3DS Server API specification

Version 1.0

Contents

Table of Contents

1   Version History

Version	Implemented By	Revision Date	Reason
1.0	Wibmo	10 Jan 2023	

Item Functionality

1.1 Business Need

Performing 3D Secure Authentication of Browser and SDK transactions on a Merchant using 3DS 2.1.0,3DS 2.2.0 & VBV 1.0.2 protocol.
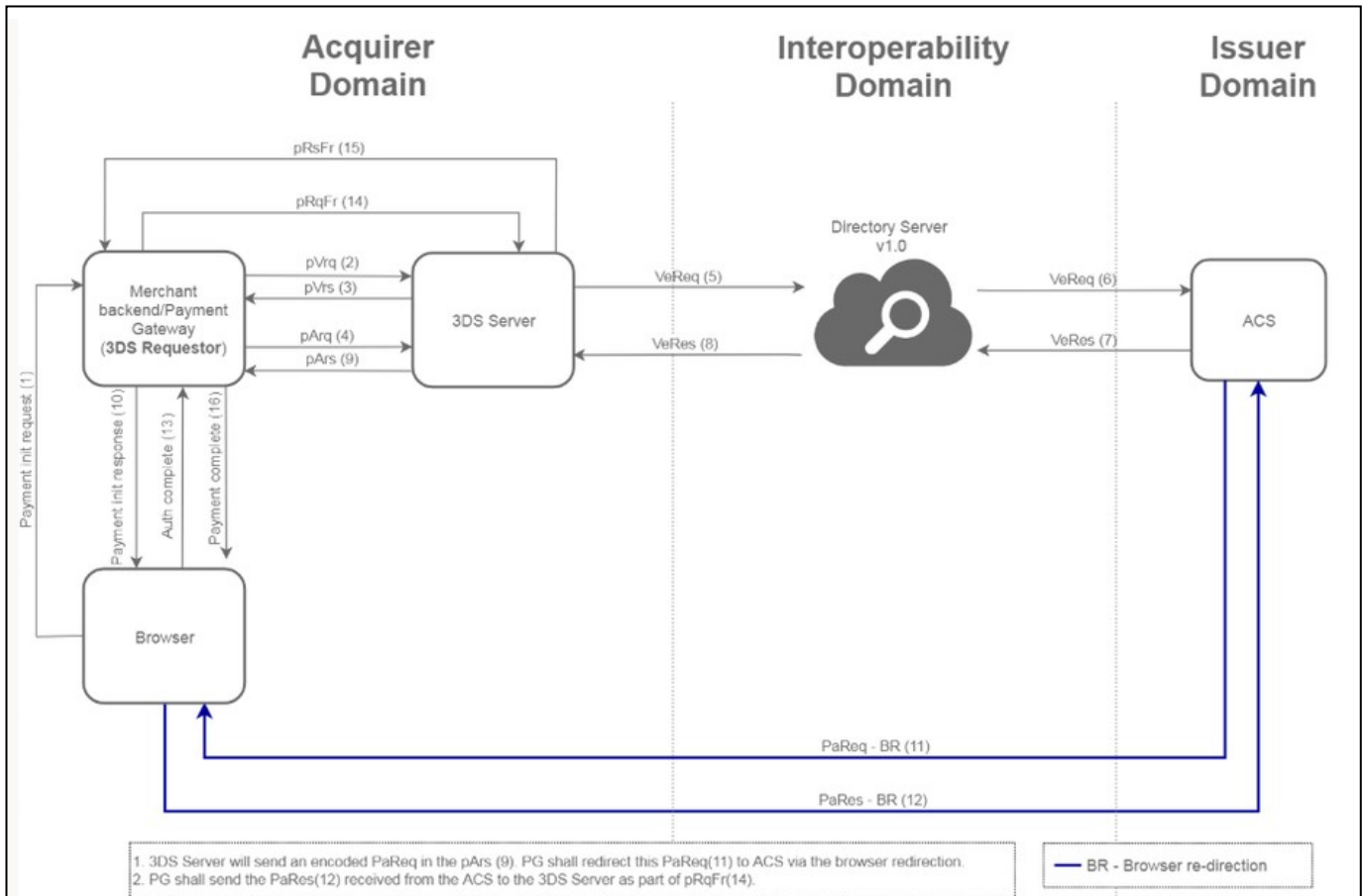
1.2 Use Cases

