EMV® Specification Bulletin No. 294

May 2023

EMV® 3-D Secure Protocol and Core Functions Specification v2.3.1.1

This Specification Bulletin No. 294 provides the updates, clarifications and errata incorporated into the EMV® 3-D Secure Protocol and Core Functions Specification since version 2.3.1.0.

Applicability

This Specification Bulletin applies to:

- *EMV® 3-D Secure Protocol and Core Functions Specification, Version 2.3.1.1*

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.

Related Documents

EMV® 3-D Secure Protocol and Core Functions Specification, Version 2.3.1.0

Effective Date

- *May 2023*

Contents

Throughout Specification

Revisions added to improve grammar, consistency, clarity and readability without any effect on the meaning or interpretation of the specification are not included in this bulletin.

Chapter 1 Introduction

1.5 Definitions

Table 1.3 Definitions

Term	Definition
Decoupled Authentication Fallback	By returning Transaction Status = D in the RReq message, the ACS requests that the 3DS Server initiate a subsequent 3DS authentication ~~with~~using Decoupled Authentication ~~supported~~.
Ends processing	In the 3-D Secure processing flow, this indicates that an error has been found by a specific 3-D Secure component, which reports the error via the appropriate Error Message as defined in Section ~~A.5.5~~A.9 or RReq message as defined in Table B.8.
Universal App Link	~~Standard~~Operating System-registered HTTPS links for opening a specific mobile app, installed on a device. The implementation is platform-specific.

Chapter 3 EMV 3-D Secure Authentication Flow Requirements

3.1 App-based Requirements

Step 8: The DS

The DS shall:

[Req 421]

If the DS creates the ARes message on the ACS's behalf (for example, the DS returns a Transaction Status = A), then the DS sets the ACS Reference Number equal to the DS Reference Number and the ACS Transaction ID equal to the DS Transaction ID and all the other ACS data elements required in the ARes message according to the DS capabilities.

Step 17: The ACS

The ACS shall:

[Req 61]

Check the data received in the CReq message and assess the status of the authentication.

- If the ACS selects Decoupled Authentication Fallback, then the ACS continues with Step 18.

The remainder of Requirement 61 is unchanged.

Step 23: The ACS

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 470]

If 3DS Requestor Decoupled Request Indicator = F or B and if Transaction Status = D in the RReq message, set Transaction Status to D in the Final CRes message.

3.2 Challenge Flow with OOB Authentication Requirements

3.2.1 OOB Requirements

Step 15: The Cardholder Interaction with the 3DS SDK

[Req 400]

For ACS UI Type = 04 or 06, if the 3DS Requestor App comes to the foreground (for example, the Cardholder returns to the 3DS Requestor App that comes to the foreground), set the value of the OOB Continuation Indicator = 02, and continue automatically (without UI interaction by the Cardholder) with Step 16 in the App-based flow (send a CReq message to the ACS).

3.2.2 OOB Automatic Switching Features

Step 13: The ACS

[Req 402]

For ACS UI Type = 06, include in the OOB challenge HTML code an action that triggers a location change to the `HTTPS://EMV3DS/openoobApp` URL when the Cardholder selects the OOB App URL button.

3.2.2.1 OOB App URL Requirements

[Req 472]

Check that the OOB App URL uses the HTTPS scheme.

If not, the 3DS SDK returns an error as defined in Section 5.9.7.

3.2.2.2 3DS Requestor App URL

When the OOB Authentication App invokes the 3DS Requestor App URL, the device OS switches to the 3DS Requestor App that moves to the foreground. The 3DS Requestor App transfers the control back to the 3DS SDK.

[Req 475]

When receiving the CReq message, the ACS shall check that the 3DS Requestor App URL uses the HTTPS scheme.

If not, the ACS returns an error as defined in Section 5.9.5.

3.3 Browser-based Requirements

Step 9: The DS

The DS shall:

[Req 411]

If the DS creates the ARes message on the ACS's behalf (for example, the DS returns a Transaction Status = A), then set the ACS Reference Number equal to the DS Reference Number and the ACS Transaction ID equal to the DS Transaction ID and all the other ACS data elements required in the ARes message according to the DS capabilities.

