TECHNICAL PAPER

3-D Secure Version 2 in SAS® Fraud Management

Last update: October 2021

Contents

Relevant Products and Releases

- SAS® Fraud Management Version 5 and later

Introduction

This paper contains the steps for avoiding Card-Not-Present Fraud using the flexible message layout of SAS Fraud Management.

As e-commerce evolves into new territories of technology, the e-commerce industry must also ensure its security. In October 2017, EMVCo released a version of 3-D Secure protocols and core function specifications (3-D Secure version 2), which support app-based authentication for mobile devices and integration with digital wallets, such as Google Pay and Apple Pay. Since then, three additional updates have been released and, given the speed at which fraud and technology are both evolving, it is imperative that financial institutions keep up.

SAS Fraud Management supports the latest 3-D protocols through its flexible message layout, which empowers users to create and add transaction data fields, as necessary. These 3-D Secure fields (data elements) can be populated with client input variables (CIVs). To enable you to use the latest data from 3-D Secure, SAS provides a predefined list of CIVs for these fields. This paper contains the steps for using these CIVs, including a table of the CIVs at the end of this paper.

For more information about the new Version of 3-D Secure Protocols and Core Functions, see the EMVCo website.

Prerequisites for Using the 3-D Secure Version 2 Data Elements in SAS Fraud Management

Here are the requirements for using the 3-D Secure version 2 fields in SAS Fraud Management:

- SAS Fraud Management version 5 and later.
- The 3-D Secure version 2 fields are defined and configured in the Orchestration layer.
- You must be logged on to SAS Fraud Management as a Senior Rules Editor, Rules Administrator, or in any role that has the following privileges:
    - Add/Delete/Modify Client Input Variable Segments
    - View Rules
- The 3DSecureV2_CIVs.xml file has been downloaded to an accessible location. This file contains the client input variables for the 3-D Secure Version 2 fields.

Using the Data Elements

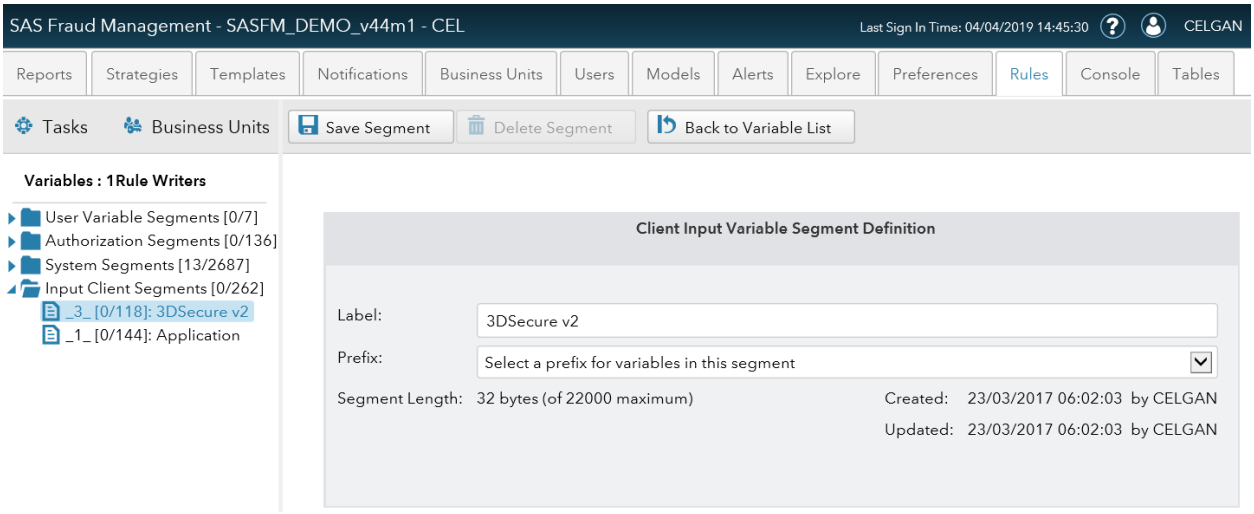
To start using the data elements in 3-D Secure version 2:

Note: The following instructions apply to SAS Fraud Management version 5.

1. Log on to SAS Fraud Management and select the **Rules** tab.
2. Select **Tasks -> List Variables**.
3. Select the **Input Client Segments** folder.
4. Click **New Segment**. The Client Input Variable Segment Definition page is displayed.
5. In the **Label** field, enter the value, **3DSecure v2**.
6. In the **Prefix** field, select **3** as the prefix for the segment.

The following figure shows the result of specifying the label and prefix:

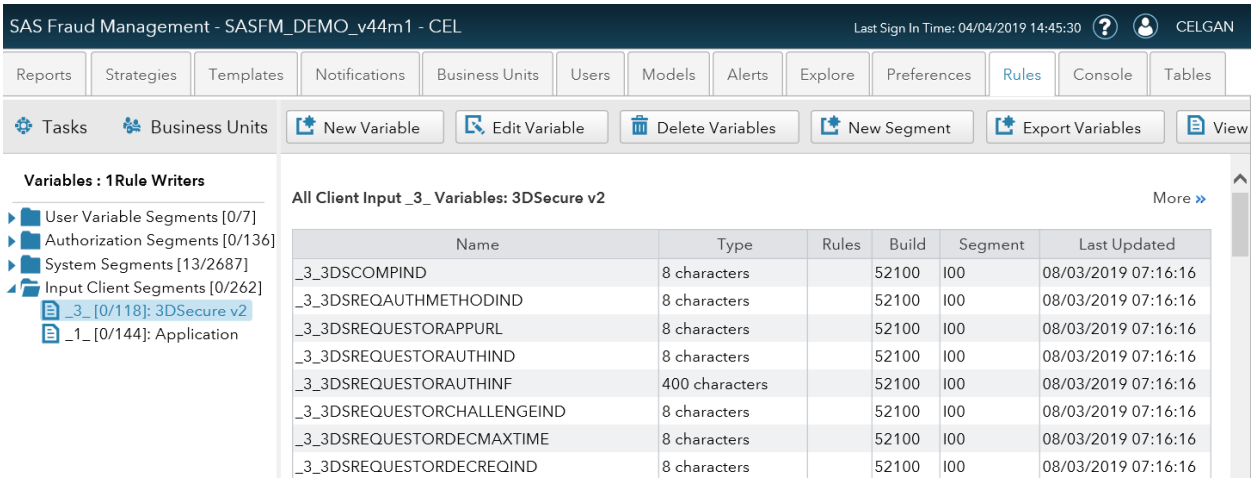
Figure 1. 3DSecure v2 Segment That You Created in SAS Fraud Management



7. Click **Save Segment**.
8. After the segment has been created, select Tasks -> Import. The Rules Import dialog box is displayed.
9. Click **Browse** to open the File Explorer window.
10. Navigate to the location of the file named 3DSecureV2_CIVs.xml.
11. Select the file and click **Open**. This action closes the File Explorer window and automatically populates the **Import File** field with the file's location.
12. Click **Submit**. The Import Results Report window shows both the successful and unsuccessful actions.