This document describes API specifications of

1) Browser Frictionless Authentication

2) Browser Challenge Authentication

3) SDK Frictionless Authentication

4) SDK Challenge Authentication

2 Transaction Flow
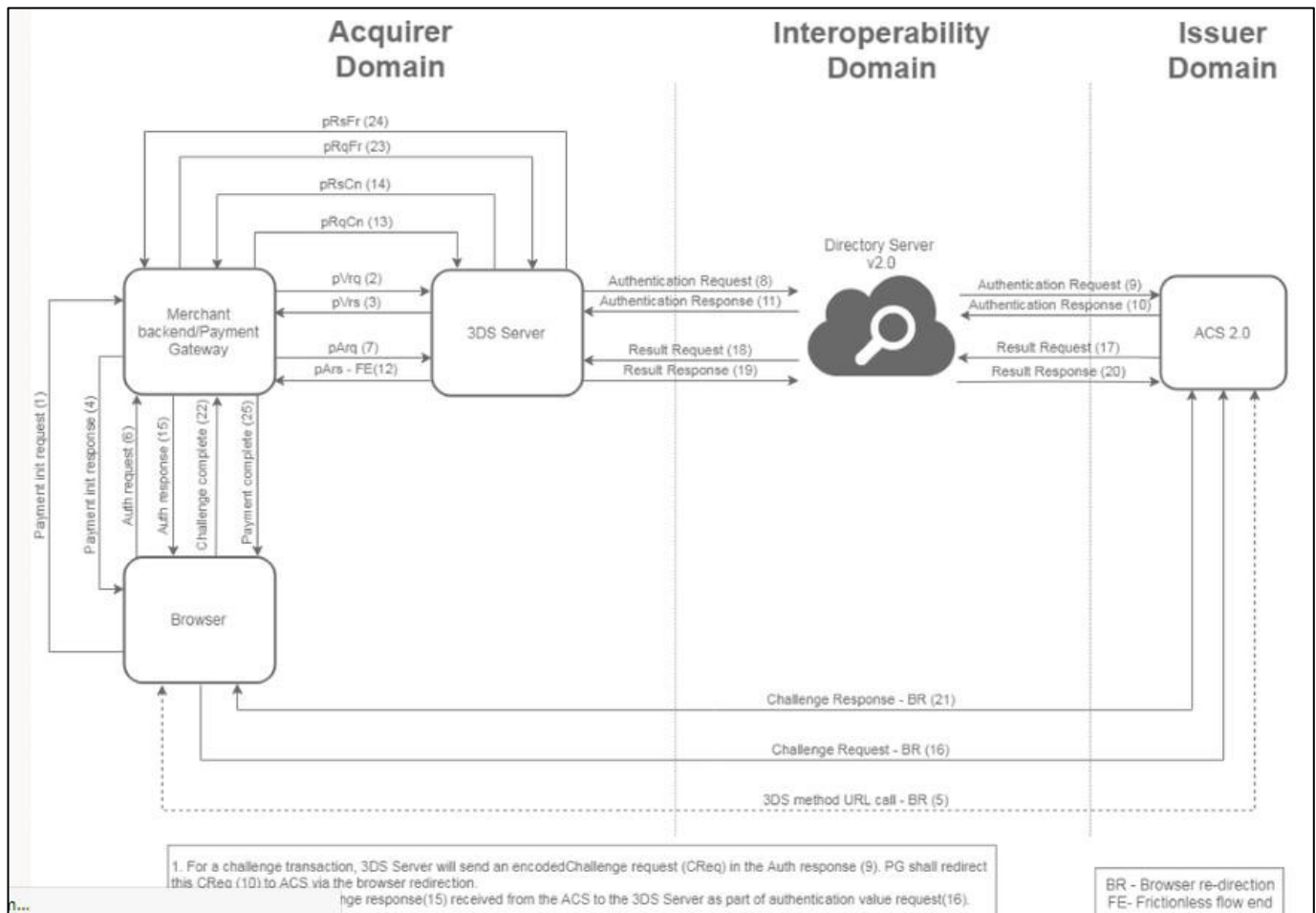
2.1 3DS 1.0 Flow

1) 3DS Requestor initiates pVrq(2) versioning request with 3DS Server

2) 3DS Server responds with pVrs(3) versioning response and provides the version supported by ACS and DS for the card BIN range. In this case, version is 1.0.2

3) 3DS Requestor initiates pArq(4) with 3DS Server with the API request with message_version as 1.0.2

4) 3DS Server initiates Vereq(3DS 1.0) message with DS and receives Veres from ACS

5) Once Veres is received with status = "Y", 3DS Server will create the Pareq, and respond to 3DS requestor with pArs(9), with encoded Pareq and ACS URL for Pareq redirection.