Step 10: The 3DS Server

The 3DS Server shall:

[Req 117]

For a transaction with a challenge (Transaction Status = C):

e. ~~Pass~~Send the CReq message using an HTTP POST through the Cardholder Browser HTML iframe as defined in Section 5.8.2 and Section A.8 (Browser CReq and CRes POST) to the ACS URL received in the ARes message, ~~by causing the Cardholder Browser to POST the form to the ACS URL~~ using a server-authenticated TLS link as defined in Section 6.1.4.2.

Step 11: The ACS

The ACS shall:

[Req 119]

Receive the CReq message from the Browser:

- Accept a Base64url-encoded CReq message with or without padding,
- Validate the message as defined in Section 5.9.6,
- Accept the Base64url-encoded Session Data with or without padding.

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

Step 13: The Cardholder

The Cardholder interacts with the UI provided by the ACS and, if requested, enters the authentication data ~~as required by the ACS UI~~.

Step 14: The Browser

The Browser sends the entered ~~authentication~~ data to the ACS over the channel established by the HTTP POST in Step 10.

Step 15: The ACS

The ACS shall:

[Req 464]

If the ACS determines that Decoupled Authentication Fallback is necessary and 3DS Requestor Decoupled Request Indicator = F or B, inform the Cardholder of Decoupled Authentication ~~in~~before the Final CRes message using the Information UI template as defined in Chapter 4.

[Req 123]

Check the authentication data received and assess the status of the authentication:

- If the ACS selects Decoupled Authentication Fallback, then the ACS continues with Step 16.

The remainder of Requirement 123 is unchanged.

Step 16: The ACS

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 465]

For a Challenge Flow (ARes Transaction Status = C), if 3DS Requestor Decoupled Request Indicator = F or B, and if the ACS has determined that Decoupled Authentication Fallback is necessary,

- ~~s~~Set Transaction Status = D.
- Set Transaction Status Reason = 29 or 30.

Step 21: The ACS

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:

[Req 471]

If 3DS Requestor Decoupled Request Indicator = F or B and if Transaction Status = D in the RReq message, set Transaction Status to D in the Final CRes message.

3.4 3RI-based Requirements

Step 2: The 3DS Server

The 3DS Server shall:

[Req 467]

In the case of Decoupled Authentication Fallback, the 3DS Server initiates a 3RI authentication within 60 seconds of receiving the RReq message from the previous transaction, containing:

- 3RI Indicator = 19 (Decoupled Authentication Fallback)
- 3DS Requestor Decoupled Request Indicator = Y
- 3DS Requestor Prior Transaction Authentication Information object:

- 3DS Requestor Prior Transaction Reference = ACS Transaction ID from the RReq message indicating that Decoupled Authentication is to be performed
- 3DS Requestor Prior Transaction Authentication Method = 02 (Cardholder challenge occurred by ACS).

Step 5: The DS

The DS shall:

[Req 412]

If the DS creates the ARes message on the ACS's behalf (for example, the DS returns a Transaction Status = A), then the DS sets the ACS Reference Number equal to the DS Reference Number and the ACS Transaction ID equal to the DS Transaction ID and all the other ACS data elements required in the ARes message according to the DS capabilities.

3.5 SPC-based Authentication Requirements

[The following note was added at the end of section introduction.]

Note: The DS may act as the FIDO Relying Party and perform some or all of the actions described for the ACS within the SPC flow.

3.5.1 3DS Requestor Initiates SPC Authentication

Step 8

The ACS recognises that SPC-based authentication is supported.

[The note at the end of Step 8 was deleted.]

~~**Note: Depending on implementation, it is possible that the DS performs the functions described in Step 8 on behalf of the ACS. In such cases, the data are provided by the DS to the ACS in Step 7 and to the 3DS Server in Step 9.**~~

Step 10f: The DS

[Req 451]

If the DS evaluates the Assertion Data on behalf of the ACS, the DS shall include the verification result in the ~~3DS Requestor Authentication Method Verification Indicator~~ corresponding DS Authentication Information Verification Indicator.

