EMV® Specification Bulletin No. 214 v1
June 2019

EMV® 3-D Secure Updates, Clarifications & Errata

This Draft Specification Bulletin No. 214 v1 provides updates, clarifications and errata incorporated into the EMV 3-D Secure Protocol and Core Functions Specification since version 2.2.0.

Applicability

This Draft 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.

Effective Date

June 2019

Contents

Chapter 1 Introduction

1.5 Definitions

Table 1.3 Definitions

Term	Definition
Directory Server ID (`directoryServerID`)	Registered Application Provider Identifier (RID) that is unique to the Payment System. RIDs are defined by the ISO 7816-5 standard. The Directory Server ID is a hex value encoded as a 10-character text. For example, 0x'A000000003' is encoded as 'A000000003'.

Chapter 3 EMV 3-D Secure Authentication Flow Requirements

3.1 App-based Requirements

The 3DS Server shall:

[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~~App.

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 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 (Transaction Status = U) is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

  Note: It is recommended that an RReq message with Transaction Status = U contains Transaction Status Reason = 24 or 26 and Challenge Cancelation Indicator = 03.

The 3DS Server shall:

[Req 346]

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 1 hour, 30 seconds for the RReq message. If an RReq message is never received, further processing is outside the scope of 3-D Secure processing.

3.3 Browser-based Requirements

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 347]

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 (Transaction Status = U) is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

  Note: It is recommended that an RReq message with Transaction Status = U contains Transaction Status Reason = 24 or 26 and Challenge Cancelation Indicator = 03.

The 3DS Server shall:

[Req 348]

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 1 hour, 30 seconds for the RReq, If an RReq message is never received, further processing is outside the scope of 3-D Secure processing.

3.4 3RI-based Requirements

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:

[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 (Transaction Status = U) is sent when the 3DS Requestor Decoupled Max Time expires—with a grace period of 1 hour.

  Note: It is recommended that an RReq message with Transaction Status = U contains Transaction Status Reason = 24 or 26 and Challenge Cancelation Indicator = 03.

The 3DS Server shall:

[Req 354]

For a Decoupled Authentication transaction, at a minimum wait the specified 3DS Requestor Decoupled Max Time plus 1 hour, 30 seconds for the RReq, If an RReq message is never received, further processing is outside the scope of 3-D Secure processing.

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~~Native Device Rendering Option and HTML~~.

4.2 App-based User Interface Overview

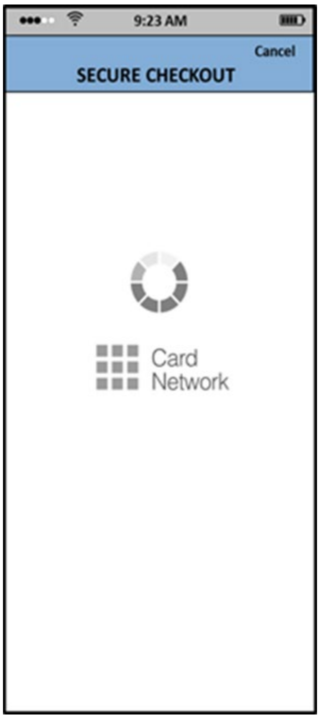
The supported digital image file types are png, jpeg, tiff and bmp. Any other image types implemented by the ACS may not be supported by the 3DS SDK.

Note: Some platforms may not natively support all image types.

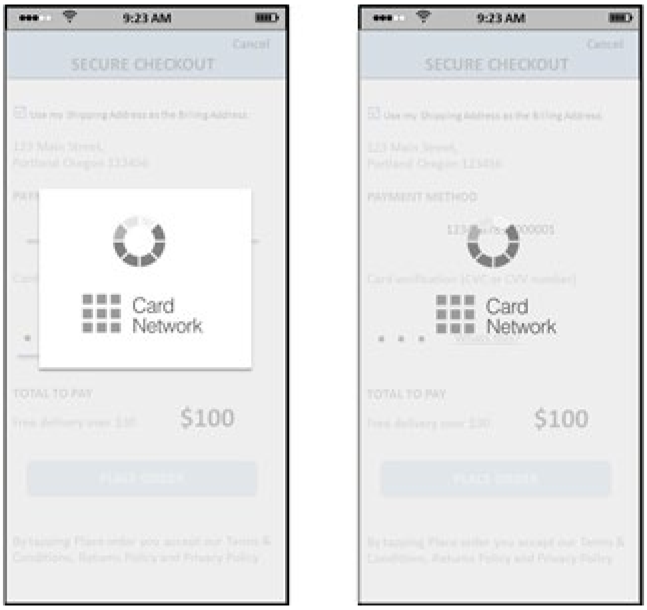
4.2.1 Processing Screen Requirements

New graphic for Figure 4.4

(Original) **Figure 4.4 Sample App-based Processing Screen**



(Updated) **Figure 4.4 Sample App-based Processing Screen**



4.2.1.1 3DS SDK/3DS Requestor App

The 3DS SDK shall for the AReq/ARes message exchange:

[Req 143]

Integrate the Processing Graphic and if requested, the DS logo into the centre of the Processing screen as depicted in Figure 4.4 with or without a white box.

The 3DS Requestor App shall for the AReq/ARes message exchange:

[Req 145]

Display the Processing screen supplied by the 3DS SDK during the entire AReq/ARes message cycle and overlay on the merchant checkout page as depicted in Figure 4.4.

The 3DS Requestor App shall in case of challenge:

[Req 388]

Set the Header zone text and the Cancel action name to be displayed by the SDK.