6) 3DS Requestor to redirect customer browsing by posting the Pareq(11) received from 3DS Server to the ACS URL.

7) ACS to perform 1.0 processing and provide Pares (12) by redirecting the browser back to 3DS Requestor.

8) 3DS Requestor to make pRqFr (14) call to 3DS Server and pass the Pares received from ACS to 3DS Server.

9) 3DS Server decodes Pares and extracts key fields like eci, cavv.

10) 3DS server responds to 3DS Requestor with pRsFr with eci, cavv.

11) 3DS requestor initiates authorization call with acquirer.

2.2   3DS 2.0 Browser Flow

1) 3DS Requestor initiates pVrq(2) versioning request with 3DS Server

2) 3DS Server responds with pVrs(3) versioning response and provides the version supported by ACS and DS for the card BIN range. In this case, version is 2.1.0

3) If a ACS method URL is available as part of the pVrs response, the 3DS requestor will load the method URL and redirect to ACS.

4) Once the method URL notification is received from ACS, the 3DS Requestor initiates pArq(7) with 3DS Server with message_version as 2.1.0

5) 3DS Server initiates AReq message with DS which is then sent to the ACS. ACS processes the request and sends an ARes.

6) If the ARes is received with status = "Y", 3DS Server will respond to the 3DS requestor in the pArs(12) with key values eci and cavv.

7) If the ARes is received with status = "C", 3DS Server will create a CReq(Challenge request-16), base64 encode it and initiate pArs(12) with the encoded Creq and ACS URL for browser redirection.

8) 3DS Requestor redirects customer browsing by posting the CReq(16) received from 3DS Server to the ACS URL.

9) ACS to perform challenge processing and complete RREQ/RRES leg.

10) After receiving RRES, ACS redirects customer browser back to 3DS Requestor with a Cres(Challenge response-21)

11) 3DS Requestor to make pRqFr (23) call to 3DS Server and pass the CRes received from ACS to 3DS Server.

12) 3DS Server decodes CRes and extracts key fields like eci, cavv.

13) 3DS server responds to 3DS Requestor with pRsFr(24) with eci, cavv.

14) 3DS requestor initiates authorization call with acquirer.

2.3   3DS 2.0 APP Flow
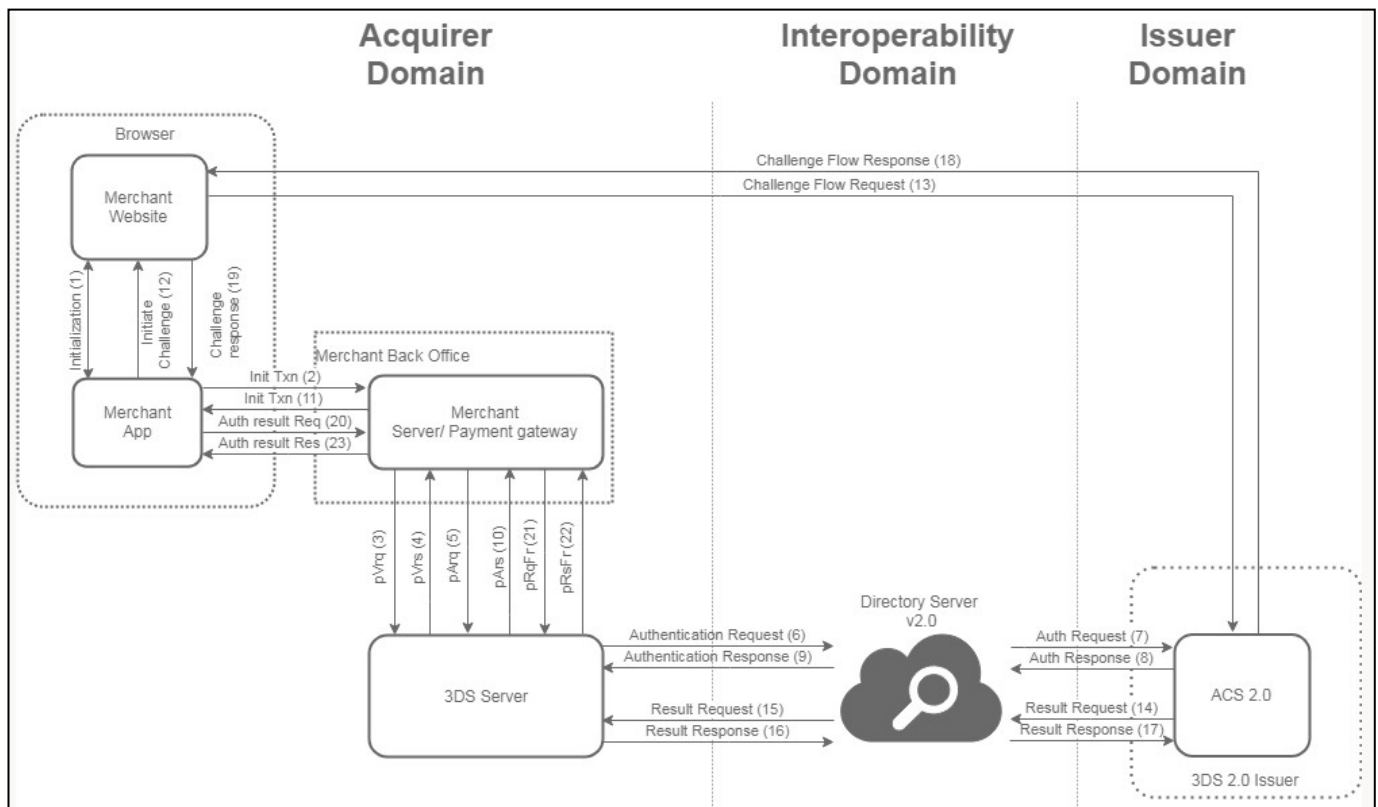
1) Merchant app initializes (1) SDK and receives device data in the response.