Figure 2 shows the imported variables that are listed in the input client segment that you created.

Figure 2. 3DSecure v2 Segment Data Elements That Are Imported into SAS Fraud Management



13. You can now start to use these fields to map the 3-D Secure Version 2 data elements into SAS Fraud Management through your preferred integration layer (for example, SAS® Business Orchestration Services).

Data Elements and Corresponding SAS Client Input Variables

The following table contains the list of 3-D Secure Version 2 data elements and the corresponding client input variables. For a full list of these data elements, including those in the preceding sections and tables, see the EMV 3-D Secure Protocol and Core Functions Specification. For more information about 3-D Secure, see https://www.emvco.com/emv-technologies/3d-secure/.

The data elements from 3-D Secure are originally in character format. Therefore, you might need to perform additional steps to convert between character and numeric format, as appropriate. For example, the date elements (such as the Purchase Date & Time and Recurring Expiry data elements) are sent in character format. The Purchase Amount element (with a maximum length of 48 characters) is also sent in character format. You can convert from character to numeric format either using SAS statements in the SAS Rules Studio (for example, using an INFORMAT statement), but some data elements must be converted through the orchestration layer to move between your system and SAS Fraud Management.

If you choose to convert the data type through the orchestration layer, then you must prepare the numeric data elements so that they are in IEEE 754 double precision 8-byte format. If you are using SAS Business Orchestration Services, then the incoming format might be converted to the SAS Fraud Management supported format.

Regardless of which method you choose to use, some work is required in the orchestration layer for these data elements so that they can be consumed by SAS Fraud Management.

The following table lists the CIVs.

***Table 1**. Client Input Variables*

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3DS Method Completion Indicator	threeDSCompInd	Indicates whether the 3-D Secure method successfully completed.	• Y: Successfully completed. • N: Did not successfully complete. • U: Unavailable. 3-D Secure Method URL was not present in the PRes message data for the card range that is associated with the cardholder's account number.	8 CHAR	_3_3DSCompInd
3DS Requestor App URL	threeDSRequestorAppURL	Merchant application declaring their URL within the CReq message so that the authentication application can call the merchant application after out-of-band (OOB) authentication has occurred. Each transaction would require a unique transaction ID by using the SDK transaction ID.	Fully qualified URL (for example, merchantScheme://appName?transID=b2385523-a66c-4907-ac3c-91848e8c0067)	400 CHAR	_3_3DSRequestorAppURL

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3DS Requestor Authentication Indicator	threeDSRequestorAuthenticationInd	Indicates the type of authentication request. This element provides additional information to the access control server (ACS) to determine the best approach for handling an authentication request.	• 01: Payment transaction. • 02: Recurring transaction. • 03: Installment transaction. • 04: Add card. • 05: Maintain card. • 06: Cardholder verification as part of EMV token ID&V. • 07-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for directory server (DS) use.	8 CHAR	_3_3DSRequestorAuthInd
3DS Requestor Authentication Information	threeDSRequestorAuthenticationInfo	Information about how the 3-D Secure requestor that authenticated the cardholder before or during the transaction. *Optional. It is recommended that this value is included.	For more information about which elements to include, see Table A.10 in the EMV 3-D Secure Protocol and Core Functions Specification. ***Note***: Data is formatted into a JSON object before being placed into the 3DS Requestor Authentication Information element of the message.	400 CHAR	_3_3DSRequestorauthInfo

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3DS Requestor Authentication Method Verification Indicator	threeDSReqAuthMethodInd	Value that represents the signature verification that was performed by the DS on the mechanism (for example, FIDO) used by the cardholder to authenticate to the 3-D Secure requestor. *Conditional inclusion based on DS rules.	• 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.	8 CHAR	_3_3DSReqAuthMethodInd
3DS Requestor Challenge Indicator	threeDSRequestorChallengeInd	Indicates whether a challenge is requested for this transaction.	• 01: No preference. • 02: No challenge was requested. • 03: Challenge was requested (3-D Secure requestor preference). • 04: Challenge was requested (mandate). • 05: No challenge was requested (transactional risk analysis has already been performed). • 06: No challenge was requested (data share only).	8 CHAR	_3_3DSRequestorChallengeInd

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
			• 07: No challenge was requested (strong consumer authentication is already performed). • 08: No challenge was requested. (Use accept list exemption if no challenge is required.) • 09: Challenge was requested. (Accept list prompt requested if a challenge is required.) • 10-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use. ***Note***: If the element is not provided, then the expected action is that the ACS would interpret it as 01, no preference.		
3DS Requestor Decoupled Max Time	threeDSRequestorDecMaxTime	Indicates the maximum amount of time (in minutes) that the 3-D Secure requestor waits for an ACS to provide the results of a decoupled authentication transaction.	Numeric values between 1 and 10080 are accepted.	8 CHAR	_3_3DSRequestorDecMaxTime

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3DS Requestor Decoupled Request Indicator	threeDSRequestorDecReqInd	Indicates whether the 3-D Secure requestor requests the ACS to use decoupled authentication and agrees to use decoupled authentication if the ACS confirms its use.	• Y: Decoupled authentication is supported and preferred if a challenge is necessary. • N: Do not use decoupled authentication. ***Note***: If the element is not provided, then the expected action is for the ACS to interpret it as N. Do not use decoupled authentication.	8 CHAR	_3_3DSRequestorDecReqInd
3DS Requestor ID	threeDSRequestorID	DS assigned 3-D Secure requestor identifier. Each DS provides a unique ID to each 3-D Secure requestor on an individual basis.	Any individual DS might impose specific formatting and character requirements on the contents of this element.	40 CHAR	_3_3DSRequestorID
3DS Requestor Name	threeDSRequestorName	DS assigned 3-D Secure requestor name. Each DS provides a unique name for each 3-D Secure requestor on an individual basis.	Any individual DS might impose specific formatting and character requirements on the contents of this element.	40 CHAR	_3_3DSRequestorName
3DS Server Reference Number	threeDSServerRefNumber	Unique identifier that is assigned by the EMVCo secretariat upon testing and approval.	Set by the EMVCo secretariat.	32 CHAR	_3_3DSServerRefNumber