~~[Req 360]~~

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

The 3DS SDK shall for the CReq/CRes message exchange:

~~[Req 361]~~

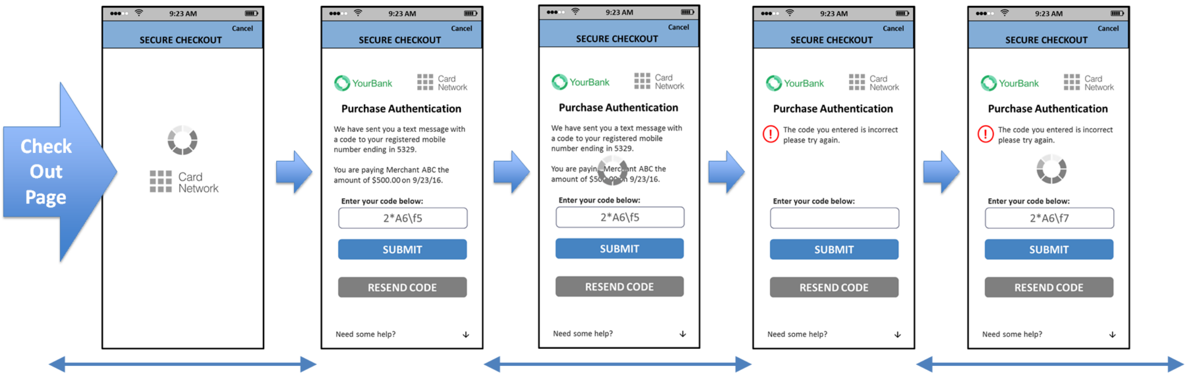
~~Display the Cancel action in the top right corner of the Header zone.~~

[Req 389]

Ensure that the Cancel action is not actionable on the Processing screen.

New Graphic for Figure 4.5

(Original) **Figure 4.5: Sample OTP/Text Template—App-based Processing Flow**

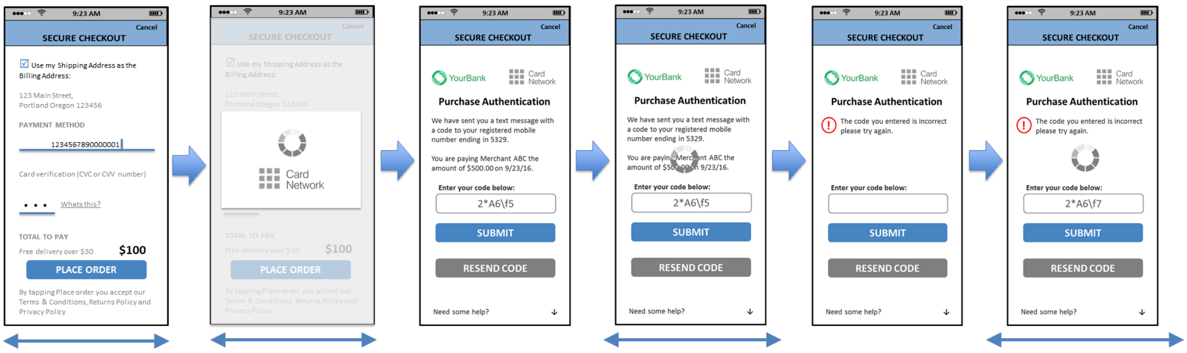

Check Out Page
9:23 AM
Cancel
SECURE CHECKOUT
Card Network
YourBank
Purchase Authentication
We have sent you a text message with a code to your registered mobile number ending in 5329.
You are paying Merchant ABC the amount of $500.00 on 9/23/16.
The code you entered is incorrect please try again.
Enter your code below:
2*A6\f5
2*A6\f7
SUBMIT
RESEND CODE
Need some help?

Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

Processing indicator is displayed by SDK

Processing indicator is displayed by SDK

(Updated) **Figure 4.5: Sample OTP/Text Template—App-based Processing Flow**


9:23 AM
Cancel
SECURE CHECKOUT
☑ Use my Shipping Address as the Billing Address:
123 Main Street, Portland Oregon 123456
PAYMENT METHOD
1234567890000001
Card verification (CVC or CVV number)
• • •
Whats this?
TOTAL TO PAY
Free delivery over $30
$100
PLACE ORDER
By tapping Place order you accept our Terms & Conditions, Returns Policy and Privacy Policy
Card Network
YourBank
Purchase Authentication
We have sent you a text message with a code to your registered mobile number ending in 5329.
You are paying Merchant ABC the amount of $500.00 on 9/23/16.
The code you entered is incorrect please try again.
Enter your code below:
2*A6\f5
2*A6\f7
SUBMIT
RESEND CODE
Need some help?

Merchant checkout page

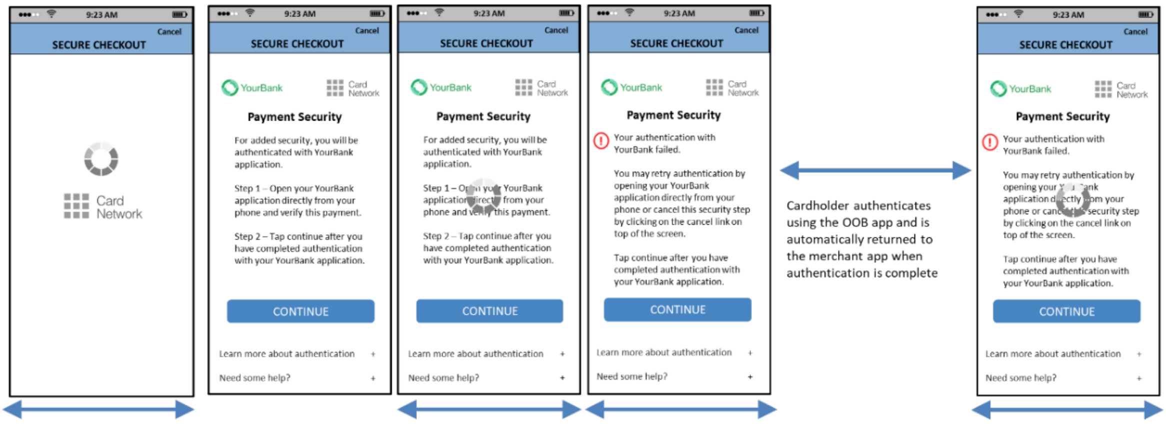
Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

Processing indicator is displayed by SDK

Processing indicator is displayed by SDK

New Graphic for Figure 4.6

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



For added security, you will be authenticated with YourBank application.