2) Merchant app sends the device data to the 3DS requestor.

3) 3DS Requestor initiates pVrq(3) versioning request with 3DS Server

4) 3DS Server responds with pVrs(4) versioning response and provides the version supported by ACS and DS for the card BIN range. In this case, version is 2.1.0.

5) The 3DS Requestor initiates pArq(5) with 3DS Server with message_version as 2.1.0

6) 3DS Server encrypts the device data and initiates AReq message with DS which is then sent to the ACS. ACS processes the request and sends an ARes.

7) If the ARes is received with status = "Y", 3DS Server will respond to the 3DS requestor in the pArs(10) with key values eci and cavv.

8) If the ARes is received with status = "C", 3DS Server will initiate pArs(10) and notify the 3DS Requestor to initiate a challenge request.

9) The merchant app is notified and requests SDK to initiates challenge request (12).

10) The SDK initiates a challenge request CReq(13) to the ACS directly.

11) ACS to perform challenge processing and complete RREQ/RRES leg.

12) After receiving RRES, ACS responds to SDK with a final Cres(Challenge response-18). Multiple Creq/Cres exchanges happen until the final validation is complete.

13) 3DS requestor is notified of the challenge completion.

14) 3DS Requestor to make pRqFr(21) call to 3DS Server.

15) 3DS server responds to 3DS Requestor with pRsFr(22) with eci, cavv.

16) 3DS requestor initiates authorization call with acquirer.

3   Interface Elements

3.1   Encrypted payload.

Request Header

Parameter	M/O/C	Sample
x-api-key	M	Actual api-key will be provided from PG during Onboarding - 777a9184-2e70-11ed-b928-005056b59d84
pgInstanceId	M	Acquirer Id provided by Wibmo – Example 8645
merchantId	M	Same as pgInstanceId

RequestBody

Parameter	M/O/C	Sample
signedEncRequestPayload	M	Request PayLoad Signed with acquirer PrivateKey, encrypted with AES256 KEY
requestSymmetricEncKey	M	Encrypted AES256 KEY with Wibmo's Public Key
iv	M	Initialization Vector (IV) value
pgInstanceId	M	Acquirer Id provided by Wibmo – Example 8645
merchantId	M	Same as pgInstanceId
clientReferenceId	C	Reference id generated at client end. If not send our API will generate it.
var1	O	
var2	O	
var3	O	

Sample Request

{

  "signedEncRequestPayload" :