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

4.1 3-D Secure User Interface Templates

The ACS shall:

[Req 342]

Support all ACS Rendering Types for the ACS supported authentication methods, at a minimum at least one ACS UI Template for each ACS Interface in addition to the Information UI template.

4.2 App-based User Interface Overview

4.2.4 Native UI Message Exchange Requirements

4.2.4.3 3DS SDK

New Requirement 473 (originally Requirement 71 in the EMV® 3-D Secure SDK Specification, which has now been deleted) was added directly after Requirement 158.

[Req 473]

If the Cardholder does not enter any data in the UI, send the Challenge No Entry field with the value = Y in the CReq message.

4.2.7 HTML Message Exchange Requirements

4.2.7.3 3DS SDK

New Requirement 474 (originally Requirement 75 in the EMV® 3-D Secure SDK Specification, which has now been deleted) was added directly after Requirement 393.

[Req 474]

When the Cardholder submits their response, if the 3DS SDK receives a blank response, then it assumes that the HTML is not valid. In this event, the 3DS SDK shall return to the ACS an Error Message (as defined in Section A.9) with Error Component = C and Error Code = 203.

Chapter 5 EMV 3-D Secure Message Handling

5.1 General Message Handling

5.1.2 HTTP Header—Content-Type

[Req 191]

The Content-Type Header requirements for CReq/CRes are:

- For Browser-based CRes, the HTTP headers shall contain the Content-Type Header: text/html and include charset of UTF-8.

  For example, Content-Type: text/html~~:~~; charset = UTF-8.

[Req 469]

For the ARes, CRes, RRes, ORes or PRes messages, the 3DS component sending the message shall include its own Transaction ID using X-Response-ID and the ~~X-Request-ID~~sender Transaction ID received in the Request message (not in the HTTP header) using the X-Request-ID, as defined in Table A.29.

5.1.4 Protocol and Message Version Numbers

Note: Protocol and Message Version Numbers are in the format: major.minor.patch (for example, 2.3.0~~0~~1).

5.5 Timeouts

5.5.1 Transaction Timeouts

[Req 455]

If the timeout expires before receiving the Assertion Data from the 3DS Requestor, send the second AReq message to the ACS with SPC Incompletion Indicator = 03 and without the 3DS Requestor Authentication Information.

5.5.2 Read Timeouts

5.5.2.2 RReq/RRes Message Timeouts

The ACS:

[Req 242]

If the DS has not responded with the RRes message or an Error message before the read timeout expiry, the ACS shall return to the DS an Error Message (as defined in Section ~~A.5.5~~A.9) with Error Component = A and Error Code = 402. The default timeout value is 5 seconds. However, a DS may specify a higher alternative value.

5.8 Browser-based Message Handling

5.8.1 3DS Method Handling

5.8.1.1 Recent Prior 3DS Method Call Does Not Exist

The ACS shall:

[Req 263]

~~Recall~~Validate the Base64url-encoded `threeDSMethodData` with or without padding from the initial 3DS POST method, and retrieve the 3DS Server Transaction ID ~~received in the initial 3DS method POST~~, then Base64url-encode the JSON object and send via a form with a field named `threeDSMethodData` in the Cardholder Browser HTML iframe using an HTTP POST method to the 3DS Method Notification URL. Refer to Table A.2 for detailed information about 3DS Method Data.

5.11 OReq/ORes Message Handling Requirements

Note: ~~If there is more than one OReq message in the message~~ In case of a sequence of OReq messages, the DS sends all the OReq messages and the ~~OReq recipient repeat~~ ACS responds with a single ORes message after receiving all the ~~previous steps starting from [Req 435]~~ OReq messages.