Step 1 – Open your YourBank application directly from your phone and verify this payment.

Step 2 – Tap continue after you have completed authentication with your YourBank application.

Your authentication with YourBank failed.

You may retry authentication by opening your YourBank application directly from your phone or cancel this security step by clicking on the cancel link on top of the screen.

Tap continue after you have completed authentication with your YourBank application.

Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

Processing indicator is displayed by SDK

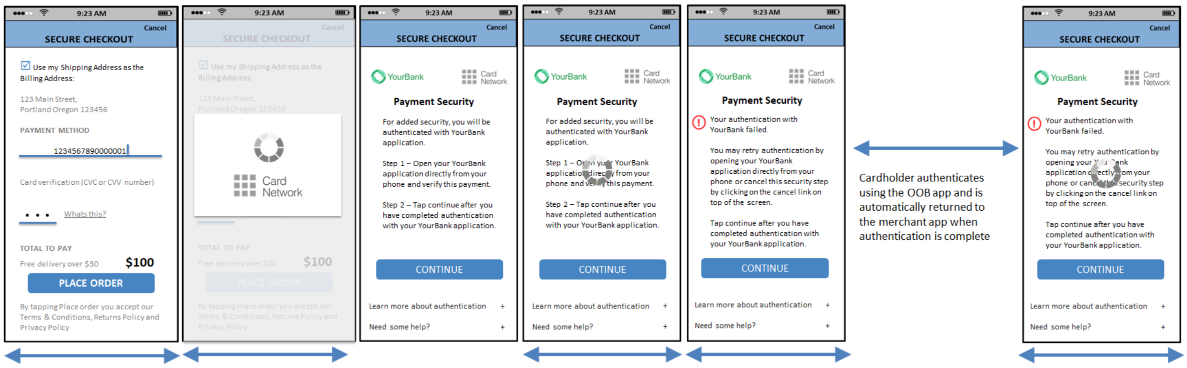
Indicator and text displayed if cardholder clicks continue without completing authentication

Cardholder authenticates using the OOB app and is automatically returned to the merchant app when authentication is complete

Processing indicator is displayed by the SDK

NOTE: Cardholder is not required to click continue when OOB and 3DS Requestor APP are on same device.

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



☑ Use my Shipping Address as the Billing Address:

123 Main Street,
Portland Oregon 123456

Card verification (CVC or CVV number)

Free delivery over $30

By tapping Place order you accept our Terms & Conditions, Returns Policy and Privacy Policy

For added security, you will be authenticated with YourBank application.

Step 1 – Open your YourBank application directly from your phone and verify this payment.

Step 2 – Tap continue after you have completed authentication with your YourBank application.

Your authentication with YourBank failed.

You may retry authentication by opening your YourBank application directly from your phone or cancel this security step by clicking on the cancel link on top of the screen.

Tap continue after you have completed authentication with your YourBank application.

Merchant checkout page

Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

Processing indicator is displayed by SDK

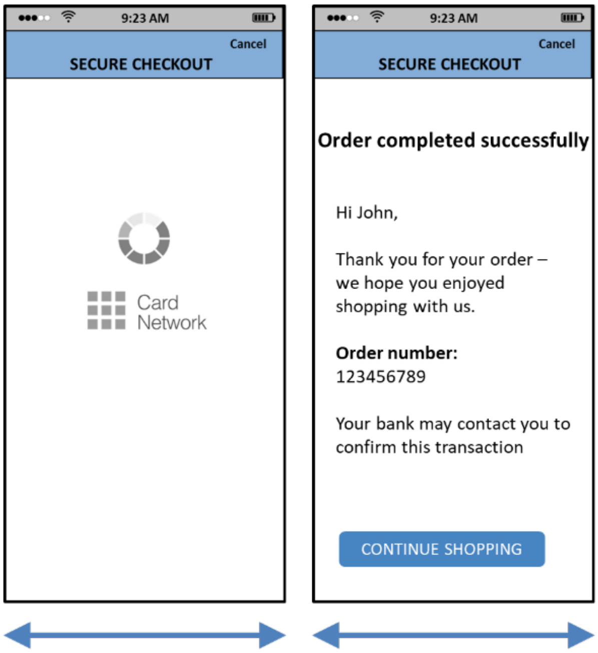
Indicator and text displayed if cardholder clicks continue without completing authentication

Cardholder authenticates using the OOB app and is automatically returned to the merchant app when authentication is complete

Processing indicator is displayed by the SDK

NOTE: Cardholder is not required to click continue when OOB and 3DS Requestor APP are on same device.

(Original) Figure 4.1: Sample Decoupled Authentication Template—App-based Processing Flow



Order completed successfully

Hi John,

Thank you for your order – we hope you enjoyed shopping with us.