"xFsQAMFBmTmA1+7X3b8u+Vyul/z5yr3iz3aISnWjfNjGo3AzES9PAj7its52NZCsrYaYkxcH2b+SPm1Jt6LFgyci07wy7UzcoNQu4KN9L0giYtHa8sAF
5rIN5xUqOiRw7yydf20TARf63Y5dMLCYeT/G+2NCgwUWKNVGgMhicm2pK+uq12IrPITKt3Qrm7ksbhxqI76N4NAGw4SUT6bAezMfPgwcBcsU922soKA8/
zf3Z/lj1lklZnsaeONs08iAv7yZlp1fguOZR/RIF//JuGFkYl5fWvO6/LWiOmFokAckWW3GfqGW47B+lXXXMCcX0O/H0NTmywshe6ZsP1PXAY1zpakxIh
KuAVJM7SlvROHGdb4x6YU07p/rBaj/ksY5tGwL/HeHOfY1pNYcAOdN3pU5c5QLwBMUM2+esY6XfyMXpmqU6CqRVWaeU9Rybv+1+Uq1Rq4heVYbEnAXT7t
1ih7zGRlG6CnE/SxPgNaUAYBSD/2ZjykD57hWUabbhkDHF8ELLTphzOiVmym1QN3zESbwVrHFjjZkGT3aelexxIEVndeI5b7ZaYf2JPo/SMfaCibeAYOG
adUNwJNd2h2qwAe4+3HyT6FXoDibyl7yKGZKx5yjiQWL06Wto3GI+Itl9aZ1bOGk6i7pxjbbV/D4x0LI6BblWSp4pr/4df8aUuTSZWqn6gN8BIEx8wbFW
jbDsHyPFAz3+WRAEJ8eZzpgXn/Ik4Cn6/42mkUJYRiCr+bAqUgpMizGFmKWG9/UX1gxcAXvAGhGDzBhDn3iDg0dz4wnvkQKCCaYnt828iE50Vepq2cU6P
dD5403ki5WmL0l9ToblErbOHiWQy7+PZ4hoGKR5eQ3hhkfiwbXlqidYxH1WfJrUijVH9lH06d+YLu44YWj0WlRjZ5mP3d+oTs2KDujRqGab2NfD643fKY
RhkU+atyJ9aKtlO9OB370XoL+d1g4GkFStC7y8P6iJSZ6Jp9Jew7sTbOzTsLL/OQ2ZuzBsGvn4WlAp3vsj1mh8GdEjG2QQPgYxfMa+4z3FFmbWznLmIhu
IVvQmlvEWGeInQb9pzN+Atnt4P/gHQ9sbEDwR4Yw6CcXqqBmdlX0vIM9/7wXHksWLPpbx+80VwMRV8XYUh40kPJZlXmbUv981mu04h/mFIysXJUyXyRc3
Ah09RPfKMqfTYwYNuVJ43YTjgqS01UyZj4ntcwO86t+1S39NoWdtssDUQO9TFqvPdqRYzrUE7nqWaBQnmknN906fCFBJWx8PMKCdpdmLvUM39surndFpF
kwqowibvyjhqi6aa+C5D5U0rOZtFyLTFKAzaHyunm1iqjs2LqtQcL5ML+SIcSroPU4Bp70AfM7zgHu1YXRc9jfJFFfOadPSyClkzbs8pz3VAHxZVV+1Tm
+Ry7gNjePkLJJSuIC8nNh2inTzpgCmNYHaUBQxko2tomtwWBO3SEn1ZfvSWLud1Wx7D8OgtXvPhVNz6VAfJlrTuB7Zhz6L45CoX0oJb5IlVpdwyXbQLlb
Mrp/N4kKT2EpPuIwkMFfpsvd6sDFJKnlGYqpFRtvnTcRJM/dlq5Y0+mm+yEunryZlXK07AZal935MwPDG7g5FGVQ0HPlZ+o131xpbihGz4h6NLRbnf25u
o9EFFHk9q4DrRKqSmk9q/nQNko8eygu+nN2RtAeydqLiRSaLUG3iimpJWkWij4/d3ez524QkKBPVRysnLuEMHD/GfnNyGx+XOneHDObzISly+8kFt6gWu
gucEmPnT1h2C71/iXbFF7dcu5qi1+0BHfIDNzac8vXOpvi82g1Ni6HLqBtYn30ZRrctGzQrh9U8U5JLPaEai6TS1jILmrdIDJlW0oQl0PUQm2q1QoHW16

ZT2vwwhyXCD7+2wHhcm4mdr7zh2/q0LENNtW4khjJ13aZPaqprkk66pLO3JxvMMyrs7wzspYqvuxJ7lT2zGcPptnNioPY8Gs9Mn32mZB8UT439PKnbL5C
4f5hEUPsBp9htXLWX+ZEELFoyoISU+tlPrqo//H6Lr3sXaVeQSsmCYMS2W6hFi43Loe5coWA0P8ClUujzSL6H0mfF1p9QkaTy6q5zzvwKEO9X4z8+r+ev
RIZ6nNcE8J+12map6vxuw==",