Annex A 3-D Secure Data Elements

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 Authentication Information		DS		03-3RI			
~~3DS Requestor Authentication Method Verification Indicator~~ ~~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~~ ~~JSON Data Type: String~~ ~~Values accepted:~~ • ~~01 = Verified~~ • ~~02 = Failed~~ • ~~03 = Not performed~~ • ~~04–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)~~ • ~~80–99 = Reserved for DS use~~	~~01-APP~~ ~~02-BRW~~ ~~03-3RI~~	~~01-PA~~ ~~02-NPA~~	~~AReq = C~~	~~Conditional based on DS rules.~~ ~~The DS populates the AReq with this data element prior to passing to the ACS.~~
3RI Indicator			• 17 = FIDO credential deletion • 18 = FIDO credential registration				

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
			• 19 = Decoupled Authentication Fallback • 20–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)				
Acquirer BIN			• This value correlates to the Acquirer BIN as defined by each Payment System ~~or DS~~.				
ACS HTML			Length: Variable, maximum ~~300 kB~~300000 characters				
ACS Signed Content			Length: Variable, maximum 16000 characters				
Authentication Method			• 16 = Electronic ID • 17–79 = 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
Browser Screen Color Depth			~~For a list of possible values, refer https://www.w3schools.com/jsref/prop_screen_colordepth.asp~~				
Challenge Additional Code	Note: If present, this field contains the value Y.		Value~~s~~ accepted: • Y = Additional choice selected • ~~N = Additional choice not selected~~				Required for Native UI: • if the Challenge Additional Label was present in the CRes message AND • if ~~the ACS offers~~ the Challenge A~~a~~dditional choice ~~button~~is selected.
Challenge Data Entry	Example: "challengeSelectInfo":[{"phon~~e~~":"Mobile **** **** 321"}, {"mail":"Email a*******g**@g***.com"}]						

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
	The Cardholder selects the phone option: "challengeDataEntry":"phone"						
Challenge Information Text Indicator			Length: 1 character				
Challenge Selection Information	Example: "challengeSelectInfo":[{"phone":"Mobile **** **** 321" }, {"mail":"Email a******g**@g***.com"}]		~~Length~~Key length: Variable, maximum 4 characters Value length: Variable, maximum 45 characters				
Device Binding Data Entry							Required if: • Device Binding Information Text was present in the previous CRes message AND

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
							• Challenge Cancelation Indicator is not present.
DS URL List			Size: Variable, 1–~~10~~99 elements				
Information Continuation Indicator							Required for ACS UI Type = 07 if the Cardholder selects the Information Continuation button on the device.
Issuer Image							~~Absent for ACS UI Type = 05 and 06.~~
Message Version Number			Example: • 99.99.99~~.~~				
OOB App Label							• ~~Required if the OOB App URL is available and ACS UI Type = 04.~~ Only present for ACS UI Type = 04 if:

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
							• OOB App URL Indicator = 01 in the CReq message AND • the ACS uses the OOB Authentication App automatic switching feature for this transaction.
OOB App Status			Length: ~~Variable, maximum~~ 2 characters				
OOB App URL							~~Required~~ Only present for [ACS UI Type = 04 if the OOB App Label is present OR ACS UI Type = ~~or~~ 06] AND if: • OOB App URL Indicator = 01 in the CReq message;

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
							AND • the ACS uses the OOB Authentication App automatic switching feature for this transaction
OOB App URL Indicator			Length: ~~Variable, maximum 48~~2 characters				
OOB Continuation Indicator							Required if: • ACS UI Type = 04~~; OR~~ ~~ACS UI Type – 06 when the 3DS SDK sends a CReq message~~ unless Challenge Additional Code is present; OR • ACS UI Type = 06 ~~= Y.~~

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
OOB Continuation Label							Required for ACS UI Type = 04 if ~~the ACS utilises OOB manual switching~~the OOB App Label is not present.

Operation Prior Transaction Reference			For example, a prior DS Transaction ID would be represented as:
			`"opPriorTransRef":~~{~~`
			`{`
			`"transIdType":"02",`
			`"transId":"4317fdc3-ad24-5443-8000-000000000891"`
			`}`
			`~~}~~`				

Payment System Image							~~Absent for ACS UI Type = 05 and 06.~~
Purchase Currency Exponent	• ~~Yen~~JPY = 0						

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
SDK App ID	Note: In case of ~~Browser-SDK~~Split-SDK/Browser, the SDK App ID value is not reliable, and may change for each transaction.						
SPC Transaction Data			Note: For NPA, Amount is set to 0 and Currency is set to any valid value.				
Transaction Challenge Exemption	~~Note: The accepted values match the values of the 3DS Requestor Challenge Indicator.~~						
Transaction Status	The Final CRes message can only contain a value of Y or N or D.						
Trust List Data Entry							Required if: • Trust List Information Text was present in the previous CRes message AND

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
							• Challenge Cancelation Indicator is not present.

