shall ensure the Cardholder Information Text is conveyed on the 3DS Requestor website.

**Note: 3-D Secure processing completes for non-Decoupled Authentication transactions.**

**Note: For a Decoupled Authentication transaction, as defined in [Req 353], the 3DS Server is now expected to wait for the ACS to authenticate the Cardholder at which point in time the ACS will send an RReq message.**

### Step 7 The ACS

The ACS shall:

**[Req 330]**

For a Decoupled Authentication transaction (Transaction Status = D), do the following:

a. Start a timer against the 3DS Requestor Decoupled Max Time

b. Authenticate the Cardholder. How an authentication decision is made is outside the scope of this specification, however the ACS objective is to complete the Cardholder authentication before the 3DS Requestor Decoupled Max Time expires.

### Step 8 The ACS

The ACS shall for a Decoupled Authentication transaction (initial Transaction Status = D) once the authentication as defined in ***[Req 330].b*** has completed, or the timer as defined in ***[Req 330].a*** has expired, do the following:

The ACS shall:

**[Req 349]**

Format the RReq message as defined in Table B.8.

**[Req 350]**

Establish a secure link with the DS as defined in Section 6.1.3.2.

**[Req 351]**

Send the RReq message to the DS.

**[Req 352]**

Ensure that one RReq message is sent to the DS for each ARes message with a Transaction Status = D.

**[Req 353]**

Ensure that:

- An RReq message is sent immediately upon obtaining an authentication result (whether successful or not).
- An RReq message without an authentication result is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

### Step 9 The DS

The DS shall:

**[Req 332]**

Receive the RReq message from the ACS and Validate as defined in section 5.9.8.

If the message is in error the DS **ends processing**.

**[Req 333]**

Establish a secure link with the 3DS Server as defined in section 6.1.2.2 using the 3DS Server URL extracted from the AReq message.

**[Req 334]**

Send the RReq message to the 3DS Server using the secure link established in [Req 333].

### Step 10 and Step 11 The 3DS Server

The 3DS Server shall:

**[Req 335]**

Receive the RReq message or Error Message from the DS and Validate as defined in section 5.9.9.

If the message is in error, the 3DS Server **ends processing**.

**[Req 336]**

Format the RRes message as defined in Table B.9 and send to the DS using the secure link established in [Req 333].

**[Req 354]**

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 30 seconds for the RReq. If an RReq message is never received, further processing is outside the scope of 3-D Secure processing.

**Note: If the RReq message is not received, then the 3DS Server should assume that the Decoupled Authentication is not successful.**

**[Req 337]**

Convey the appropriate response to the 3DS Requestor.

### Step 12 The DS

The DS shall:

**[Req 338]**

Receive the RRes message or Error Message from the 3DS Server and Validate as defined in section 5.9.10.

If the message is in error the DS **ends processing**.

**[Req 339]**

Log the transaction information as required by the DS.

**[Req 340]**

Send the RRes message to the ACS as received from the 3DS Server using the secure link established in [Req 333].

### Step 13 The ACS

The ACS shall:

**[Req 341]**

Receive and log the RRes message or Error Message from the DS and Validate as defined in section 5.9.11.

If the message is in error the ACS **ends processing**.

**Note: 3-D Secure processing completes.**

# Chapter 4 EMV 3-D Secure User Interface Templates, Requirements, and Guidelines

This chapter provides requirements, template examples, and guidelines for building the User Interface (UI) to support 3-D Secure authentication ~~for both App-based and Browser-based implementations~~.

## 4.1 3-D Secure User Interface Templates

**Note: The user interface provided by the ACS for Decoupled Authentication is outside the scope of the EMV 3-D Secure protocol.**

The 3DS SDK shall:

**[Req 314]**

~~All Device Rendering Options supported shall be supported by the SDK and ACS components.~~ Support all Device Rendering Options.

**[Req 358]**

For the Native UI Type, display UI data elements provided by the ACS within the applicable zones as defined in Table A.18 and depicted in Figure 4.1.

The ACS shall:

**[Req 342]**

Support at least one Native Device Rendering Option and HTML.

**[Req 359]**

For the App-based HTML UI Type and Browser-based UI, create HTML with form ~~UI data~~ elements within the applicable zones as ~~outlined defined in Table A.18 and depicted~~ in Figure 4.1. The ~~expected~~ format is outlined~~depicted~~ in sections 4.2.6 and 4.3.3.

### 4.2.1 Processing Screen Requirements

**[Req 360]**

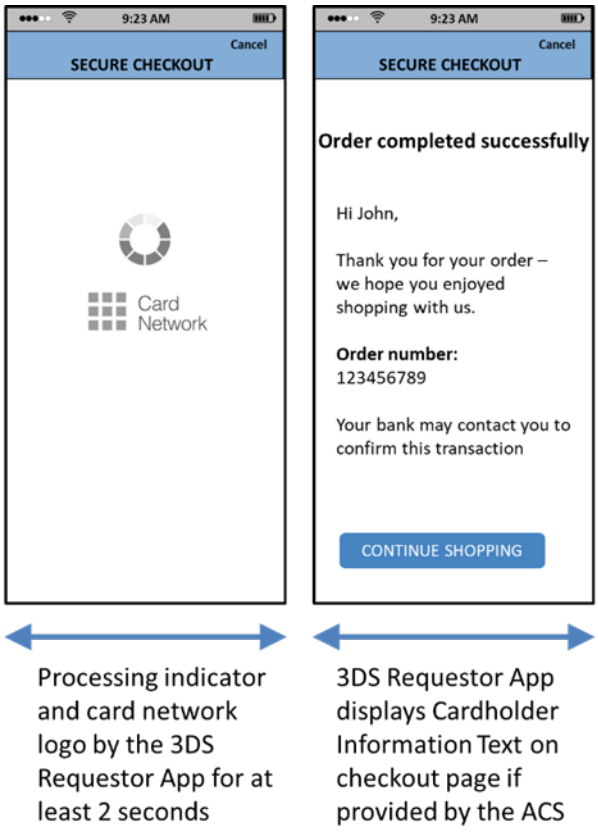
Display the Cancel action in the top ~~right~~ corner of the Header zone.

**[Req 361]**

Display the Cancel action in the top ~~right~~ corner of the Header zone.