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3DS Server Operator ID	threeDSServerOperatorID	DS assigned 3-D Secure server identifier. Each DS can provide a unique ID for each 3-D Secure server on an individual basis. *The requirements that this element is present is DS specific.	Any individual DS might impose specific formatting and character requirements on the contents of this element.	32 CHAR	_3_3DSServerOperatorID
3DS Server Transaction ID	threeDSServerTransID	Universally unique transaction identifier that is assigned by the 3-D Secure server to identify a single transaction. *Required in the error message if available (for example, it can be obtained from a message or is being generated).	Canonical format as defined in IETF RFC 4122. You can use any of the specified versions if the output meets the specified requirements.	40 CHAR	_3_3DSServerTransID

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
3RI Indicator	threeRIInd	Indicates the type of 3RI request. This element provides additional information to the ACS to determine the best approach for handing a 3RI request.	• 01: Recurring transaction. • 02: Installment transaction. • 03: Add card. • 04: Maintain card information. • 05: Account verification. • 06: Split or delayed shipment. • 07: Top-up. • 08: Mail order. • 09: Telephone order. • 10: Accept list status check. • 11: Other payment. • 12-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use	8 CHAR	_3_3RIInd

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Account Type	acctType	Indicates the type of account (for example, for a multi-account card product). *Required if 3-D Secure requestor is asking a cardholder for the account type that they are using before making the purchase. Required in some markets (for example, for merchants in Brazil). Otherwise, it is optional.	• 01: Not applicable. • 02: Credit. • 03: Debit. • 04-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: DS or payment system-specific.	8 CHAR	_3_acctType
Acquirer BIN	acquirerBIN	Acquiring institution identification code as assigned by the DS receiving the AReq message.	This value correlates to the acquirer BIN as defined by each payment system or DS.	16 CHAR	_3_acquirerBIN
Acquirer Merchant ID	acquirerMerchantID	Acquirer-assigned merchant identifier. This identifier might be the same value that is used in the authorization request that was sent on behalf of the 3-D Secure requestor and is represented in ISO 8583 formatting requirements.	Individual directory servers might impose specific format and character requirements on the contents of this element.	40 CHAR	_3_acquirerMerchantID
ACS Challenge Mandated Indicator	acsChallengeMandated	Indicates whether a challenge is required in order for the transaction to be authorized because of local mandates, regional mandates, or other variables.	• Y: Challenge is required. • N: Challenge is not required.	8 CHAR	_3_acsChallengeMandated

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
ACS Counter ACS to SDK	acsCounterAtoS	The counter that is used as a security measure in the ACS to 3-D Secure SDK secure channel.		8 CHAR	_3_acsCounterAtoS
ACS Decoupled Confirmation Indicator	acsDecConInd	Indicates whether the ACS confirms usage of Decoupled Authentication and agrees to use Decoupled Authentication to authenticate the cardholder.	• Y: Confirms that decoupled authentication will be used. • N: Decoupled authentication will not be used. ***Note***: if the value in the 3DS Requestor Decoupled Request Indicator element is N, then a value of Y cannot be returned in the ACS Decoupled Confirmation Indicator element. ***Note***: If the value in the Transaction Status element is D, then a value of N in this element is not valid.	8 CHAR	_3_acsDecConInd

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
ACS Ephemeral Public Key (QT)	acsEphemPubKey	Public key component of the ephemeral key pair that is generated by the ACS and is used to establish session keys between the 3-D Secure SDK and the ACS. The element is contained within the ACS signed content JSON web signature (JWS) object. For more information, see section 6.2.3.2 of the EMV 3-D Secure Protocol and Core Functions Specification.		400 CHAR	_3_acsEphemPubKey
ACS Operator ID	acsOperatorID	DS assigned ACS identifier. Each DS can provide a unique ID to each ACS on an individual basis.	Any individual DS might impose specific formatting and character requirements on the contents of this element.	32 CHAR	_3_acsOperatorID
ACS Reference Number	acsReferenceNumber	Unique identifier that is assigned by the EMVCo secretariat upon testing and approval.	Set by the EMVCo secretariat.	40 CHAR	_3_acsReferenceNumber
ACS Transaction ID	acsTransID	Universally unique transaction identifier that is assigned by the ACS to identify a single transaction. Required in the error message if available (for example, if it can be obtained from a message or is being generated).	Canonical format as defined in IETF RFC 4122. You can use any of the specified versions if the output meets specified requirements.	40 CHAR	_3_acsTransID

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
ACS UI Type	acsUiType	User interface type that the 3-D Secure SDK renders. This type includes the specific data mapping and requirements.	• 01: Text. • 02: Single select. • 03: Multi-select. • 04: OOB. • 05: HTML. • 06-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_acsUiType
Address Match Indicator	addrMatch	Indicates whether the cardholder's shipping address and cardholder billing address are the same.	• Y: Cardholder's shipping address matches their billing address. • N: Cardholder's shipping address does not match their billing address.	8 CHAR	_3_addrMatch

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Authentication Method	authenticationMethod	Authentication approach that the ACS used to authenticate the cardholder for this transaction. ***Note***: This is in the RReq message from the ACS only. It is not passed to the 3-D Secure server URL. ***Note***: For 3RI, this element is present only for decoupled authentication. The ACS is required to send this element. This element is not present in the RReq message from the DS to the 3-D Secure server URL.	• 01: Static passcode. • 02: SMS text message one-time password (OTP). • 03: Key fob or Europay, Mastercard, and Visa (EMV) card reader OTP. • 04: Application OTP. • 05: OTP other. • 06: Knowledge-based authentication (KBA). • 07: OOB biometrics. • 08: OOB log on. • 09: OOB other. • 10: Other. • 11: Push confirmation. • 12-79: Reserved for future EMVCo use (values invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_authenticationMethod

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Authentication Type	authenticationType	Indicates the type of authentication method the issuer will use to challenge the cardholder. The type can be in either the ARes message or what was used by the ACS when in the RReq message. This type is required in the ARes message if the value in the Transaction Status element is C or D in the ARes message. This type is required in the RReq message if the value in the Transaction Status element is Y or N in the RReq message.	• 01: Static. • 02: Dynamic. • 03: OOB. • 04: Decoupled. • 05-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_authenticationType