  "requestSymmetricEncKey" :
"cHOj205sox0eAFUEajWravTUzAP+5b1Yk7rbyIvxszj64hbFHQjxVS8MATGgioC0i8kso6aDPgckesWZCMAtOERWbYeEY3nA8AXr/8pRlZntiowbqqUT
Hodj1hTh+7+wOJ3Eo6l4RVgIEru/AZ0fVq5c9oIL+8QmGj9gFJpO4GRAr++lx2eee2LcsXoZk6NcbrevJCogjxvVFrBrq0sDpriI3KMCo8bgTiG7TMyB+
TSc/dx6En4JEDhy5iqws4lJcOw8C/JZDu9qb8NqG1jalPb7cGrHarOrfNMWOEwu4jFeUEONb37Y6CnwT39sykcgOLSFqSTH4O3CDzbuDLnsBA==",

  "pgInstanceId" : "abcdefgh",

  "merchantId" : "pqrstuvws123",

   "iv" : "nbXTfdxxouQoOllf",

  "clientReferenceId" : "aaddvkklllle123344"

}

Response Message Body

Parameter	M/O/C	Sample
signedEncResponsePayload	M	Response PayLoad Signed with wibmo PrivateKey, encrypted with AES256 KEY
responseSymmetricEncKey	M	Encrypted AES256 KEY with Acquirer Public Key
iv	M	Action To Be Performed
clientReferenceId	M	Same Request clientReferenceId will be returned
statusCode	M	Transaction status is success or failure
errorMessage	M	Success or Failure message
var1	O	
var2	O	
var3	O	

Sample Response

{

   "signedEncResponsePayload":
"LTPpSHNwAuEthTTDlmO0G9QY5dKfT7COTFaJe+7FhKkrgVYrSkJIxQeFWhi0tEghUDm54yE4QokEk42ifRpenCcGC1fLF+ReOsErEhCEHy1mUUE+34so
WWdhXqEY3GflWyJK6v7sr1A6UVKgJCraSpJy5Ubhzrxtt10Jh/bojo6NJysRQszgEnYUagzDqW5YVIjgG9InJ/2meJpQt3aCx9scgHG6A8iJBqNmaJYg1
cjB4KVRZGFzRSu3TKF3miSmwG7CU1qC8+9F+DyD2ExQV9/8puN5bpVlJkiOnye1GGzyBh3LXXGYDS7yaKoR6joGsPuFrJN48uZy9UqrS/qvaCo9/zGhh2
gZEe1qxGNxV649AW5pdQMdrvRGgYRghioAOtgLJneSnADjO5L4xWEn1wnY/QjTxpCPh52n4K7PxtjxPS6wOTZaqOUY32+fn7Fn3O3pjBr5go6Dasynkl2
UeRs4obc5ReUD3AwSonvqVAtLCyApmmCUAHZloCWVd20NHubzQRPJHPmHjx+bmTn6etPO2w/rS4Y1KhGlSQ5WzDUJzYh3MMOhV7aKXTeKmbxLuEKQebZl
8ajEIv3DKLZjAk5cmuFk8el8TuiTpsXTxnqR7Azapc2JZHZBBoMvhcpW/1ACnbsdI3vc9kltEQThRWXqhuyoIMdijUifUmNAScStbZMMPGbNdx1tey313
YiP6awakCCHyEyFHsmofOPQRMxxoMe5z32UF1Ky/mzVOde1Abn8ZLJuFw/NI7fSYLfYTKQxklGe+vjmB0czti96TuUc0A9rSFhvXJUjjwQpiuzLbT9fmQ
jzh+WLl7lVSf7Tc21bePN4ZYQv9jF24SVeN8jsMrtUXgkYShucUmNDcpiBzCyWYjKH/HG1MMGhhEKpBo7xScrdqZ8k7/8jf1mXBqwe+CwHBjewCV55GUa
TBJBhorv5ftIqQCNvvDXDvWeEa/OJ2f/Ze8oNzi1KcRlKkFhIqzQAuUUCAQIJ3wnIwfBlpRXXqbj4mK2M0/CUoMUKpARe+VLJFmF7kPmp36gaY2oi2cFw
mtshPGX/JZGR9va5u2Rps329AoA1DMyvsh0SoOcZp54X8qYKg8EXlG+TLVlqcOc4fN4oSwMkV8JvT1s0nu7/bSNR6afRI12omVxYml3VljKoGNRCgMN2R
+LYi5ziOvFm9kO4IdF1vjQhAqxH8TvuqCX2zgqjNwd/1Nbwfx2wl/ufMd/BsjkbUOQKt0CZTt8y7vYGh3gCMCpDxIG1dirLED+liVFaZybzhZhQUHG3ot
iDNhDfjQJn/3B0CKG6YCdHJjUg",