*New Figure 4.7. Note subsequent figures were renumbered accordingly.*

**Figure 4.7: Sample Decoupled Authentication Template—App-based Processing Flow**




**Notes:**

- **For Decoupled Authentication, the UI provided by the ACS for cardholder authentication is out of scope of the EMV 3-D Secure specifications.**

### 4.2.1.1 3DS SDK/3DS Requestor App

Figure 4.6 provides a sample format for the Out of Band template and 3DS Requestor App on the same device for an App-based processing flow.

### 4.2.2.1 3DS SDK/ACS

**[Req 362]**

For the ACS UI Type, display the supported UI data elements in their applicable zones and order as defined in Table A.18 and depicted in Figure 4.1. The expected format is depicted in sections 4.2.3 and 4.2.6.

If the SDK receives an unsupported UI data element(s) for this ACS UI Type, the 3DS SDK does not display the UI data elements, proceeds with the challenge and does not send an error message to the ACS.

**[Req 369]**

Display the Cancel action in the top ~~right~~ corner of the header zone as depicted in Figure 4.1.

**[Req 387]**

Only include the UI data elements supported for the selected ACS UI Type as defined in Table A.18.

**Figure 4.6 Sample OOB Template (OOB App and 3DS Requestor App on same device)—App-based Processing Flow**

*Updated Graphic*

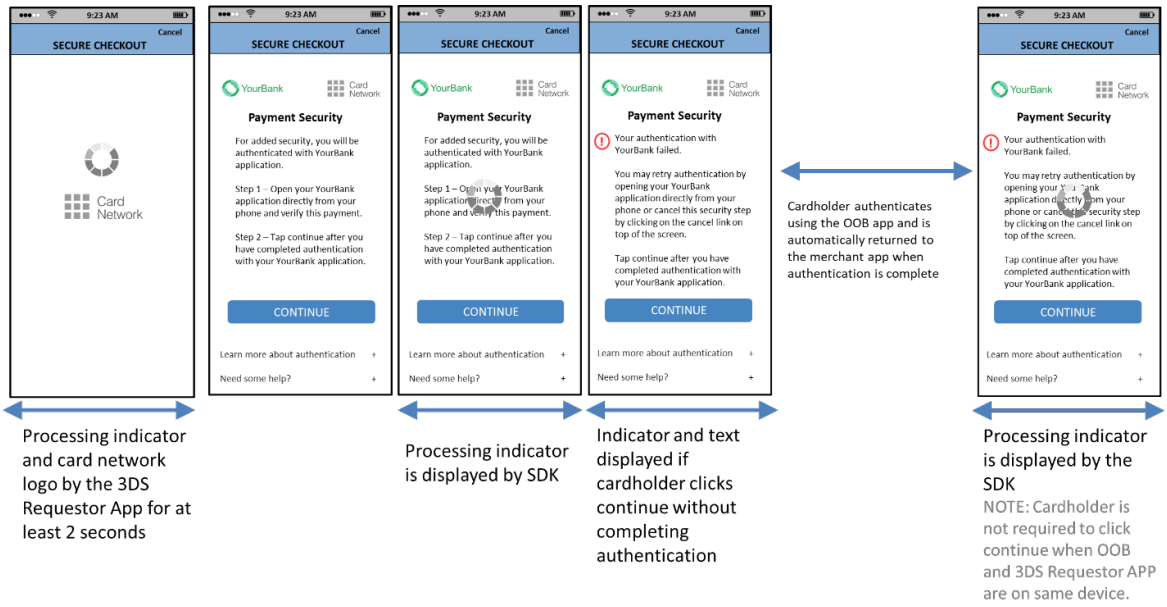
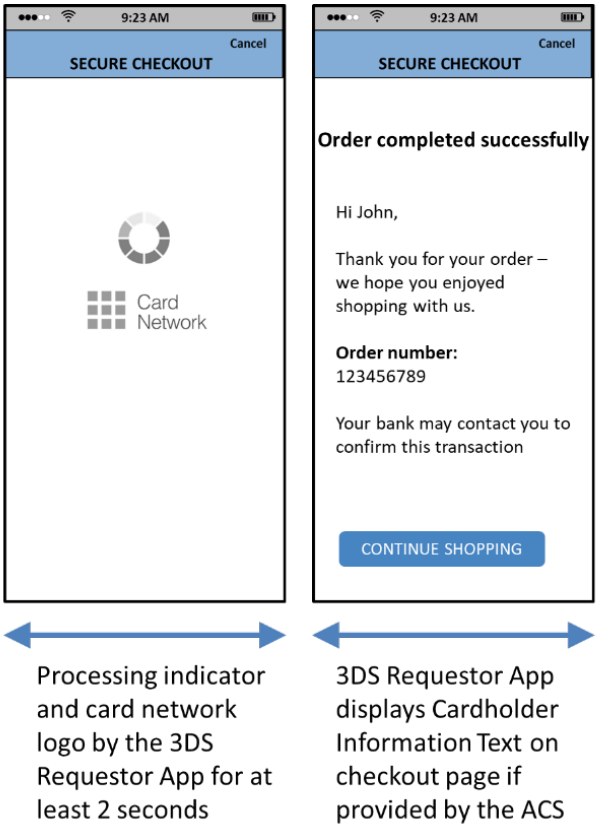