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Authentication Value	authenticationValue	Payment system-specific value that is provided by the ACS or the DS using an algorithm that was defined by the payment system. The authentication value might be used to provide proof of authentication. 01-payment authentication (PA): Required if the value in the Transaction Status element is Y or A. Conditional based on DS rules if the value in the Transaction Status element is I. Omitted from the RReq message when it is sent as an abandonment notification. 02-non-payment authentication (NPA): Conditional based on DS rules.	A 20-byte value that has been Base64 encoded, giving a 28-byte result.	32 CHAR	_3_authenticationValue

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Browser IP Address	browserIP	IP address of the browser as returned by the HTTP headers to the 3-D Secure requestor. Include this element where regionally acceptable.	• IPv4 address is represented in the dotted decimal format of 4foursets of decimal numbers separated by dots. The decimal number in each set is in the range 0 to 255 (for example, IPv4 address: 1.12.123.255). • IPv6 address is represented as eight groups of four hexadecimal characters, each group representing 16 bits (two octets). The groups are separated by colons (for example, IPv6 address: 2011:0db8:85a3:0101:0101:8a2e:0370:7334). For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification.	48 CHAR	_3_browserIP

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Browser Java Enabled	browserJavaEnabled	Boolean value that indicates whether the cardholder's browser can execute Java. This value is returned from the navigator.javaEnabled property. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification. Required when the Browser JavaScript Enabled element is set to true. Otherwise, it is optional.	Valid values are true or false.	8 CHAR	_3_browserJavaEnabled
Browser JavaScript Enabled	browserJavascriptEnabled	Boolean that represents the ability of the cardholder browser to execute JavaScript. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification.	Valid vales are true or false.	8 CHAR	_3_browserJavascriptEnabled
Browser Language	browserLanguage	The browser language, as defined in IETF BCP47. It is returned from the navigator.language property. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification.		8 CHAR	_3_browserLanguage

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Browser Screen Color Depth	browserColorDepth	The bit depth (in bits per pixel) of the color palette for displaying images. This value is obtained from the cardholder's browser using the screen.colorDepth property. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification. Required when the Browser JavaScript Enabled element is set to true. Otherwise, it is optional.	• 1: 1 bit. • 4: 4 bits. • 8: 8 bits. • 15: 15 bits. • 16: 16 bits. • 24: 24 bits. • 32: 32 bits. • 48: 48 bits.	8 CHAR	_3_browserColorDepth
Browser Screen Height	browserScreenHeight	Total height of the cardholder's screen in pixels. This value is returned from the screen.height property. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification. Required when The Browser JavaScript Enabled element is set to true. Otherwise, it is optional.		Numeric	_3_browserScreenHeight

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Browser Screen Width	browserScreenWidth	Total width of the cardholder's screen (in pixels). This value is returned from the screen.width property. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification. Required when The Browser JavaScript Enabled element is set to true. Otherwise, it is optional.		Numeric	_3_browserScreenWidth
Browser Time Zone	browserTZ	Time-zone offset (in minutes) between UTC and the cardholder's browser's local time. The offset is positive if the local time zone is behind UTC, and negative if it is ahead of UTC time. Required when The Browser JavaScript Enabled element is set to true. Otherwise, it is optional. For more information, see section A.5.2 in the EMV 3-D Secure Protocol and Core Functions Specification.	Value is returned from the getTimezoneOffset() method. Example time zone offset values in minutes: If UTC is -5 hours: • 300 • +300 If UTC is +5 hours: • -300	Numeric	_3_browserTZ

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Card/Token Expiry Date	cardExpiryDate	Expiry date of the primary account number (PAN) or token supplied to the 3-D Secure requestor by the cardholder. The requirements for the presence of this element are DS specific.	***Note***: Incoming format is YYMM.	8 CHAR	_3_cardExpiryDate
Cardholder Account Number	acctNumber	Account number that will be used in the authorization request for payment transactions. This value can be represented by PAN or token.	Format represented by ISO 7812.	24 CHAR	_3_acctNumber
Cardholder Billing Address City	billAddrCity	The city of the cardholder's billing address that is associated with the card that was used for this purchase.		56 CHAR	_3_billAddrCity

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Cardholder Billing Address Country	billAddrCountry	The country of the cardholder's billing address that is associated with the card that was used for this purchase. Required if the cardholder's billing address state is present. 01-PA: Required unless market or regional mandate restricts sending this information. 02-NPA: Required (if available) unless market or regional mandate restricts sending this information.	The ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5 in the EMV 3-D Secure Protocol and Core Functions Specification.	8 CHAR	_3_billAddrCountry
Cardholder Billing Address Line 1	billAddrLine1	First line of the street address or equivalent local portion of the cardholder's billing address that is associated with the card that was used for this purchase. 01-PA: Required unless market or regional mandate restricts sending this information. 02-NPA: Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_billAddrLine1

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Cardholder Billing Address Line 2	billAddrLine2	Second line of the street address or equivalent local portion of the cardholder's billing address that is associated with the card that was used for this purchase. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_billAddrLine2
Cardholder Billing Address Line 3	billAddrLine3	Third line of the street address or equivalent local portion of the cardholder's billing address that is associated with the card that was used for this purchase. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_billAddrLine3
Cardholder Billing Address Postal Code	billAddrPostCode	ZIP code or other postal code of the cardholder's billing address that is associated with the card that was used for this purchase. 01-PA: Required unless market or regional mandate restricts sending this information. 02-NPA: Required (if available) unless market or regional mandate restricts sending this information.		16 CHAR	_3_billAddrPostCode

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Cardholder Billing Address State	billAddrState	The state or province of the cardholder's billing address that is associated with the card that was used for this purchase. 01-PA: Required unless market or regional mandate restricts sending this information, or if state is not applicable for this country. 02-NPA: Required (if available) unless market or regional mandate restricts sending this information, or if state is not applicable for this country.	The country subdivision code defined in ISO 3166-2.	8 CHAR	_3_billAddrState
Cardholder Email Address	email	The email address that is associated with the account that is either entered by the cardholder or is on file with the 3-D Secure requestor. Required unless market or regional mandate restricts sending this information.	Needs to meet the requirements in Section 3.4 of IETF RFC 5322.	400 CHAR	_3_email

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name

Cardholder Home Phone Number	homePhone	The home phone number that was provided by the cardholder.
		