A.7 3DS Method Data

Clarification was added in the introduction to correct a typographical error.

The data is exchanged between the 3DS Requestor and the ACS via the Cardholder Browser.

A.8 Browser CReq and CRes POST

Table A.3: 3DS CReq/CRes POST Data

Data Element / Field Name	Description	Recipient	Length/Format/Values	Message Inclusion
3DS Requestor Session Data			Length: Variable, maximum 1024 characters	

Browser CReq–CRes Data Examples

Example 1

```
CReq message
{
     "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
     "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
```

```
      "threeDSRequestorURL":"https://merchant.com/url",
      "messageType":"CReq",
      "messageVersion":"2.3.01"
}
```

Example 2

```
CRes message
{
      "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
      "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
      "transStatus":"Y",
      "messageType":"CRes",
      "messageVersion":"2.3.01
}
```

A.9 Error Code, Error Description, and Error Detail

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

Value	Error Code	Error Description	Error Detail
313		An RReq message is received although there was no challenge (Transaction Status not equal to C or D or S) for this transaction.	The ACS sends an RReq message but the Transaction Status in the corresponding ARes message was not = C or D or S.

A.10 Excluded ISO Currency and Country Code Values

Table A.5: Excluded Currency Code and Country Code Values

ISO Code	Numeric ~~V~~value not permitted for 3-D Secure	Alphabetic value not permitted for 3-D Secure	Definition
ISO 4217	955	XBA	European Composite Unit
ISO 4217	956	XBB	European Monetary Unit
ISO 4217	957	XBC	European Unit of Account 9
ISO 4217	958	XBD	European Unit of Account 17
ISO 4217	959	XAU	Gold
ISO 4217	960	XDR	I.M.F.
ISO 4217	961	XAG	Silver
ISO 4217	962	XPT	Platinum

ISO Code	Numeric ~~V~~value not permitted for 3-D Secure	Alphabetic value not permitted for 3-D Secure	Definition
ISO 4217	963	XTS	Reserved for testing
ISO 4217	964	XPD	Palladium
ISO 4217	999	XXX	No currency is involved
ISO 3166-1	901–999		Reserved by ISO to designate country names not otherwise defined

A.11 Card Range Data

Table A.6: Card Range Data

Data Element/Field Name	Description	Length/Format/Values	Inclusion
Supported Message Extension		Size: Variable, 1–~~10~~15 elements	

Card Range Data Example

```
{"cardRangeData": [
                    {"ranges": [
     {"start": "1000000000000000",
      "end": "1000000000005000"},
     {"start": "1000000000006000",
      "end": "1000000000007000"}
                     ],
                    "actionInd": "A",
                    "issuerCountryCode": "356",
                    "dsProtocolVersions": ["2.2.0","2.3.0","2.3.1"],
                    "acsProtocolVersions": [
     {"version": "2.2.0",
     "acsInfoInd": ["01", "02"],
     "threeDSMethodURL": "https://www.acs.com/script1",
     "supportedMsgExt": [
          {"id": "A000000802-001","version": "2.0"},
          {"id": "A000000802-004","version": "1.0"}
     ]},
     {"version": "2.3.0",
     "acsInfoInd": ["01", "02", "03", "04", "80"],
     "threeDSMethodURL": "https://www.acs.com/script2"
     }
```

```
      {"version": "2.3.1",
      "acsInfoInd": ["01", "02", "03", "04", "81"],
      "threeDSMethodURL": "https://www.acs.com/script3"
      }
                          ]
                      }
                  ]
}
```

The DS URL List data element contains information returned in a PRes message to the 3DS Server from the specific DS that contains the list of URLs that the 3DS Server can use to communicate with a DS.

The 3DS Server replaces the previous DS URL List with the latest received in the PRes message. If the DS URL List is absent from the PRes message, the 3DS Server deletes all existing DS URLs.