**Figure 4.7 Sample Decoupled Authentication Template—App-based Processing Flow**

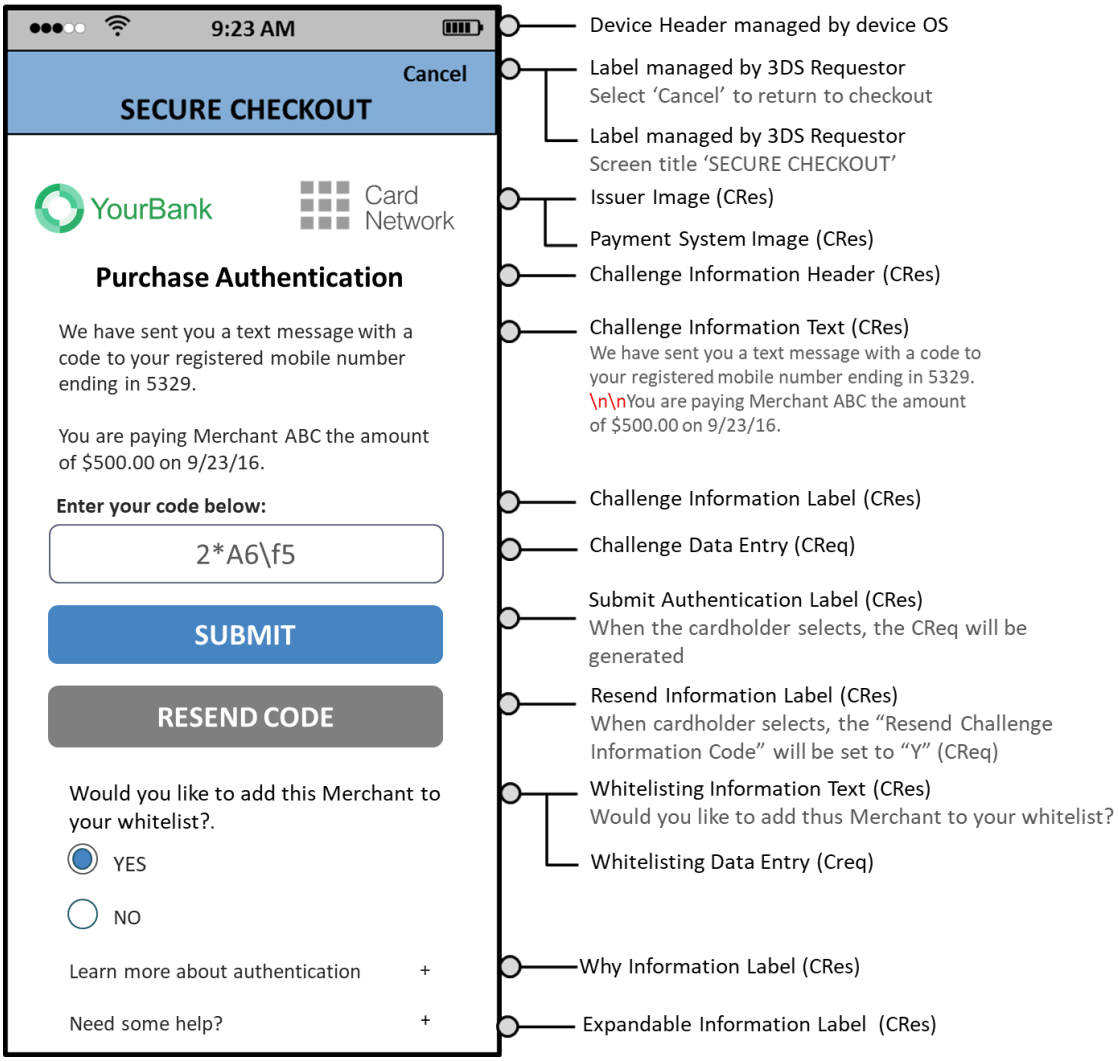
*Updated Graphic*



## 4.2.3 Native UI Templates

**Figure 4.14 Sample ~~Challenge Additional~~Whitelisting Information Text—PA**

*Updated Graphic*




## 4.2.4 Native UI Message Exchange Requirements

**~~[Req 316]~~**

~~When Challenge Additional Information Text is present, the SDK would replace the Challenge Information Text and Challenge Information Text Indicator with the Challenge Additional Information Text when the 3DS Requestor App is moved to the foreground.~~

## 4.2.5.1 3DS SDK/ACS

**[Req 373]**

Display the Cancel action in the top ~~right~~ corner of the header zone as depicted in Figure 4.1.

**[Req 374]**

Create HTML with ~~the UI~~form elements in the applicable zones ~~as defined in Table A.18 and depicted~~ outlined in Figure 4.1. The expected format is ~~depicted~~ outlined in section 4.2.6.

## 4.2.7 HTML Message Exchange Requirements

**~~[Req 317]~~**

~~When the ACS HTML Refresh element is present, the SDK replaces the ACS HTML with the contents of ACS HTML Refresh when the 3DS Requestor App is moved to the foreground.~~

## 4.3.1 Processing Screen Requirements

### 4.3.1.2 The ACS

The ACS shall:

**[Req 177]**

Create and maintain versions of the HTML that correspond to the sizes of the Challenge Window Size data element as defined in Table A.1 and provide the appropriate size in the CRes message based upon the Challenge Window Size that was provided by the 3DS Server in the ~~ARes~~AReq message.

**~~[Req 379]~~**

~~Create HTML with the UI elements in the Branding, Challenge/Processing and Information zones as defined in Table A.18 and depicted in the UI templates in Section 4.3.3~~ .

## 4.3.2 Browser Display Requirements

### 4.3.2.1 ACS

**[Req 380]**

Create HTML with t~~he UI~~form elements in the applicable zones as ~~defined in Table A.18 and depicted~~outlined in Figure 4.1. The ~~expected~~ format is ~~depicted~~ outlined in the UI templates in Section 4.3.3.

### 4.3.3 Browser UI Templates

**Note: For browser-based Decoupled Authentication transactions, the 3DS Requestor website displays the Processing Screen followed by a display of the Cardholder Information Text within the 3DS Requestors checkout page (this is the same as App-based Decoupled transactions, as illustrated in Figure 4.7).**

## 4.4 3RI Considerations

~~3RI transactions do not have a user interface and therefore there are no user interface considerations~~.

The two types of 3RI transactions have different UI considerations. The first type mainly concerns recurrent transactions where the 3DS Requestor wants to verify that a subscription user still has a valid form of payment. As the cardholder is not present, there is no user interface presented for this type of 3RI transaction.

The second type of 3RI transaction is when the 3DS Requestor requests Decoupled Authentication as a method to authenticate the Cardholder, for example, a MOTO transaction. The user interface provided by the ACS for Decoupled Authentication is outside the scope of the EMV 3-D Secure protocol. The 3DS Requestor can optionally display a Processing Screen during AReq/ARes message processing and convey the Cardholder Information Text element if provided by the ACS in the ARes message. For a MOTO transaction, the 3DS Requestor's customer service representative, can covey the Cardholder Information Text verbally for transactions conducted via a land line or feature phone.

# Chapter 5 EMV 3-D Secure Message Handling Requirements

## 5.1.4 Protocol and Message Version Numbers

**[Req 311]**

3DS components shall support all active protocol versions. 3-D Secure messages containing an active Message Version Number supported by the 3-D Secure component ~~are~~shall be processed according to the requirements of the specified protocol version (See Table 1.5).