   "symmetricEncKey":
"iPeXe2KXche23UZHURwFw+BdORL5xSPp66wXVJfAQRNcKR+nnwZ4dOsAKJX3dmSQ0lx6Cp6MpZBZo2UQH2eQJbt1SJmFK2pPFNXD+L7wYcBs/p4xg4xk
8l7HK7E1qkxoJEsKS9DunqYvl4IjW/GVS9G2+rHSEB2VrRlP4Q3k++Tb8Rp94nFjSv6wYIz4ghZdLllqnbw056rAG9mOF3i00box5kGZdX4xG+oLjT/GS
zi56mx2SvctNXmiB4N9+6BC7GxbkCc4lLYhRa9MDTPcoz1HkF1Cjcp+ldYGZsYf3KllfmmrVeIlBq8F9ABUzwZjot3GE12gX4EdZSnRryabfA==",

   "iv": "Ob06nKjivp+plDCY",

   "clientReferenceId" : "aaddvkkllllle123344",

   "statusCode": "PG99200",

   "errorMessage": **null**,

   "var1": **null**,

```
    "var2": null,
    "var3": null
}
```

Error Codes

Error Codes	Error Message	Http Status Code
PG99401	Attempted login from unauthorized IP	401 Unauthorized
PG99405	Request Method Not Allowed for API Access	405 Method Not Allowed
PG99429	DDOS Attack Detected from Requestor	429 Too Many Requests
PG99410	Cross Site Forgery Detected in API Request Message Payload	410 Gone
PG99400	Code Injection Detected in API Request Message Payload	400 Bad Request
PG99503	API Back-end Service Not Available or Timed-Out	503 Service Unavailable
PG99429	API Access Quota Exceeded	429 Too Many Requests
PG99500	Backend Service Provided Unexpected Response	500 Internal Server Error
PG99401	Invalid Client Certificate	401 Unauthorized
PG99401	Scope Validation Failed	401 Unauthorized
PG99401	Invalid API Key	401 Unauthorized
PG99401	Signature verification Failed	401 Unauthorized
PG99400	Decryption Failed	400 Bad Request
PG99400	Bad Request	400 Bad Request

3.2   ThreeDSRequestor Interface

3.2.1   A2.3DSS.FUN.ThreeDSRequestor.001 ThreeDSRequestor to 3DS Server Version Request API

ThreeDSRequestor does a version request to 3DS Server application, for checking whether the BIN is 2.0 enabled or not.

Below API Request needs to be initiated by ThreeDSRequestor, 3DS Server will share the version request URL , ThreeDSRequestor to make sure merchantTransID is appended as in the URL for every transaction.

pVrq URL Format:

URL Attribute	Example
HTTP Verb	POST
URL Format	<a href="https://<server-name>/3dsserverapi/v5/pVrq/<acquirerID>/<merchantID>" class="bare">https://<server-name>/3dsserverapi/v5/pVrq/ <acquirerID>/<merchantID&gt;
URL Attribute	**Example**

Sample URL	https://3ds2-api-3dsserverdemo.pc.enstage-sas.com/3dsserverapi/v5/pVrq/6111/ 54c8fefe-e694-3569-7864-d4329ce60971

pVrq JSON Request body:

```
{
    "messageType":"pVrq",
    "deviceChannel": "02",
    "p_messageVersion": "2.1.0",
    "merchantTransID": "54c8fefe-e694-3569-7864-d4329ce60971",
    "acctNumber": "xxxxxx",
    "acquirerBIN": "000000999",
    "acquirerID" :"8126", "threeDSRequestorMethodNotificationRespURL":
"https://merchantsecure.com/fetchNotificationRequest/<acquirerID>"
}
```

3.2.2 A2.3DSS.FUN.ThreeDSRequestor.002 3DS Server Responsefor ThreeDSRequestor Version Request (pVrq) API

3DS Server responds with ACS supported versions, and unique Transaction ID for that transaction.