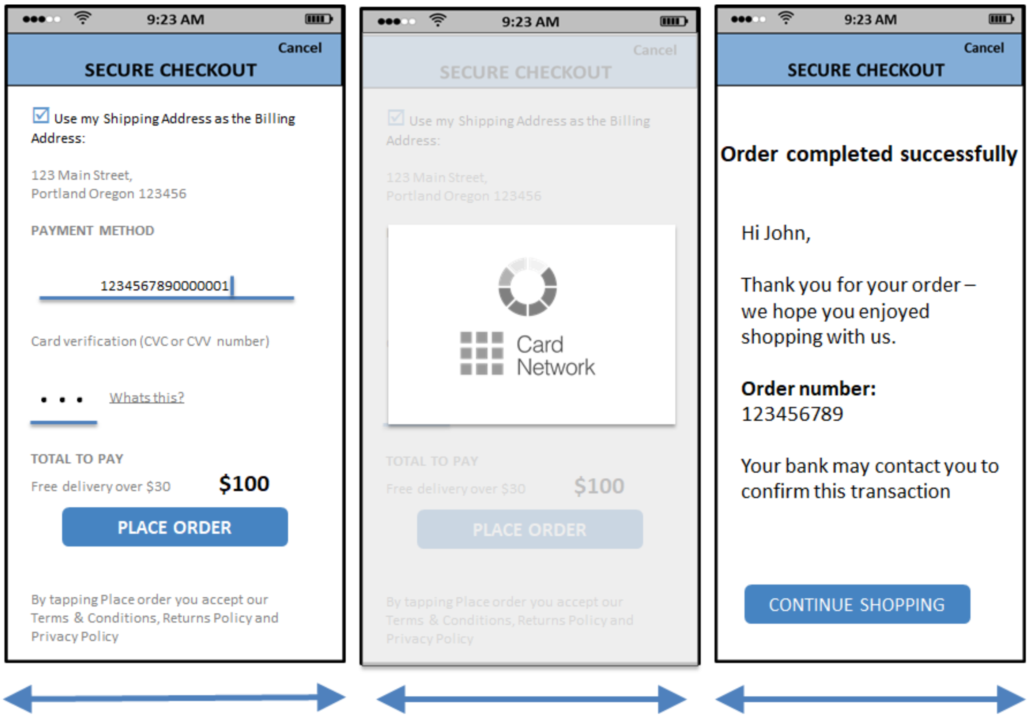
Order number: 123456789

Your bank may contact you to confirm this transaction

Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

3DS Requestor App displays Cardholder Information Text on checkout page if provided by the ACS

(Updated) Figure 4.2: Sample Decoupled Authentication Template—App-based Processing Flow



9:23 AM

Cancel

SECURE CHECKOUT

☑ Use my Shipping Address as the Billing Address:

123 Main Street,
Portland Oregon 123456

PAYMENT METHOD

1234567890000001

Card verification (CVC or CVV number)

• • • Whats this?

TOTAL TO PAY

Free delivery over $30 $100

PLACE ORDER

By tapping Place order you accept our Terms & Conditions, Returns Policy and Privacy Policy

9:23 AM

Cancel

SECURE CHECKOUT

☑ Use my Shipping Address as the Billing Address:

123 Main Street,
Portland Oregon 123456

Card Network

TOTAL TO PAY

Free delivery over $30 $100

PLACE ORDER

By tapping Place order you accept our Terms & Conditions, Returns Policy and Privacy Policy

9:23 AM

Cancel

SECURE CHECKOUT

Order completed successfully

Hi John,

Thank you for your order – we hope you enjoyed shopping with us.

Order number:
123456789

Your bank may contact you to confirm this transaction

CONTINUE SHOPPING

Merchant checkout page

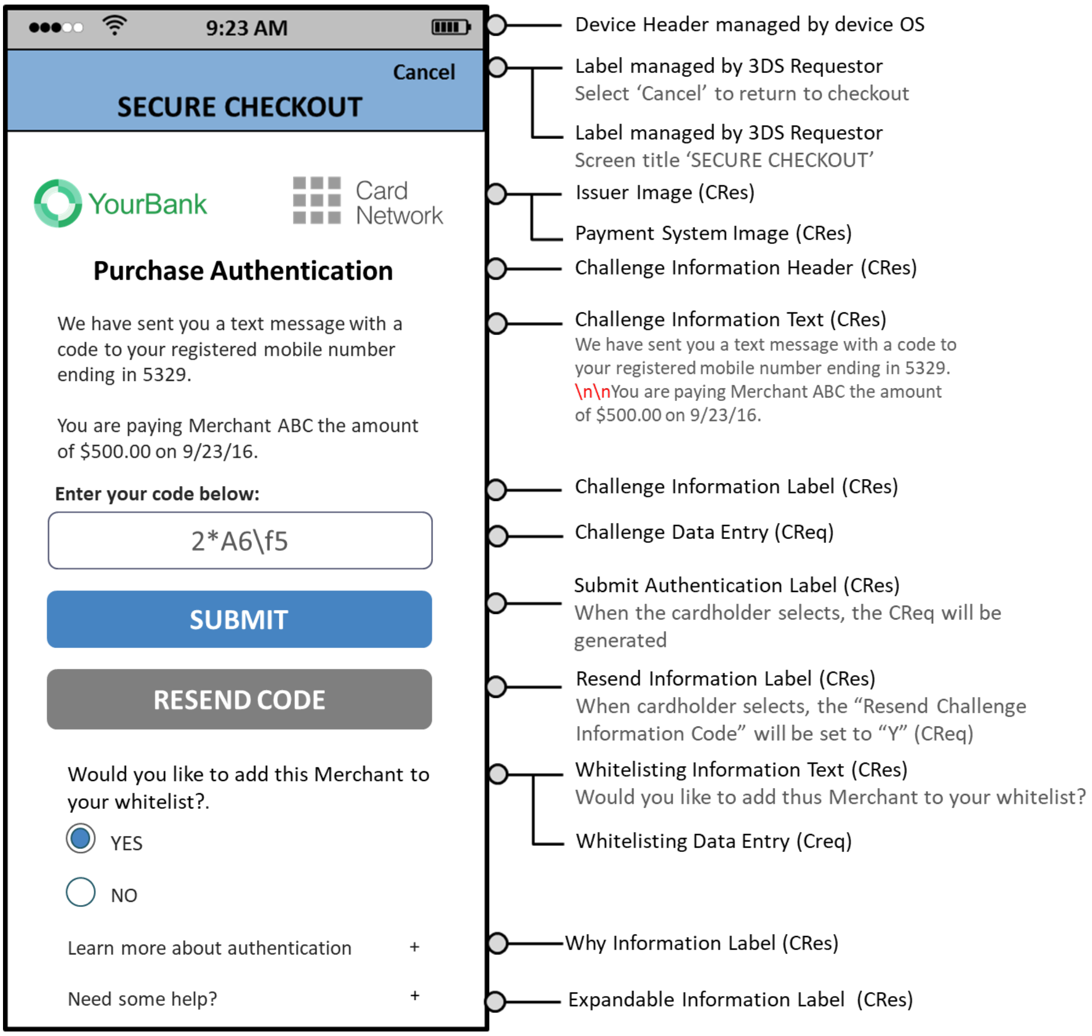
Processing indicator and card network logo by the 3DS Requestor App for at least 2 seconds