		Required (if available) unless market or regional mandate restricts sending this information.
			Country code and subscriber sections of the number represented by the following named fields:
			
			• cc
			• subscriber
			
			For more information about format and length, see ITU-E.164.
			
			Example:
			“homePhone”: {
			“cc”: “1” ,
			“subscriber”: “1234567899”
			}
				16 CHAR	_3_homePhone

Cardholder Information Text	cardholderInfo	Text provided by the ACS or issuer to the cardholder during a frictionless or decoupled transaction. The issuer can provide information to the cardholder (for example, “Additional authentication is needed for this transaction. Please contact (issuer’s name) at xxx-xxx-xxxx (ten-digit phone number). Required if the ACS Decoupled Confirmation Indicator element is set to Y. Otherwise, it is optional for the ACS.	***Note***: If the element is populated, then this information is required to be conveyed to the cardholder by the merchant.	128 CHAR	_3_cardholderInfo

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name

Cardholder Mobile Phone Number	mobilePhone	The mobile phone number that was provided by the cardholder.
		
		Required (if available) unless market or regional mandate restricts sending this information.
			Country code and subscriber sections of the number represented by the following named fields:
			
			• cc
			• subscriber
			
			For more information about format and length, see ITU-E.164.
			
			Example:
			“mobilePhone”: {
			“cc”: “1” ,
			“subscriber”: “1234567899”
			}
				16 CHAR	_3_mobilePhone

Cardholder Name	cardholderName	Name of the cardholder.	Alphanumeric special characters that are listed in Appendix B of EMV Book 4, Cardholder, Attendant, and Acquirer Interface Requirements.	48 CHAR	_3_cardholderName
Cardholder Shipping Address City	shipAddrCity	City portion of the shipping address that was requested by the cardholder. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_shipAddrCity

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Cardholder Shipping Address Country	shipAddrCountry	Country of the shipping address that was requested by the cardholder. Required if cardholder's shipping address state is present. Required (if available) unless market or regional mandate restricts sending this information.	The ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5 in the EMV 3-D Secure Protocol and Core Functions Specification.	8 CHAR	_3_shipAddrCountry
Cardholder Shipping Address Line 1	shipAddrLine1	First line of the street address or equivalent local portion of the shipping address that was requested by the cardholder. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_shipAddrLine1
Cardholder Shipping Address Line 2	shipAddrLine2	Second line of the street address or equivalent local portion of the shipping address that was requested by the cardholder. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_shipAddrLine2
Cardholder Shipping Address Line 3	shipAddrLine3	Third line of the street address or equivalent local portion of the shipping address that was requested by the cardholder. Required (if available) unless market or regional mandate restricts sending this information.		56 CHAR	_3_shipAddrLine3

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Cardholder Shipping Address Postal Code	shipAddrPostCode	The ZIP code or other postal code of the shipping address that was requested by the cardholder. Required (if available) unless market or regional mandate restricts sending this information.		16 CHAR	_3_shipAddrPostCode
Cardholder Shipping Address State	shipAddrState	The state or province of the shipping address that is associated with the card being used for this purchase. Required (if available) unless market or regional mandate restricts sending this information, or State is not applicable for this country.	The country subdivision code defined in ISO 3166-2.	8 CHAR	_3_shipAddrState

Cardholder Work Phone Number	workPhone	The work phone number that was provided by the cardholder.
		
		Required (if available), unless market or regional mandate restricts sending this information.
			Country code and subscriber sections of the number represented by the following named fields:
			
			• cc
			• subscriber
			
			For more information about format and length, see ITU-E.164.
			
			Example:
			“workPhone”: {
			“cc”: “1” ,
			“subscriber”: “1234567899”
			}
				24 CHAR	_3_workPhone

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Challenge Cancellation Indicator	challengeCancel	Indicates to the ACS and the DS whether the authentication has been canceled. Required in the CReq message for 01-APP if the authentication transaction was canceled by user interaction with the cancellation button in the UI or for other reasons as indicated. Required in the RReq message if the ACS identifies that the authentication transaction was canceled for reasons as indicated. A value of 04 or 05 is required when the value in the Transaction Status Reason element is 14.	• 01: Cardholder selected cancel. • 02: Reserved for future EMVCo use. (Values are invalid until defined by EMVCo.) • 03: Transaction timed out—decoupled authentication. • 04: Transaction timed out at ACS—other timeouts. • 05: Transaction timed out at ACS. The first CReq message was not received by the ACS. • 06: Transaction error. • 07: Unknown. • 08: Transaction timed out at SDK. • 09-79: Reserved for future EMVCo use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for future DS use.	8 CHAR	_3_challengeCancel

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Challenge Completion Indicator	challengeCompletionInd	Specifies the state of the ACS challenge cycle and whether the challenge has completed or required additional messages. Must be populated in all CRes messages to convey the current state of the transaction. ***Note***: If set to Y, the ACS will populate the Transaction Status element in the CRes message.	• Y: Challenge was completed, and no further challenge message exchanges are required. • N: Challenge has not completed, and additional challenge message exchanges are required.	8 CHAR	_3_challengeCompletionInd

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Challenge Data Entry	challengeDataEntry	Contains the data that the cardholder entered into the native UI text field. ***Note***: A value of 05 in the ACS UI Type element is not supported. Example: challengeSelectInfo: “challengeDataEntry”:”phone” Required when the ACS UI Type element is 01, 02, or 03, challenge data has been entered in the UI, and both the Challenge Cancellation Indicator element and Resend Challenge Information Code element are not present. For Challenge Data Entry element conditions, see Table A.14 in the EMV 3-D Secure Protocol and Core Functions Specification.		48 CHAR	_3_challengeDataEntry

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Challenge HTML Data Entry	challengeHTMLDataEntry	Data that the cardholder entered into the HTML UI. ***Note***: ACS UI Types 01, 02, 03, and 04 are not supported. Required when the ACS UI Type element is 05 and the Challenge Cancellation Indicator element is not present.		400 CHAR	_3_challengeHTMLDataEntry
Challenge Information Header	challengeInfoHeader	Header text that for the challenge information screen that is being presented.	If this element is populated, then this information is displayed to the cardholder.	48 CHAR	_3_challengeInfoHeader
Challenge Information Label	challengeInfoLabel	Label to modify the Challenge Data Entry element that is provided by the issuer.	If this element is populated, then this information is displayed to the cardholder.	48 CHAR	_3_challengeInfoLabel
Challenge Information Text	challengeInfoText	Text provided by the ACS or issuer to the cardholder during the Challenge Message exchange.	If this element is populated, then this information is displayed to the cardholder. ***Note***: Carriage returns are supported in this element and are represented by an “\n”.	400 CHAR	_3_challengeInfoText