## 5.1.5 Message Parsing

**[Req 196]**

Message meets applicable ~~technical and security~~ requirements as defined in Annex A~~ and Chapter 6~~.

## 5.1.6 Message Content Validation

**[Req 209]**

If there are additional data elements received that are not specified for the Message Type, Device Channel and Message Category but the message otherwise passes validation, the message shall be considered valid. ~~However, the additional elements (with the exception of data extensions) shall be ignored and shall not be sent to the next 3DS component in the flow.~~

For the additional data elements received (with the exception of data extensions), the receiving 3DS component shall EITHER:

- Ignore the additional data elements and not send them to the next 3DS component in the flow

  OR

- Check the format of the additional data elements:
  - If the format is correct, ignore the additional data elements and do not send them to the next 3DS component in the flow.
  - If the format is incorrect, the receiving 3DS component responds with an error message to the sending 3DS component.

**For Example:**

- The DS receives an AReq message from the 3DS Server with additional data elements that are not specified in Table A.1 for the AReq Message Type, Device Channel and Message Category and the DS validates the AReq content and drops the additional elements when sending the AReq message to the ACS.

  OR

- If the additional data elements in the AReq message do not pass format checking, the DS can respond with an error message to the 3DS Server.

## 5.6 PReq/PRes Message Handling Requirements

**[Req 246]**

3DS Servers shall make a call to each registered DS every 24 hours at a minimum, and once per hour at a maximum to refresh their cache, conditional on no errors found during PRes message processing.

**[Req 303]**

- If the 3DS Server submits more than one request for Card Range Data within one hour, the DS:
  - Returns to the 3DS Server an Error Message (as defined in Section A.5.5) with Error Component = D and Error Code = 103.

### 5.9.3.1 Message in Error

The DS:

If a message is in error and a specific transaction can be identified, the DS sends to the 3DS Server using the secure link established in [Req 12] for an app-based transaction, [Req 90] for a browser-based transaction, or [Req 275] for a 3RI transaction EITHER an:

### 5.9.3.2 Error Message Received

If an error message is received and a specific transaction can be identified, the DS sends to the 3DS Server using the secure link established in [Req 12] for an app-based transaction, [Req 90] for a browser-based transaction, or [Req 275] for a 3RI transaction EITHER an:

## 5.9.11 ACS RRes Message Error Handling—01-APP

- For a message that cannot be recognised, the ACS:
  - If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, the ACS:
- For an RRes message, the ACS Validates the RRes message (as defined in Table B.9 and Section 5.1.6):
  - If any data element present fails validation, the ACS:
    - If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, sends to the 3DS SDK an Error Message (as defined in Section A.5.5) with Error Component = A and Error Code = 203 using the secure link established in [Req 56].
  - If any required data elements are missing, the ACS:
    - If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, sends to the 3DS SDK an Error Message (as defined in Section A.5.5) with Error Component = A and Error Code = 201 using the secure link established in [Req 56].
- For an Error message, if a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, the ACS sends to the 3DS SDK an Error Message (as defined in Section A.5.5) with Error Component = A and Error Code = 403 using the secure link established in [Req 56].

## 5.9.12 ACS RRes Message Error Handling—02BRW

- For a message that cannot be recognised, the ACS:
  - If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, the ACS sends to the 3DS Server (via Browser) a CRes message.
- For an RRes message, the ACS Validates the RRes message (as defined in Table B.9 and Section 5.1.6):
  - If any data element present fails validation, the ACS:

- If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, sends to the 3DS Server (via Browser) a CRes message.

- If any required data elements are missing, the ACS:
  - If a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, sends to the 3DS Server (via Browser) a CRes message.

- For an Error message, if a specific transaction can be identified and the transaction is not a Decoupled Authentication transaction, the ACS sends to the 3DS Server (via Browser) a CRes message.

# Chapter 6 EMV 3-D Secure Security Requirements

### 6.2.2.2 DS Decryption

- Decrypts the SDK Encrypted Data field from the AReq message according to JWE (RFC 7516). The parameter values supported in this version of the specification are:
  - "alg": RSA-OAEP-256
  - If the enc parameter of the JWE in the SDK Encrypted Data field indicates that A128CBC-HS256 was used for encryption:

    "enc": A128CBC-HS256
  - If the enc parameter of the JWE in the SDK Encrypted Data field indicates that A128GCM was used for encryption:

    "enc": A128GCM
  - All other parameters: not present
- Conducts a Diffie-Hellman key exchange process according to JWA (RFC 7518) in Direct Key Agreement mode using curve P-256, QSDK, and dDS to produce a CEK. The parameter values supported in this version of the specification are:
  - If the enc parameter of the JWE in the SDK Encrypted Data field indicates that A128CBC-HS256 was used for encryption:

    "enc": A128CBC-HS256
  - If the enc parameter of the JWE in the SDK Encrypted Data field indicates that A128GCM was used for encryption:

    "enc": A128GCM

# Annex A 3-D Secure Data Elements

- 03-3RI—Deviceless Payment Authentication/Verification of Account

## A.4 EMV 3-D Secure Data Elements

**Table A.1 EMV 3-D Secure Data Elements**

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| 3DS Requestor App URL<br>Field Name: `threeDSRequestorAppURL` | Merchant app declaring their URL within the CReq message so that the Authentication app can call the Merchant app after OOB authentication has occurred. Each transaction would require a unique Transaction ID by using the SDK Transaction ID. | 3DS SDK | Length: Variable, maximum 256 characters<br>JSON Data Type: String<br>Value accepted: Fully Qualified URL<br>Example value:<br>merchantScheme://appName?transID=b2385523-a66c-4907-ac3c-91848e8c0067 | 01-APP | 01-PA<br>02-NPA | CReq = O | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| 3DS Requestor Authentication Method Verification Indicator<br>Field Name: `threeDSReqAuthMethodInd` | Value that represents the signature verification performed by the DS on the mechanism (e.g., FIDO) used by the cardholder to authenticate to the 3DS Requestor. | DS | Length: 2 characters<br>JSON Data Type: String<br>Values accepted:<br>• 01 = Verified<br>• 02 = Failed<br>• 03 = Not Performed<br>• 04–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)<br>• 80–99 = Reserved for DS use | 01-APP<br>02-BRW | 01-PA<br>02-NPA | AReq = C | Conditional based on DS rules. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| 3DS Requestor Challenge Indicator | | | • 05 = No challenge requested (transactional risk analysis is already performed)<br>• 06 = No challenge requested (Data share only)<br>• 07 = No challenge requested (strong consumer authentication is already performed)<br>• 08 = No challenge requested (utilise whitelist exemption if no challenge required)<br>• 09 = Challenge requested (whitelist prompt requested if challenge required)<br>• ~~5~~10–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) | | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| 3DS Requestor Decoupled Max Time<br>Field Name: `threeDSRequestorDecMaxTime` | Indicates the maximum amount of time that the 3DS Requestor will wait for an ACS to provide the results of a Decoupled Authentication transaction (in minutes). | 3DS Server | Length: 5 characters<br>JSON Data Type: String<br>Numeric values between 1 and 10080 accepted. | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | AReq = O | |
| 3DS Requestor Decoupled Request Indicator<br>Field Name:<br>`threeDSRequestorDecReqInd` | Indicates whether the 3DS Requestor requests the ACS to utilise Decoupled Authentication and agrees to utilise Decoupled Authentication if the ACS confirms its use. | 3DS Server | Length: 1 character<br>JSON Data Type: String<br>Values accepted:<br>• Y = Decoupled Authentication is supported and preferred if challenge is necessary<br>• N = Do not use Decoupled Authentication<br>Note: if the element is not provided, the expected action is for the ACS to interpret as N, do not use Decoupled Authentication. | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | AReq = O | |
| 3DS Server URL | | | | 03-3RI | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| 3RI Indicator | | | • 06 = Split/delayed shipment<br>• 07 = Top-up<br>• 08 = Mail Order<br>• 09 = Telephone Order<br>• 10 = Whitelist status check<br>• 11 = Other payment<br>• ~~6~~12–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) | | 01-PA | | |
| ACS Challenge Mandated Indicator | | | | 03-3RI | | | Required if Transaction Status = C or D. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| ACS Decoupled Confirmation Indicator<br>Field Name: acsDecConInd | Indicates whether the ACS confirms utilisation of Decoupled Authentication and agrees to utilise Decoupled Authentication to authenticate the Cardholder. | ACS | Length: 1 character<br>JSON Data Type: String<br>Values accepted:<br>• Y = Confirms Decoupled Authentication will be utilised<br>• N = Decoupled Authentication will not be utilised<br>Note: if 3DS Requestor Decoupled Request Indicator = N, a value of Y cannot be returned in the ACS Decoupled Confirmation Indicator.<br>Note: if Transaction Status = D, a value of N is not valid. | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | ARes = C | Required if Transaction Status = D |
| ACS Rendering Type | | | | | | RReq = ~~R~~C | For RReq, required unless ACS Decoupled Confirmation = Y. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Authentication Method | Note: For 3RI, only present for Decoupled Authentication. | | • 11 = Push Confirmation<br>• 12–79 = Reserved for future EMVCo use (values invalid until defined by EMVCo)<br>• 80–99 = Reserved for ~~future~~ DS use | 03-3RI | | | |
| Authentication Type | | | • 04 = Decoupled<br>• ~~04~~05–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) | | | | Required in the ARes message if the Transaction Status = C or D in the ARes message. |
| Authentication Value | Payment System-specific value provided by the ACS or ~~as part of the ACS~~ DS using an algorithm defined by Payment System.~~registration for each supported DS.~~ | **DS** | | | | | 01-PA:<br>Conditional based on DS rules if Transaction Status = I |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Browser Java Enabled | | | | | | AReq = ~~R~~C | Required when Browser JavaScript Enabled = true; otherwise Optional. |
| Browser JavaScript Enabled<br>Field Name: `browserJavaEnabled` | Boolean that represents the ability of the cardholder browser to execute Javascript.<br>Refer to Section A.5.2 for additional detail. | 3DS Server | JSON Data Type: Boolean<br>Values accepted:<br>• true<br>• false | 02-BRW | 01-PA<br>02-NPA | AReq = R | |
| Browser Screen Color Depth | | | | | | AReq = ~~R~~C | Required when Browser JavaScript Enabled = true; otherwise Optional. |
| Browser Screen Height | | | | | | AReq = ~~R~~C | Required when Browser JavaScript Enabled = true; otherwise Optional. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Browser Screen Width | | | | | | AReq = ~~R~~C | Required when Browser JavaScript Enabled = true; otherwise Optional. |
| Browser Time Zone | Time ~~difference~~ zone offset in minutes between UTC ~~time~~ and the Cardholder browser local time~~, in minutes~~.<br>Note that the offset is positive if the local time zone is behind UTC and negative if it is ahead. | | Length: Variable, 1–5 characters<br>Example time zone offset values in minutes:<br>If UTC -5 hours:<br>• 300<br>• +300<br>If UTC +5 hours:<br>• -300 | | | AReq = ~~R~~C | Required when Browser JavaScript Enabled = true; otherwise Optional. |
| Cardholder Information Text | Text provided by the ACS/Issuer to Cardholder during a Frictionless or Decoupled transaction ~~that was not authenticated by the ACS~~. The Issuer can ~~optionally~~ provide information to Cardholder. | | Note: If field is populated this information ~~can optionally~~ be ~~displayed~~ is required to be conveyed to the cardholder by the merchant. | 3RI | | ARes = ~~O~~C | Required if ACS Decoupled Confirmation Indicator = Y. Otherwise, Optional for the ACS. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Card Range Data | Additionally, identifies the 3DS features the ACS supports, for example, Whitelisting or Decoupled Authentication. | | | ~~01-PA~~<br>~~02--NPA~~<br>N/A | | | |