3DS Requestor App displays Cardholder Information Text on checkout page if provided by the ACS

4.2.3 Native UI Templates

New graphic for Figure 4.14

***(Original)* Figure 4.14 Sample Whitelisting Information Text—PA**



Purchase Authentication

We have sent you a text message with a code to your registered mobile number ending in 5329.

You are paying Merchant ABC the amount of $500.00 on 9/23/16.

Enter your code below:

2*A6\f5

Would you like to add this Merchant to your whitelist?.

● YES

○ NO

Device Header managed by device OS

Label managed by 3DS Requestor
Select 'Cancel' to return to checkout

Label managed by 3DS Requestor
Screen title 'SECURE CHECKOUT'

Issuer Image (CRes)

Payment System Image (CRes)

Challenge Information Header (CRes)

Challenge Information Text (CRes)
We have sent you a text message with a code to your registered mobile number ending in 5329. \n\nYou are paying Merchant ABC the amount of $500.00 on 9/23/16.

Challenge Information Label (CRes)

Challenge Data Entry (CReq)

Submit Authentication Label (CRes)
When the cardholder selects, the CReq will be generated

Resend Information Label (CRes)
When cardholder selects, the "Resend Challenge Information Code" will be set to "Y" (CReq)

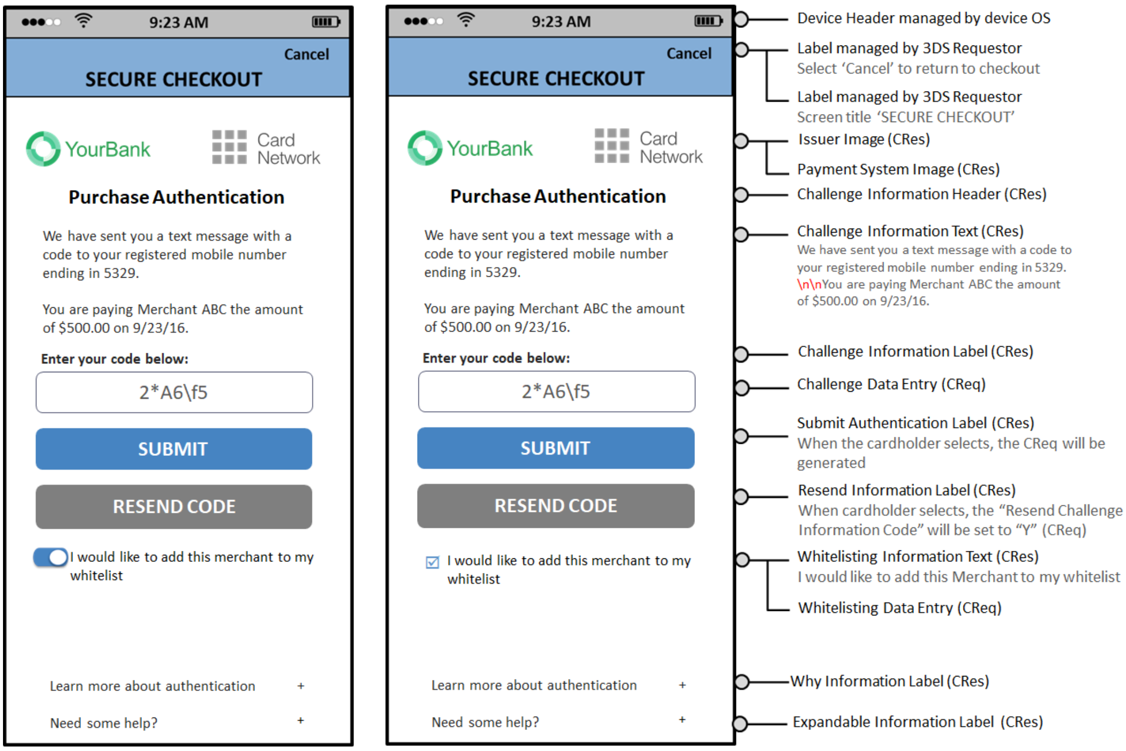
Whitelisting Information Text (CRes)
Would you like to add thus Merchant to your whitelist?