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Challenge No Entry	challengeNoEntry	Specifies whether the cardholder submitted an empty response (that is, no data was entered in the UI). Note: If present, then this element contains a value of Y. Required when the ACS UI Type element is 01, 02, or 03, challenge data has been entered in the UI, and both the Challenge Cancellation Indicator element and Resend Challenge Information Code element are not present.	Y: No data entry.	8 CHAR	_3_challengeNoEntry
Challenge Window Size	challengeWindowSize	Dimensions of the challenge window that has been displayed to the cardholder. The ACS replies with content that is formatted to appropriately render in this window to provide the best possible user experience. Preconfigured sizes are width x height in pixels of the window that is displayed in the cardholder's browser window.	• 01: 250 x 400. • 02: 390 x 400. • 03: 500 x 600. • 04: 600 x 400. • 05: Full screen.	8 CHAR	_3_challengeWindowSize

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Device Channel	deviceChannel	Indicates the type of channel interface that is being used to initiate the transaction.	• 01: Application-based (APP). • 02: Browser (BRW). • 03: 3-D Secure requestor initiated (3RI). • 04-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_deviceChannel
DS End Protocol Version	dsEndProtocolVersion	The most recent active protocol version that is supported for the DS. ***Note***: Optional within the card range data (as defined in Table A.6 in the EMV 3-D Secure Protocol and Core Functions Specification).		8 CHAR	_3_dsEndProtocolVersion
DS Start Protocol Version	dsStartProtocolVersion	The most recent active protocol version that is supported for the DS. ***Note***: Optional within the card range data (as defined in Table A.6 in the EMV 3-D Secure Protocol and Core Functions Specification).		8 CHAR	_3_dsStartProtocolVersion

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
DS Reference Number	dsReferenceNumber	EMVCo-assigned unique identifier to track approved DS. The DS populates the AReq message with this element before passing to the ACS.		32 CHAR	_3_dsReferenceNumber
DS Transaction ID	dsTransID	Universally unique transaction identifier that is assigned by the DS to identify a single transaction The DS populates the AReq message with this element before passing to the ACS. Required in the error message, if available (for example, it can be obtained from a message or is being generated).	Canonical format as defined in IETF RFC 4122. You can use any of the specified versions if the output meets specified requirements.	40 CHAR	_3_dsTransID
Electronic Commerce Indicator (ECI)	eci	Payment system-specific value provided by the ACS or DS to indicate the results of the attempt to authenticate the cardholder. The requirements for the presence of this element are DS specific.	Payment system specific.	8 CHAR	_3_eci
Error Code	errorCode	Code indicating the type of problem that is identified in the message.	For valid values, see Table A.4 in the EMV 3-D Secure Protocol and Core Functions Specification.	8 CHAR	_3_errorCode

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Error Component	errorComponent	Code indicating the 3-D Secure component that identified the error.	• C: 3-D Secure SDK. • S: 3-D Secure server. • D: DS. • A: ACS.	8 CHAR	_3_errorComponent
Error Message Type	errorMessageType	Identifies the message type that was identified as erroneous. Conditional on whether the message type is recognized.	See the Message Type element.	8 CHAR	_3_errorMessageType
EMV Payment Token Indicator	payTokenInd	A value of true indicates that the transaction was de-tokenized before being received by the ACS. This element is populated by the system that resides in the 3-D Secure domain where the de-tokenization occurred (that is, the 3-D Secure server or the DS). ***Note***: The Boolean value of true is the only valid response for this field when it is present. Required if there is a de-tokenization of an account number.	True	8 CHAR	_3_payTokenInd

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
EMV Payment Token Source	payTokenSource	This element is populated by the system that resides in the 3-D Secure domain where the de-tokenization occurred. Required if the EMV Payment Token Indicator element is true.	• 01: 3-D Secure server. • 02: DS. • 03-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_payTokenSource
Expandable Information Label	expandInfoLabel	Label displayed to the cardholder for the content in Expandable Information Text element.		48 CHAR	_3_expandInfoLabel
Expandable Information Text	expandInfoText	Text provided by the issuer from the ACS that is displayed to the cardholder for additional information. The format is an expandable text field.	***Note***: Carriage returns are supported in this element and are represented by an "\n".	48 CHAR	_3_expandInfoText
Installment Payment Data	purchaseInstalData	Indicates the maximum number of authorizations permitted for installment payments. Required if the merchant and cardholder have agreed to installment payments (that is, if the value in the 3-D Secure requestor's Authentication Indicator element is 03). This element is omitted if the transaction not an installment payment authentication.	Value should be greater than 1. Example values that would be accepted: • 2 • 02 • 002	Numeric	_3_purchaseInstalData

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Interaction Counter	interactionCounter	Indicates the number of authentication cycles that were attempted by the cardholder. This value is tracked by the ACS.		Numeric	_3_interactionCounter
Merchant Category Code	mcc	DS-specific code that describes the merchant's type of business, product, or service. This element is optional, but you are strongly recommended to include it for 02-NPA if the merchant is also the 3-D Secure requestor.	This value correlates to the merchant category code as defined by each payment system or DS.	8 CHAR	_3_mcc
Merchant Country Code	merchantCountryCode	Country code of the merchant. This value correlates to the merchant country code as defined by each payment system or DS. This element is optional, but you are strongly recommended to include it for 02-NPA if the merchant is also the 3-D Secure requestor.	The ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5 in the EMV 3-D Secure Protocol and Core Functions Specification. ***Note***: The same value also must be used in the authorization request.	8 CHAR	_3_merchantCountryCode

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Message Category	messageCategory	Identifies the category of the message for a specific use case.	• 01: PA. • 02: NPA. • 03-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_messageCategory
Message Type	messageType	Identifies the type of message that is passed.	• AReq • ARes • CReq • CRes • PReq • PRes • RReq • RRes • Erro	8 CHAR	_3_messageType