Its JSON Data Type: Array of objects contains:

- the 3DS Server to DS URL
- the DS Country Code (optional)

Table A.7: DS ~~URLs~~URL List

Data Element/Field Name	Description	Length/Format/Values	Inclusion
3DS Server to DS URL			~~O~~R

A.13 3DS Requestor Risk Information

A.13.2 Merchant Risk Indicator

Table A.11: Merchant Risk Indicator

Data Element/Field Name	Description	Length/Format/Values
Transaction Characteristics Field Name: `transChar`	Indicates to the ACS specific transactions identified by the Merchant.	Size: Variable, 1–2 elements JSON Data Type: Array of string String: 2 characters Value accepted: 01 = Cryptocurrency transaction 02 = NFT transaction

A.13.3 3DS Requestor Authentication Information

Table A.12: 3DS Requestor Authentication Information

Data Element/Field Name	Source	Description	Length/Format/Values
3DS Requestor Authentication Data	3DS Server		Length: Variable, m~~M~~aximum ~~20000~~50000 characters
3DS Requestor Authentication Method	3DS Server		• 10 = Electronic ID Authentication Data • 11–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)

Data Element/Field Name	Source	Description	Length/Format/Values
3DS Requestor Authentication Timestamp	3DS Server		
DS Authentication Information Verification Indicator Field Name: dsAuthInfVerifInd	DS	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. The DS populates this data element prior to passing to the ACS.	Length: 2 characters JSON Data Type: String Values accepted: • 01 = Verified • 02 = Failed • 03 = Not performed • 04–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use

A.13.7 Challenge Data Entry

Table A.16: Challenge Data Entry

Challenge Data Entry	ACS UI Type	Challenge Cancelation Indicator	Resend Challenge Information Code	Challenge Additional Code	Challenge No Entry	Response
~~Missing~~	~~01, 02, or 03~~	~~Missing~~	~~Missing~~	~~Present~~ • ~~Value = N~~	~~Present~~ • ~~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.~~

A.13.8 Transaction Status Conditions

Table A.17: Transaction Status Conditions

Transaction Status	ARes	Final CRes	RReq	Error Response
D = Challenge Required; Decoupled Authentication confirmed	Valid[10]	~~Invalid~~Valid[11]	Valid[11]	• ARes: Refer to Section 5.9.3 and use Error Code = 203 if Condition not met • Final CRes: ~~End processing (no Error):~~ Not applicable • RReq: Refer to Section 5.9.8 and use Error Code = 203 if Condition not met

Footnote 11: This indicator (D) can be sent only if 3DS Requestor Decoupled Request Indicator = F or B within the AReq message.

A.14 UI Data Elements

Table A.20: UI Data Elements

Data Element / Field Name	Zone	Display Order (Top-down)		ACS UI Type				
		Portrait	Landscape	01 = Text	02 = Single Select	03 = Multi Select	04 = OOB	07 = Information
Information Continuation Label		~~11~~10						
OOB App Label		~~10~~9						
OOB Continuation Label		~~11~~10						
Resend Information Label		~~11~~10						

Data Element / Field Name	Zone	Display Order (Top-down)		ACS UI Type				
		Portrait	Landscape	01 = Text	02 = Single Select	03 = Multi Select	04 = OOB	07 = Information
Submit Authentication Label		~~10~~9						
Trust List Information Text		~~8~~7 or ~~13~~12						
Why Information Label		~~15~~14						
Why Information Text		~~16~~15						

Note: The data elements listed in Table A.20 are not needed for ACS UI Type = 05 and 06 (HTML and HTML OOB template).

A.21 SPC Transaction Data

Table A.28: SPC Transaction Data

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Currency			Length: 3 characters, alphabetic Values accepted: • ISO 4217 three-~~digit~~character alphabetic currency code~~s~~, other than those listed in Table A.5.	

Annex B Message Format

B.1 AReq Message Format

Table B.1: AReq Data Elements

Data Element	Field Name
~~3DS Requestor Authentication Method Verification Indicator~~	~~threeDSReqAuthMethodInd~~

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