Whitelisting Data Entry (Creq)

Why Information Label (CRes)

Expandable Information Label (CRes)

(Updated) Figure 4.14 Sample Whitelisting Information Text—PA



Purchase Authentication

We have sent you a text message with a code to your registered mobile number ending in 5329.

You are paying Merchant ABC the amount of $500.00 on 9/23/16.

Enter your code below:

2*A6\f5

I would like to add this merchant to my whitelist

☑ I would like to add this merchant to my whitelist

Device Header managed by device OS

Label managed by 3DS Requestor
Select 'Cancel' to return to checkout

Label managed by 3DS Requestor
Screen title 'SECURE CHECKOUT'

Issuer Image (CRes)

Payment System Image (CRes)

Challenge Information Header (CRes)

Challenge Information Text (CRes)
We have sent you a text message with a code to your registered mobile number ending in 5329. \n\nYou are paying Merchant ABC the amount of $500.00 on 9/23/16.

Challenge Information Label (CRes)

Challenge Data Entry (CReq)

Submit Authentication Label (CRes)
When the cardholder selects, the CReq will be generated

Resend Information Label (CRes)
When cardholder selects, the "Resend Challenge Information Code" will be set to "Y" (CReq)

Whitelisting Information Text (CRes)
I would like to add this Merchant to my whitelist

Whitelisting Data Entry (CReq)

Why Information Label (CRes)

Expandable Information Label (CRes)

4.2.4.1 3DS SDK

The 3DS SDK shall:

[Req 153]

After submitting the CReq message to the ACS, display the same Processing screen as during the AReq/ARes message until the CRes message is received, or timeout is exceeded.

4.2.7.3 3DS SDK

The 3DS SDK shall:

[Req 171]

Return control to the 3DS Requestor App when the Cancel action in the 3DS Requestor header is selected.

On HTML submit:

- The web view will return~~, either~~ a parameter string (HTML Action = GET) ~~or form data (HTML Action = POST)~~ containing the cardholder's data input.
- The SDK passes the received data, unchanged, to the ACS in the Challenge HTML Data Entry data element of the CReq message. The SDK shall not modify or reformat the data.

Chapter 5 EMV 3-D Secure Message Handling

5.1.3 Base64/Base64url Encoding

[Req 193]

Base64 ~~and Base64url~~ decoding software shall ignore any white space (such as carriage returns or line ends) within Base64 ~~and Base64url~~ encoded data and shall not treat the presence of such characters as an error.

5.1.6 Message Content Validation

[Req 309]

Unless explicitly noted, if a conditionally optional or optional field is sent as empty or null, the receiving component shall return an Error Message (as defined in Section A.5.5) with the applicable Error Component and Error Code = 203.

For Example:

The DS receives an ARes message from the ACS with an empty conditionally Optional data element that is specified in Table A.1 for the Message Type, Device Channel and Message Category but the condition is not met. Such as, acsChallengeMandated = "" and transStatus = Y. The DS validates the ARes message content and returns an error to the ACS and can return an ARes message or Error to the 3DS Server.

Chapter 6 EMV 3-D Secure Security Requirements

Multiple updates are made to section 6.2 Security Functions. These edits are included in the following section and additionally for clarity, are included at the end of this section in a "clean" final format with no revision marks. Click here to view the "clean" version of these edits.

6.2.2.1 3DS SDK Encryption

The 3DS SDK:

- If P_{DS}, is an RSA key:
  - Encrypts the JSON object according to JWE (RFC 7516) using JWE Compact Serialization. The parameter values ~~supported in~~for this version of the specification and to be included in the JWE protected header are:
- Else if P_{DS} is an EC key:
  - Conducts a Diffie-Hellman key exchange process according to JWA (RFC 7518) in Direct Key Agreement mode using ECDH-ES, curve P-256, d_{SDK}, ~~and~~ P_{DS} with Concat KDF to produce a 256-bit CEK. The Concat KDF parameter values ~~supported in~~for this version of the specification are:
    - ~~"alg":ECDH-ES~~
    - ~~"apv":DirectoryServerID~~
    - ~~"epk": P_{DS}, in JSON Web Key (JWK) format~~
      ~~{"kty":"EC"~~
      ~~"crv":"P-256"}~~
    - ~~All other parameters: not present~~
    - Keydatalen = 256
    - AlgorithmID = empty string (length = 0x00000000)
    - PartyUInfo = empty string (length = 0x00000000)
    - PartyVInfo = `directoryServerID` (length || ascii string)
    - SuppPubInfo = Keydatalen (0x00000100)
    - SuppPrivInfo = empty octet sequence
  - ~~CEK: "kty":oct - 256 bits~~
  - Generates 128-bit random data as IV (included in the JWE)
  - Encrypt the JSON object according to JWE (RFC 7516) using the CEK and JWE Compact Serialization. The parameter values ~~supported~~for this version of the specification and to be included in the JWE protected header are:
    - "alg":~~dir~~"ECDH-ES"
    - "epk": Q_{SDK},
      {"kty": "EC",
      "crv": "P-256"
      "x":x coordinate of Q_{SDK}
      "y":y coordinate of Q_{SDK}}

6.2.2.2 DS Decryption

The DS:

- If the protected header of the JWE in the SDK Encrypted Data field indicates that ~~a RSA key~~RSA-OAEP-256 was used for encryption:

- Decrypts the SDK Encrypted Data field from the AReq message according to JWE (RFC 7516) using RSA-OAEP-256 and either A128CBC-HS256 or A128GCM as indicated by the "enc" parameter in the protected header. ~~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~~