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Message Version Number	messageVersion	Protocol version identifier. The protocol version number of the specification that is used by the system that created the message. The Message Version Number element is set by the 3-D Secure server that originates the protocol with the AReq message. The Message Version Number element does not change during a 3-D Secure transaction.	For valid values, see Table 1.5 in the EMV 3-D Secure Protocol and Core Functions Specification.	8 CHAR	_3_messageVersion
Notification URL	notificationURL	Fully qualified URL of the system that receives the CRes message or the error message. The CRes message is posted by the ACS through the cardholder's browser at the end of the challenge and receipt of the RRes message.	A fully qualified URL.	400 CHAR	_3_notificationURL

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
OOB App Label	oobAppLabel	Label to be displayed for the link to the OOB application URL (for example: "oobAppLabel": "Click here to open Your Bank App"). ***Note***: This element has been defined to support future enhancements to the OOB message flow. An ACS does not provide this value and a 3-D Secure SDK does not perform any processing and does not display the OOB App Label element in this version of the specification.		48 CHAR	_3_oobAppLabel
OOB App URL	oobAppURL	Mobile deep link to an authentication application that was used in the out-of-band authentication. The application URL opens the appropriate location within the authentication application. ***Note***: This element has been defined to support future enhancements to the OOB message flow. An ACS does not provide this value and a 3-D Secure SDK does not perform any processing and does not display the OOB App Label element in this version of the specification.	A fully qualified URL.	300 CHAR	_3_oobAppURL

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
OOB Continuation Indicator	oobContinue	Indicator to notify the ACS that the cardholder has completed the authentication as requested by clicking the Continue button in an OOB authentication method. ***Note***: The Boolean value of true is the only valid response for this element when it is present. Required when the ACS UI Type element is 04, OOB (the cardholder has selected that option on the device).	True	8 CHAR	_3_oobContinue
OOB Continuation Label	oobContinueLabel	Label to be used in the UI for the button that the user selects when they have completed the OOB authentication. Required when the ACS UI Type element is 04, OOB (the cardholder has selected that option on the device). ***Note***: If present, either of the following elements must also be present: • Challenge Information Header element • Challenge Information Text element		48 CHAR	_3_oobContinueLabel

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Purchase Amount	purchaseAmount	Purchase amount in minor units of currency with all punctuation removed. When used in conjunction with the Purchase Currency Exponent element, proper punctuation can be calculated. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03.	An example: purchase amount is USD 123.45. Example values that would be accepted are the following: • 12345 • 012345 • 0012345	Numeric	_3_purchaseAmount
Purchase Currency	purchaseCurrency	Currency in which the purchase amount is expressed. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03.	The ISO 3166-1 numeric three-digit country code, other than exceptions listed in Table A.5 in the EMV 3-D Secure Protocol and Core Functions Specification.	8 CHAR	_3_purchaseCurrency
Purchase Currency Exponent	purchaseExponent	Minor units of currency as specified in the ISO 4217 currency codes. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03.	Example values that would be accepted are the following: • USD=2 • Yen=0	Numeric	_3_purchaseExponent
Purchase Date & Time	purchaseDate	Date and time (in UTC) of the purchase. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03. ***Note***: Incoming datetime format is YYYYMMDDHHMMSS.		Datetime	_3_purchaseDate

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Recurring Expiry	recurringExpiry	Date after which no further authorizations will be performed. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03. ***Note***: Incoming datetime format is YYYYMMDD.		Date	_3_recurringExpiry
Recurring Frequency	recurringFrequency	Indicates the minimum number of days between authorizations. Required for 02-NPA if the 3DS Requestor Authentication Indicator element is 02 or 03.	Example values that would be accepted are the following: • 31 • 031 • 0031	Numeric	_3_recurringFrequency
Resend Challenge Information Code	resendChallenge	Indicator to the ACS to resend the challenge information code to the cardholder. Required for the native UI text field if the cardholder asks the ACS to resend the challenge information.	• Y: Resend. • N: Do not resend.	8 CHAR	_3_resendChallenge
Resend Information Label	resendInformationLabel	Label to be used in the UI for the button that the user selects when they would like the authentication information resent. Required for the native UI text field if the ACS allows the cardholder to request a resend of the authentication information.		48 CHAR	_3_resendInformationLabel

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Results Message Status	resultsStatus	Indicates the status of the results request message from the 3-D Secure server to provide additional data to the ACS. The Results Message Status element indicates whether the message was successfully received for further processing or will be used to provide more detail about why the challenge could not be completed from the 3-D Secure client to the ACS.	• 01: The RReq message received for further processing. • 02: The CReq message was not sent to the ACS by the 3-D Secure requestor. (The 3-D Secure server or 3-D Secure requestor opted out of the challenge.) • 03: The ARes message was not delivered to the 3-D Secure requestor due to a technical error. (The Transaction Status element is C or D.) • 04-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_resultsStatus
SDK App ID	sdkAppID	Universally unique ID that is created when the 3-D Secure requestor application is installed on a consumer device. A new ID is generated and stored by the 3-D Secure SDK for each installation.	Canonical format as defined in IETF RFC 4122. This transaction might use any of the specified versions as long as the output meets specified requirements.	40 CHAR	_3_sdkAppID

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
SDK Counter SDK to ACS	sdkCounterStoA	Counter used as a security measure in the 3-D Secure SDK to ACS secure channel.		Numeric	_3_sdkCounterStoA
SDK Ephemeral Public Key (QC)	sdkEphemPubKey	Public key component of the ephemeral key pair that is generated by the 3-D Secure SDK and used to establish session keys between the 3-D Secure SDK and the ACS. In the AReq message, this element is present as its own object. In the ARes message, this element is contained within the ACS signed content JWS Object. For more information, see Section 6.2.3.1 in the EMV 3-D Secure Protocol and Core Functions Specification. For the ARes message, see the ACS signed content JSON web signature (JWS) object.		400 CHAR	_3_sdkEphemPubKey
SDK Maximum Timeout	sdkMaxTimeout	Indicates the maximum amount of time (in minutes) for all exchanges.	A value greater than or equal to 5.	Numeric	_3_sdkMaxTimeout

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
SDK Reference Number	sdkReferenceNumber	Identifies the vendor and version for the 3-D Secure SDK that is integrated in a 3-D Secure requestor application that is assigned by EMVCo when the 3-D Secure SDK is approved.		32 CHAR	_3_sdkReferenceNumber
SDK Transaction ID	sdkTransID	Universally unique transaction identifier that is assigned by the 3-D Secure SDK to identify a single transaction. Required in the error message, if available (for example, it can be obtained from a message or is being generated).	Canonical format as defined in IETF RFC 4122. This transaction might use any of the specified versions if the output meets specified requirements.	40 CHAR	_3_sdkTransID