| Cardholder Billing Address Line 2 | | | | | | | ~~01-PA:~~<br>~~Required unless market or regional mandate restricts sending this information.~~<br>~~02-NPA:~~<br>Required (if available) unless market or regional mandate restricts sending this information. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Cardholder Billing Address Line 3 | | | | | | | ~~01-PA:~~<br>~~Required unless market or regional mandate restricts sending this information.~~<br>~~02-NPA:~~<br>Required (if available) unless market or regional mandate restricts sending this information. |
| ~~Challenge Additional Information Text~~<br>~~Field Name: challengeAddInfo~~ | ~~Text provided by the ACS/Issuer to Cardholder during OOB authentication to replace Challenge Information Text and Challenge Information Text Indicator in the OOB Template.~~ | ~~ACS~~ | ~~Length: Variable, maximum 256 characters~~<br>~~JSON Data Type: String~~<br>~~If field is populated this information is displayed to the Cardholder by the SDK when the 3DS Requestor App is brought to the foreground.~~ | ~~01-APP~~ | ~~01-PA~~<br>~~02-NPA~~ | ~~CRes = O~~ | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Challenge Cancelation Indicator | | | 03 = Transaction Timed Out—Decoupled Authentication~~Reserved for future EMVCo use (values invalid until defined by EMVCo)~~ | 03-3RI | | | |
| Challenge No Entry<br>Field Name: `challengeNoEntry` | Indicator informing that the Cardholder submits an empty response (no data entered in the UI).<br>Note: If present this field contains the value Y. | 3DS SDK | Length = 1 character<br>JSON Data Type = String<br>Value accepted:<br>Y = No Data Entry | 01-APP | 01-PA<br>02-NPA | CReq = C | Required when:<br>• ACS UI Type = 01, 02, or 03, AND<br>• Challenge Data Entry AND<br>• Challenge Cancelation Indicator AND<br>• Resend Challenge Information Code<br>Are not present. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Challenge Selection Information | Example:<br>"challengeSelectInfo": [<br>{"phone": "Mobile **** **** 321"},<br>{"mail": "Emaila*******g**@g***.com"}<br>] | | | | | | |
| Device Rendering Options Supported | Note: As established in [Req 314], all Device Rendering Options must be supported by the SDK ~~and ACS components~~. | | | | | | |
| DS End Protocol Version | | | | ~~01-PA~~<br>~~02—NPA~~<br>N/A | | | |
| DS Start Protocol Version | | | | ~~01-PA~~<br>~~02—NPA~~<br>N/A | | | |
| DS URL | | | | 03-3RI | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Electronic Commerce Indicator (ECI) | Payment System-specific value provided by the ACS or DS to indicate the results of the attempt to authenticate the Cardholder. | DS | | | | | |
| EMV Payment Token Source<br>Field Name: `payTokenSource` | This data element will be populated by the system residing in the 3-D Secure domain where the de-tokenization occurs. | 3DS Server<br>DS | Length: 2 characters<br>JSON Data Type: String<br>Values accepted:<br>• 01 = Directory Server<br>• 02 = 3DS Server<br>• 03-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)<br>• 80-99 = Reserved for DS use | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | AReq = C | Required if EMV Payment Token Indicator = true |
| Instalment Payment Data | | | | 03-3RI | | | |
| OOB App Label | | ~~ACS~~N/A | | | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| OOB App URL | | ~~ACS~~N/A | | | CRes = ~~C~~O | | Note: This element has been defined to support future enhancements to the OOB message flow. An ACS will not provide this value and a 3DS SDK will not perform any processing of the OOB App URL in this version of the specification. |
| Purchase Amount | | | | 03-3RI | | | |
| Purchase Currency | | | | 03-3RI | | | |
| Purchase Currency Exponent | | | | 03-3RI | | | |
| Purchase Date & Time | | | | 03-3RI | | | |
| Recurring Expiry | | | | 03-3RI | | | |
| Recurring Frequency | | | | 03-3RI | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Results Message Status | | | | 03-3RI | | | |
| SDK Transaction ID | | | | | | RReq = R<br>RRes = R | |
| Serial Number | | | Length: Variable, maximum 20 alphanumeric characters | ~~01-APP~~<br>~~02-BRW~~<br>N/A | ~~01-PA~~<br>~~02-NPA~~<br>N/A | | |
| Transaction Status | Note: If the 3DS Requestor Challenge Indicator = 06 (No challenge requested; Data share only), then a Transaction Status of C is not valid. | | • Y = Authentication/ Account Verification Successful<br>• D = Challenge Required; Decoupled Authentication confirmed<br>I = Informational Only; 3DS Requestor challenge preference acknowledged. | | | | ~~For the CRes, only present in the final CRes message.~~<br>See Table A.14 for 01-PA Transaction Status conditions.<br>For 02-NPA, Conditional as defined by the DS.<br>Note: CRes indicates Final CRes. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Transaction Status Reason | | | • 22 = ACS technical issue<br>• 23 = Decoupled Authentication required by ACS but not requested by 3DS Requestor<br>• 24 = 3DS Requestor Decoupled Max Expiry Time exceeded<br>• 25 = Decoupled Authentication was provided insufficient time to authenticate cardholder. ACS will not make attempt<br>• 26 = Authentication attempted but not performed by the cardholder<br>• ~~22~~27–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) | | | | |
| Transaction Type | | | | 03-3RI | | | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Whitelisting Data Entry<br>Field Name: `whitelistingDataEntry` | Indicator provided by the SDK to the ACS to confirm whether whitelisting was opted by the cardholder. | SDK | Length: 1 character<br>JSON Data Type: String<br>Values accepted:<br>• Y = Whitelisting Confirmed<br>• N = Whitelisting Not Confirmed | 01-APP | 01-PA<br>02- NPA | CReq = C | If Whitelisting Information Text was present in the CRes message, SDK must provide this data element to the ACS in the CReq message. |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Whitelisting Information Text<br>Field Name: `whitelistingInfoText` | Text provided by the ACS/Issuer to Cardholder during a Whitelisting transaction.<br>For example, “Would you like to add this Merchant to your whitelist?” | ACS | Length: Variable, maximum 64 characters | 01-APP | 01-PA<br>02- NPA | CRes = O | If present, must be displayed by the SDK. |
| Whitelist Status<br>Field Name: `whiteListStatus` | Enables the communication of trusted beneficiary/whitelist status between the ACS, the DS and the 3DS Requestor. | 3DS Server<br>ACS | Length: 1 character<br>JSON Data Type: String<br>Values accepted:<br>• Y = 3DS Requestor is whitelisted by cardholder<br>• N = 3DS Requestor is not whitelisted by cardholder<br>• E = Not eligible as determined by issuer<br>• P = Pending confirmation by cardholder<br>• R = Cardholder rejected<br>• U = Whitelist status unknown, unavailable, or does not apply<br>Note: valid values in the AReq message are Y or N | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | AReq = O<br>ARes = O<br>RReq = O | |