- Else, if the protected header of the JWE in the SDK Encrypted Data field indicates that ~~an EC key~~ECDH-ES was used for encryption:
  - Conducts a Diffie-Hellman key exchange process according to JWA (RFC 7518) in Direct Key Agreement mode using ECDH-ES, curve P-256, Q_{SDK}, and d_{DS} with the parameter values from the protected header and Concat KDF to produce a 256-bit CEK. The Concat KDF parameter values ~~supported in~~for this version of the specification are:
    - ~~"alg":ECDH-ES~~
    - ~~"apv": DirectoryserverID~~
    - ~~"epk": Q_{SDK}~~
    - ~~{"kty":"EC"~~
    - ~~"crv":"P-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~~
    - Keydatalen = 256
    - AlgorithmID = empty string (length = 0x00000000)
    - PartyUInfo = empty string (length = 0x00000000)
    - PartyVInfo = `directoryServerID` (length || ascii string)
    - SuppPubInfo = Keydatalen (0x00000100)
    - SuppPrivInfo = empty octet sequence
  - ~~CEK: "kty":oct - 256 bits~~
  - Decrypt the JWE in the SDK Encrypted Data field according to JWE (RFC 7516) using the CEK and either A128CBC-HS256 or A128GCM as indicated by the “enc” parameter in the protected header. If the algorithm is A128GCM the leftmost 128bits of CEK is used~~ with the received IV~~. If decryption fails, ceases processing and reports error.

6.2.3.2 ACS Secure Channel Setup

The ACS:

- Completes the Diffie-Hellman key exchange process as a local mechanism according to JWA (RFC 7518) in Direct Key Agreement mode using ECDH-ES, curve P-256, d_T and Q_C with Concat KDF to produce a ~~pair of~~ 256-bit CEK~~s (one for each direction)~~ which ~~are~~is identified ~~by~~to the ACS Transaction ID. ~~In order to obtain 256 bits of keying material from the included Concat KDF function assume an "enc" parameter of ECDH-ES+A256KW and assume the algorithmID to be null for the KDF[8].~~ (*Footnote 8 also deleted*: [8]~~Note this is using RFC 7518 only for key derivation.~~). The Concat KDF parameter values ~~supported~~ ~~in~~for this version of the specification are:
  - ~~"alg":ECDH-ES~~
  - ~~"apv": SDK Reference Number~~
  - ~~"epk": Q_C (received in the AReq message as `sdkEphemKey`)~~
  - ~~{"kty":"EC"~~
~~"crv":"P-256"}~~
  - ~~All other parameters: not present~~
  - Keydatalen = 256
  - AlgorithmID = empty string (length = 0x00000000)
  - PartyUInfo = empty string (length = 0x00000000)
  - PartyVInfo = `sdkReferenceNumber` (length || ascii string)
  - SuppPubInfo = Keydatalen (0x00000100)
  - SuppPrivInfo = empty octet sequence
  - ~~CEK: "kty":oct -~~ 256 bits ~~extracted~~ allocated as:
- Generates a digital signature of the full JSON object according to JWS (RFC 7515) using JWS Compact Serialization. The parameter values ~~supported in~~for this version of the specification and to be included in the JWS header are:

6.2.3.3 3DS SDK Secure Channel Setup

The 3DS SDK:

- Using the CA public key of the DS CA identified from information provided by the 3DS Server, ~~Validate~~validates the JWS from the ACS according to JWS (RFC7515) using either PS256 or ES256 as indicated by the "alg" parameter in the header. ~~The 3DS SDK is required to support both "alg" parameters PS256 and ES256.~~ If validation fails, ceases processing and report error.
- Completes the Diffie-Hellman key exchange process according to JWA (RFC 7518) in Direct Key Agreement mode using curve P-256, d_C and Q_T, with Concat KDF to produce a ~~pair of~~ 256-bit CEK~~s (one for each direction)~~, which ~~are~~is identified to the ACS Transaction ID received in the ARes message. ~~In order to obtain 256 bits of keying material from the included Concat KDF function assume an "enc" parameter of ECDH-ES+A256KW and assume the algorithmID to be null for the KDF[10].~~ ~~(~~*Footnote 10 also deleted:* ~~[10] Note this is using RFC 7518 only for key derivation).~~ The Concat KDF parameter values supported ~~in~~for this version of the specification are:
  - ~~"alg":ECDH-ES~~
  - ~~"apv": SDK Reference Number~~
  - ~~"epk": Q_T (received in the AReq message as `acsEphemPubKey`) which is part of ACS Signed Content)~~

- ~~{"kty":"EC"~~
  ~~"crv":"P-256"}~~
- ~~All other parameters: not present~~
- Keydatalen = 256
- AlgorithmID = empty string (length = 0x00000000)
- PartyUInfo = empty string (length = 0x00000000)
- PartyVInfo = `sdkReferenceNumber` (length || ascii string)
- SuppPubInfo = Keydatalen (0x00000100)
- SuppPrivInfo = empty octet sequence
- CEK: ~~"kty":oct -~~256 bits ~~extracted~~ allocated as:

If the ACS signature is valid, the 3DS SDK has confirmed the authenticity of the ACS, that the session keys are fresh, and that the ACS_URL is correct.

6.2.4.1 3DS SDK—CReq

For CReq messages sent from the 3DS SDK to the ACS, the 3DS SDK:

- Encrypts the JSON object according to JWE (RFC 7516) using the CEK$_{S\text{-}A}$ obtained in Section 6.2.3.3 and JWE Compact Serialization. The parameter values ~~supported in~~for this version of the specification and to be included in the JWE protected header are:
- Sends the resulting JWE to the ACS as the ~~encrypted~~ protected CReq message.