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Submit Authentication Label	submitAuthenticationLabel	Label used in the UI for the button that the user selects when they have completed the authentication. ***Note***: This is not used for OOB authentication. Required when the ACS UI Type element is 01, 02, or 03. ***Note***: If present, either of the following elements must also be present: • Challenge Information Header element • Challenge Information Label element • Challenge Information Text element		48 CHAR	_3_submitAuthenticationLabel
Transaction Status	transStatus	Indicates whether a transaction qualifies as an authenticated transaction or an account verification. ***Note***: The Final CRes message can contain only a value of Y or N. ***Note***: If the 3-D Secure Requestor Challenge Indicator element is 06	• Y: Authentication verification was successful. • N: Not authenticated or the account was not verified. Transaction denied.	8 CHAR	_3_transStatus

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
		(No challenge was requested (data share only)), then a value of C in this Transaction Status element is not valid. For 02-NPA, Conditional as defined by the DS, see Table A.15, Transaction Status Conditions, in the EMV 3-D Secure Protocol and Core Functions Specification.	• U: Authentication or account verification could not be performed because of a technical or other problem, as indicated in the ARes or RReq messages. • A: Attempts at processing were performed. Transaction was not authenticated or verified, but a proof of attempted authentication or verification is provided. • C: Challenge is required. Additional authentication is required using a CReq or CRes message. • D: Challenge is required. Decoupled authentication is confirmed. • R: Authentication or account verification was rejected. The issuer is rejecting verification and requests that authorization not be attempted.		

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
			• I: Informational only. 3-D Secure requestor challenge preference was acknowledged.		
Transaction Status Reason	transStatusReason	Provides information about why the Transaction Status element has the specified value. For 01-PA, this element is required if the Transaction Status element is N, U, or R. For 02-NPA, this element is conditional as defined by the DS.	• 01: Card authentication failed. • 02: Unknown device. • 03: Unsupported device. • 04: Exceeds authentication frequency limit. • 05: Expired card. • 06: Invalid card number. • 07: Invalid transaction. • 08: No card record. • 09: Security failure. • 10: Stolen card. • 11: Suspected fraud. • 12: Transaction is not permitted for the cardholder. • 13: Cardholder is not enrolled in the service.	8 CHAR	_3_transStatusReason

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
			• 14: Transaction timed out at the ACS. • 15: Low confidence. • 16: Medium confidence. • 17: High confidence. • 18: Very High confidence. • 19: Exceeds the ACS' maximum number of challenges. • 20: Non-payment transaction is not supported. • 21: 3RI transaction is not supported. • 22: ACS technical issue. • 23: Decoupled authentication is required by the ACS but was not requested by the 3-D Secure requestor. • 24: 3-D Secure requestor decoupled maximum expiry time was exceeded.		

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
			• 25: Decoupled authentication was provided with insufficient time to authenticate the cardholder. ACS will not make an authentication attempt. • 26: Authentication was attempted, but not performed by the cardholder. • 27-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.)		
Transaction Type	transType	Identifies the type of transaction that is being authenticated. This element is required in some markets (for example, for merchants in Brazil). Otherwise, this element is optional.	• 01: Goods or service purchase. • 03: Check acceptance. • 10: Account funding. • 11: Quasi-cash transaction. • 28: Prepaid activation and load. Note: Values are derived from the 8583 ISO standard.	8 CHAR	_3_transType

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Trust Listing Data Entry	Trustlisting DataEntry	Indicator provided by the SDK to the ACS to confirm whether the cardholder chose accept listing. If the Trustlisting Information Text element is present in the CRes message, then the SDK must provide this element to the ACS in the CReq message.	• Y: Accept listing is confirmed. • N: Accept listing is not confirmed.	8 CHAR	_3_whitelistingDataEntry
Trust Listing Information Text	trustlistingInfoText	Text provided by the ACS or issuer to the cardholder during an accept listing transaction (for example, “Would you like to add this merchant to your accept list?”). If this element is present, then it must be displayed by the SDK.		64 CHAR	_3_whitelistingInfoText

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
Trust List Status	trustListStatus	Enables the communication of trusted beneficiary or accept list status between the ACS, the DS, and the 3-D Secure requestor.	• Y: 3-D Secure requestor is accept listed by the cardholder. • N: 3-D Secure requestor is not accept listed by the cardholder. • E: Not eligible as determined by the issuer. • P: Pending confirmation by the cardholder. • R: Cardholder rejected. • U: Accept list status unknown, unavailable, or does not apply. ***Note***: Valid values that are in the AReq message are Y or N.	8 CHAR	_3_whiteListStatus

Data Element	Field Name	Description	Values Accepted	Data Type	Client Input Variable Name
trustListStatus Source	trustListStatusSource	This element is populated by the value in the trustlistStatus element. This element is required if the trustlistStatus element is present.	• 01: 3-D Secure server. • 02: DS. • 03: ACS. • 04-79: Reserved for EMVCo future use. (Values are invalid until defined by EMVCo.) • 80-99: Reserved for DS use.	8 CHAR	_3_whiteListStatusSource
Why Information Label	whyInfoLabel	Label to be displayed to the cardholder for the "why" information section.		48 CHAR	_3_whyInfoLabel
Why Information Text	whyInfoText	Text provided by the issuer that is displayed to the cardholder to explain why the cardholder is being asked to perform the authentication task.	***Note***: Carriage returns are supported in this element and are represented by an “\n”.	400 CHAR	_3_whyInfoText

References

Website of EMV® 3-D Secure. **https://www.emvco.com/emv-technologies/3d-secure/**.

EVM Technologies. “EMV-3D Secure Protocol and Core Functions Specifications.” **https://www.emvco.com/emv-technologies/3d-secure/**. Last Modified 30 September, 2021.

Open SSL Software Foundation. 2010. “OpenSSL Cryptography and SSL/TLS Toolkit.” Available at **www.openssl.org/**.

SAS Institute Inc. 2011. “Configuring IBM WebSphere Application Server 7 for Web Authentication with SAS® 9.3 Web Applications.” Cary, NC. Available at **support.sas.com/resources/thirdpartysupport/v93/appservers/ConfiguringWAS7WebAuth.pdf**

Release Information Content Version: 1.0 October 2021

To contact your local SAS office, please visit: sas.com/offices