| Data Element/ Field Name | Description | Source | Length/Format/ Values | Device Channel | Message Category | Message Inclusion | Condition Inclusion |
|---|---|---|---|---|---|---|---|
| Whitelist Status Source<br>Field Name: `whiteListStatusSource` | This data element will be populated by the system setting Whitelist Status. | 3DS Server<br>DS<br>ACS | Length: 2 characters<br>JSON Data Type: String<br>Values accepted:<br>• 01 = 3DS Server<br>• 02 = DS<br>• 03 = ACS<br>• 04-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)<br>• 80-99 = Reserved for DS use | 01-APP<br>02-BRW<br>03-3RI | 01-PA<br>02-NPA | AReq = C<br>ARes = C<br>RReq = C | Required if Whitelist Status is present. |

### A.5.3 3DS Method Data

### 3DS Method Data Examples

- **Example 1:** `threeDSMethodData` to be sent to ACS in the 3DS Method HTTP form POST from 3DS Requestor

```
<form name="frm" method="POST" action="Rendering URL">
<input type="hidden" name="threeDSMethodData"
value="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSIsInRocmVlRFNNZXRob2ROb3RpZmljYXRpb25VUkwiOiJ0aHJlZURTTWV0aG9kTm90aWZpY2F0aW9uVVJMIn0">
</form>

Decoded threeDSMethodData:
{"threeDSServerTransID":"3ac7caa7-aa42-2663-791b-
2ac05a542c4a","threeDSMethodNotificationURL":"threeDSMethodNotificationURL"}
```

- **Example 2:** `threeDSMethodData` to be sent to 3DS Method Notification URL from the ACS

```
<form name="frm" method="POST" action="threeDSMethodNotificationURL">
<input type="hidden" name="threeDSMethodData"
value="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2My03OTFiLTJhYzA1YTU0MmM0YSJ9">
</form>

Decoded threeDSMethodData:
{"threeDSServerTransID":"3ac7caa7-aa42-2663-791b-2ac05a542c4a"}
```

## A.5.5 Error Code, Error Description, and Error Detail

**Table A.4 Error Code, Error Description, and Error Detail**

| Value | Error Code | Error Description | Error Detail |
|---|---|---|---|
| 301 | | | Invalid meaning Transaction ID not recognised, or Transaction ID is recognised as a duplicate. |

## A.5.7 Card Range Data

**Table A.6 Card Range Data**

| Data Element/Field Name | Description | Length/Format/Values | Inclusion |
|---|---|---|---|
| ACS Information Indicator<br>Field Name: `acsInfoInd` | Provides additional information to the 3DS Server. The element lists all applicable values for the card range.<br>Example:<br>{<br>"acsInfoInd":[”01", “02”, “03”, “04”]<br>} | Length: 2 characters<br>JSON Data Type: Array of String<br>String values accepted:<br>• 01 = Authentication Available at ACS<br>• 02 = Attempts Supported by ACS or DS<br>• 03 = Decoupled Authentication Supported<br>• 04 = Whitelisting Supported<br>• 05–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)<br>• 80–99 = Reserved for DS use | O |
| Action Indicator | Note: M (Modify the card range data) is used only to modify or update data associated with the card ranges, not to modify the Start Range and End Range. | • M = Modify the card range data | |

## A.7.3 3DS Requestor Authentication Information

**Table A.10: 3DS Requestor Authentication Information**

| Data Element/Field Name | Description | Length/Format/Values |
|---|---|---|
| 3DS Requestor Authentication Data | • 07, then this element can carry FIDO Attestation data with the FIDO assurance data signed.<br>• 08, then this element can carry the SRC assurance data. | Length: maximum ~~2048~~20,000 characters |
| 3DS Requestor Authentication Method | | • 07 = Login to the cardholder account at the 3DS Requestor system using FIDO Authenticator (FIDO assurance data signed)<br>• 08 = SRC Assurance Data<br>• ~~07~~09–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) |

## A.7.5 ACS Rendering Type

**Table A.12: ACS Rendering Type**

| Data Element/Field Name | Description | Length/Format/Values |
|---|---|---|
| ACS UI Template | Note: HTML Other is the only valid in combination with 02 = HTML UI. If used with 01 = Native UI, the DS will respond with Error = 203 as described in sections 5.9.3 and 5.9.8. | |

## A.7.7 Challenge Data Entry

*New Section and Table. Note: Subsequent Annex A Sections/Tables were renumbered accordingly.*

The Challenge Data Entry (`challengeDataEntry`) contains the data that the Cardholder entered in the Native UI text field. Table A.14 identifies the 3-D Secure message handling when this element is missing, assuming that no other errors are found.

**Table A.14 Challenge Data Entry**

| Challenge Data Entry | ACS UI Type | Challenge Cancelation Indicator | Resend Challenge Information Code | Challenge No Entry | Response |
|---|---|---|---|---|---|
| Missing | 01, 02, or 03 | Missing | Missing | Present<br>• Value = Y | The ACS assumes that the Cardholder has not entered challenge data in the UI and therefore the ACS does not send the 3DS SDK an Error Message, but instead sends a CRes message. |
| Missing | 01, 02, or 03 | Present | Missing | Missing | The ACS sends the 3DS SDK a CRes message. |
| Missing | 01, 02, or 03 | Missing | Present<br>Value = Y | Missing | The ACS sends the 3DS SDK a CRes message. |
| Missing | 01, 02, or 03 | Missing | Present<br>Value = N | Present<br>• Value = Y | The ACS assumes that the Cardholder has not entered challenge data in the UI and therefore the ACS does not send the 3DS SDK an Error Message, but instead sends a CRes message. |
| Missing | 01, 02, or 03 | Present | Present | Present<br>• Value = Y | If at least two of the fields Challenge Cancelation Indicator, Resend Challenge Information Code and/or Challenge No Data Entry are present, the ACS sends the 3DS SDK an Error Message. |

## A.7.8 Transaction Status Conditions

The Transaction Status (`transStatus`) indicates whether a transaction qualifies as an authenticated transaction or account verification. The conditions on which indicators are valid within the 3-D Secure messages are outlined in Table A.15.