6.2.4.2 3DS SDK—CRes

For CRes messages received by the 3DS SDK from the ACS, the 3DS SDK:

- Decrypts the message according to JWE (RFC 7516) using either A128CBC-HS256 or A128GCM and the CEK$_{A\text{-}S}$ obtained in Section 6.2.3.3 as identified by the "enc" and "kid" parameters in the protected header. If decryption fails, ceases processing and reports error.

6.2.4.3 ACS—CReq

For CReq messages received by the ACS from the 3DS SDK, the ACS:

- Decrypts the message according to JWE (RFC 7516) using either A128CBC-HS256 or A128GCM and the CEK$_{S\text{-}A}$ obtained in Section 6.2.3.2 as identified by the "enc" and "kid" parameters in the protected header. If decryption fails, ceases processing and reports error.

6.2.4.4 ACS—CRes

For CRes messages sent from the ACS to the 3DS SDK the ACS:

- Encrypts the JSON object according to JWE (RFC 7516) using the same "enc" algorithm used by the 3DS SDK for the CReq message, the CEK$_{A\text{-}S}$ obtained in Section 6.2.3.2 identified by "kid" and JWE Compact Serialization. The parameter values ~~supported in~~for this version of the specification and to be included in the JWE protected header are:
- Sends the resulting JWE to the 3DS SDK as the ~~encrypted~~ protected CRes message.

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 App URL						CReq = ~~O~~C	Required if 3DS Requestor App URL is supported.
3DS Requestor Authentication Indicator			07 = Billing Agreement ~~07~~08–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)				
3DS Requestor Authentication Method Verification Indicator							Conditional based on DS rules. The DS populates the AReq with this data element prior to passing to the ACS.
3DS Requestor Decoupled Max Time						AReq = ~~O~~C	Required if Decoupled Request Indicator = Y.

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
3RI Indicator			12 = Billing Agreement ~~12~~13–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)				
ACS Rendering Type	Identifies the ACS ~~UI~~ Interface and ACS UI Template that the ACS will first present to the consumer.						For RReq, required unless ACS Decoupled Confirmation Indicator = Y.
Authentication Method	Note: This is in the RReq message from the ACS only. It is not passed to the 3DS Server~~ URL~~.						This field is present in the RReq message from the ACS to the DS but is not present in the RReq message from the DS to the 3DS Server. ~~This field is not present in the RReq message from the DS to the 3DS Server URL.~~

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
BrowserJavaScript Enabled Field Name: browserJavascriptEnabled *Note: The field name was incorrectly identified in SB 207. There was no change made in the specification.*							
Cardholder Email Address							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**
Challenge Data Entry							Required when: • ACS UI Type = 01, 02, or 03, AND • Challenge data has been entered in the UI, AND • Challenge Cancelation Indicator is not present AND • Resend Challenge Information Code is not present ~~Are not present.~~

Data Element/ Field Name	**Description**	**Source**	**Length/Format/ Values**	**Device Channel**	**Message Category**	**Message Inclusion**	**Condition Inclusion**
Challenge No Entry							Required when: • ACS UI Type = 01, 02, or 03, AND • Challenge Data Entry is not present, AND • Challenge Cancelation Indicator is not present AND • Resend Challenge Information Code is not present ~~Are not present.~~
Device Rendering Options Supported	~~Defines~~ Identifies the SDK ~~UI types~~Interface and SDK UI Type that the device supports for displaying specific challenge user interfaces within the SDK.						
DS Start Protocol Version	The ~~most recent~~ earliest (i.e. oldest) active protocol version that is supported for the DS.						
Instalment Payment Data							• Required for 03-3RI if 3RI Indicator = 02.

Data Element/ Field Name	Description	Source	Length/Format/ Values	Device Channel	Message Category	Message Inclusion	Condition Inclusion
Interaction Counter	Indicates the number of authentication cycles (excluding Decoupled Authentication) attempted by the Cardholder.					RReq = ~~R~~C	Required unless ACS Decoupled Confirmation Indicator = Y.
Purchase Amount							• Required for 02-NPA if 3RI Indicator = 01, 02, 06, 07, 08, 09, 11.
Purchase Currency							• Required for 02-NPA if 3RI Indicator = 01, 02, 06, 07, 08, 09, 11.
Purchase Currency Exponent							• Required for 02-NPA if 3RI Indicator = 01, 02, 06, 07, 08, 09, 11.
Purchase Date & Time							• Required for 02-NPA if 3RI Indicator = 01, 02, 06, 07, 08, 09, 11.
Recurring Expiry							• Required for 03-3RI if 3RI Indicator = 01 or 02.
Recurring Frequency							• Required for 03-3RI if 3RI Indicator = 01 or 02.

A.5.7 Card Range Data

Table A.6 Card Range Data

Data Element/Field Name	Description	Length/Format/Values	Inclusion
ACS End Protocol Version		Note: If the ACS End Protocol Version is not available, this value is the DS End Protocol Version for that card range.	
ACS Start Protocol Version		Note: If the ACS Start Protocol Version is not available, this value is the DS Start Protocol Version for that card range.	

A.7.3 3DS Requestor Information

The 3DS Requestor Authentication Information contains optional information about how the cardholder authenticated during login to their 3DS Requestor account. The detailed data elements, which are optional, are outlined in Table A.10.

A.7.4 3DS Requestor Prior Transaction Authentication Information

The 3DS Requestor Prior Transaction Authentication Information contains optional information about a 3DS cardholder authentication that occurred prior to the current transaction. The detailed data elements, which are optional, are outlined in Table A.11.

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