**Table A.15: Transaction Status Conditions**

| Transaction Status Indicator | ARes | Final CRes | RReq | Error Response |
|---|---|---|---|---|
| Y = Authentication Verification Successful | Valid | Valid | Valid | Not Applicable |
| N = Not Authenticated /Account Not Verified; Transaction denied | Valid | Valid | Valid | Not Applicable |
| U = Authentication/ Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq | Valid | Invalid | Valid | Final CRes: End processing (no Error) |
| A = Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided | Valid | Invalid | Valid | Final CRes: End processing (no Error) |
| C = Challenge Required; Additional authentication is required using the CReq/CRes | Valid [14] | Invalid | Invalid | Final CRes: End processing (no Error) |
| D = Challenge Required; Decoupled Authentication confirmed | Valid [15] | Invalid | Invalid | • ARes: Refer to section 5.9.3 and use Error Code = 203 if Condition not met<br>• Final CRes: End processing (no Error)<br>• RReq: Refer to section 5.9.8 and use Error Code = 203 |
| R = Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorisation not be attempted. | Valid | Invalid | Valid | Final CRes: End processing (no Error) |

[14] This indicator (C) is not valid if Device Channel = 03 within the AReq message.

[15] This indicator (D) can be sent only if the 3DS Requestor Decoupled Request Indicator = Y within the AReq message.

| Transaction Status Indicator | ARes | Final CRes | RReq | Error Response |
|---|---|---|---|---|
| I = Informational Only; 3DS Requestor challenge preference acknowledged | Valid [16] | Invalid | Invalid | • ARes: Refer to section 5.9.3 and use Error Code = 203 if Condition not met<br>• Final CRes: End processing (no Error)<br>• RReq: Refer to section 5.9.8 and use Error Code = 203 |

*Note: Footnote numbers differ in the actual specification.*

[16] This indicator (I) can be sent only if the 3DS Requestor Challenge Indicator = 05, 06, or 07 within the AReq message.

## A.8 UI Data Elements

Table A.18 specifies the placement of UI data elements on the UI with respect to the zones defined in Section 4.1.

**Table A.18 UI Data Elements**

| Data Element | Field Name | Zone | Top-down Display Order | ACS UI Type | | | |
|---|---|---|---|---|---|---|---|
| | | | | OTP | Single Select | Multi Select | OOB |
| Challenge Information Header | challengeInfoHeader | 3 | 2 | Y | Y | Y | Y |
| Challenge Information Label | challengeInfoLabel | 3 | 4 | Y | Y | Y | N |
| Challenge Information Text | challengeInfoText | 3 | 3 | Y | Y | Y | Y |
| Challenge Information Text Indicator | challengeInfoTextIndicator | 3 | 3 | Y | Y | Y | Y |
| Challenge Selection Information | challengeSelectInfo | 3 | 5 | N | Y | Y | N |
| Expandable Information Label | expandInfoLabel | 4 | 12 | Y | Y | Y | Y |
| Expandable Information Text | expandInfoText | 4 | 13 | Y | Y | Y | Y |
| Issuer Image | issuerImage | 2 | 1 | Y | Y | Y | Y |
| OOB App Label | oobAppLabel | 3 | 5 | N | N | N | N |
| OOB Continuation Label | oobContinueLabel | 3 | 6 | N | N | N | Y |
| Payment System Image | psImage | 2 | 1 | Y | Y | Y | Y |
| Resend Information Label | resendInformationLabel | 3 | 8 | Y | N | N | N |
| Submit Authentication Label | submitAuthenticationLabel | 3 | 7 | Y | Y | Y | N |

| Data Element | Field Name | Zone | Top-down Display Order | ACS UI Type | | | |
|---|---|---|---|---|---|---|---|
| | | | | OTP | Single Select | Multi Select | OOB |
| Whitelisting Information Text | whitelistingInfoText | 3 | 9 | Y | Y | Y | Y |
| Why Information Label | whyInfoLabel | 4 | 10 | Y | Y | Y | Y |
| Why Information Text | whyInfoText | 4 | 11 | Y | Y | Y | Y |

# Annex B Message Format

## B.1 AReq Message Data Elements

### Table B.1 AReq Data Elements

| Data Element | Field Name |
|---|---|
| 3DS Requestor Authentication Method Verification Indicator | threeDSReqAuthMethodInd |
| 3DS Requestor Decoupled Max Time | threeDSRequestorDecMaxTime |
| 3DS Requestor Decoupled Request Indicator | threeDSRequestorDecReqInd |
| Browser JavaScript Enabled | browserJavascriptEnabled |
| EMV Payment Token Source | payTokenSource |
| Whitelist Status | whiteListStatus |
| Whitelist Status Source | whiteListStatusSource |

## B.2 ARes Message Data Elements

### Table B.2 ARes Data Elements

| Data Element | Field Name |
|---|---|
| ACS Decoupled Confirmation Indicator | acsDecConInd |
| Whitelist Status | whiteListStatus |
| Whitelist Status Source | whiteListStatusSource |

## B.3 CReq Message Data Elements

### Table B.3 CReq Data Elements

| Data Element | Field Name |
|---|---|
| 3DS Requestor App URL | threeDSRequestorAppURL |
| Challenge No Entry | challengeNoEntry |
| Whitelisting Data Entry | whitelistingDataEntry |

## B.4 CRes Message Data Elements

**Table B.4 CRes Data Elements**

| Data Element | Field Name |
|---|---|
| ~~ACS HTML Refresh~~ | ~~acsHTMLRefresh~~ |
| ~~Challenge Additional Information Text~~ | ~~challengeAddInfo~~ |
| Whitelisting Information Text | whitelistingInfoText |

## B.8 RReq Message Data Elements

**Table B.8 RReq Data Elements**

| Data Element | Field Name |
|---|---|
| SDK Transaction ID | sdkTransID |
| Whitelist Status | whiteListStatus |
| Whitelist Status Source | whiteListStatusSource |

## B.9 RRes Message Data Elements

**Table B.9 RRes Data Elements**

| Data Element | Field Name |
|---|---|
| SDK Transaction ID | sdkTransID |

# Annex D Approved Transport Layer Security Versions

### D.1.1 Cipher Suites for TLS 1.2

Curve P-256 shall be used and indicated in the cipher suite extension.

# Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. 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 THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications 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 the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications 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 these Specifications 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 the EMV® Specifications