pVrs: 3DS Server to ThreeDSRequestor version fetch Response:

```
{
      "messageType": "pVrs",
      "deviceChannel": "02",
      "p_messageVersion": "2.1.0",
      "acsStartVersion": "2.1.0",
      "acsEndVersion": "2.1.0",
      "dsStartVersion": "2.1.0",
      "dsEndVersion": "2.1.0",

      "acsInfoInd":["01", "02", "03", "04"],
      "scheme":"Visa",

      "directoryServerID":"scheme directory server id", "merchantTransID":
      "54c8fefe-e694-3569-7864-d4329ce60971",  "threeDSServerTransID":
      "5e56dd9b-9eae-4977-a2ea-230a1bb205ca",
      "threeDSServerPaRqURL": "https://3ds2-api-3dsserverdemo.pc.enstage-sas.com/3dsser
verapi/v4/pArq/indblr-blrrel/6111",

      "threeDSACSMethodURL":  "https://3ds2-ui-acsdev.com/v1/acs/services/threeDSMethod
/9111?cardType=V",
      "threeDSJSBrowserDetailFetchURL": "https://3ds2-api-3dsserverdev.com/static/clien t.min.js",
      "threeDSMethodDataFormPost": {
          "threeDSMethodData":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjNhYzdjYWE3LWFhNDItMjY2
My03OTFiLTJhYzA1YTU0MmM0YSIsInRocmVlRFNNZXRob2ROb3RpZmljYXRpb25VUkwiOiJ0aHJlZURTTWV0
aG 9kTm90aWZpY2F0aW9uVVJMIn0"
      },
      "errorCode":"000",
      "errorDesc":""

}
```

3.2.3   A2.3DSS.FUN.ThreeDSRequestor.003 ThreeDSRequestor to 3DS Server Request API

ThreeDSRequestor initiating pArq request which includes transaction details and threeDSServerTransID.

ThreeDSRequestor to make sure acquirer ID shared by 3DS Server during on boarding and merchantTransID received in pVrs response is appended in the URL for every transaction.

PArq needs to be posted to the URL from field "threeDSServerPaRqURL" of "pVrs" response.

PArq URL Format:

URL Attribute	Example
HTTP Verb	POST
URL Format 2.0	https://<server-name>/3dsserverapi/v5/pArq/indblr-blrrel/<acquirerID>/<merchantID>;

Sample URL 2.0	https://3ds2-api-3dsserverdemo.pc.enstage-sas.com/3dsserverapi/v5/pArq/ indblr-blrrel/6111/54c8fefe-e694-3569-7864-d4329ce60971

pArq v4: ThreeDSRequestor to 3DS Server transaction initiation request 2.0

```
{
        "messageVersion": "2.1.0",
        "threeDSRequestorURL": "http://test-wibmo-requestor.com/uat/test",
        "threeDSServerRefNumber": "3DS_LOA_SER_WIBM_020100_0064",
        "threeDSServerTransID": "62656197-5b8a-4226-a6ac-97f8b444e43e",
        "acquirerBIN": "000000999",
        "acquirerMerchantID": "",
        "addrMatch": "Y",
        "cardExpiryDate": "2212",
        "acctNumber": "",
        "deviceChannel": "02",
        "mcc": "7922",
        "merchantCountryCode": "840",
        "merchantName": "MyPoolin",
        "messageCategory": "01",
        "messageType": "pArq",
        "purchaseAmount": "10000",
        "purchaseCurrency": "356",
        "purchaseExponent": "2",
        "purchaseDate": "20200227160014",
        "browserJavascriptEnabled": false,

        "strictRegionalAuthenticationRules": false,
        "browserAcceptHeader": "*/*",
        "browserIP": "127.0.0.1",
        "browserJavaEnabled": false,
        "browserLanguage": "en_US",
        "browserColorDepth": "24",
        "browserScreenHeight": "768",
        "browserScreenWidth": "1366",
        "browserTZ": "-330",
        "browserUserAgent": "mozilla/5.0+(x11;+ubuntu;+linux+x86_64;+rv:72.0)+gecko/20100101+firefox/72.0",
        "threeDSRequestorAuthenticationInd": "01",
        "threeDSServerOperatorID": "10061597",
        "threeDSRequestorFinalAuthRespURL": "http://192.168.108.54:2000/getCRes/6111",
        "threeDSCompInd": "N",
        "merchantUrl": "https://3ds2-cust-api-acsdemo.pc.enstage-sas.com/Merchant-Simulator-demo/pgResponse.html",
        "merchantTransID": "54c8fefe-e694-3569-7864-d4329ce60971",
        "messageExtension": [{
                        "name": "name",
                        "id": "id",
                        "criticalityIndicator": false,
                        "data": {
                                "valueOne": "value1",
                                "valueTwo": "value2"
                        }
```

```json
        },
        {
                "name": "Travel Industry",
                "id": "A000000802-002",
                "criticalityIndicator": false,
                "data": {
                        "agencyIndicator": "Y",
                        "air": {
                                "airlineTicketInfo": {
                                        "currencyMismatchIndicator": "Y",
                                        "ticketAmount": "75000",
                                        "ticketCount": "03",
                                        "ticketCurrency": "123"
                                },
                                "itineraryInfo": {
                                        "flightIndicator": "01",
                                        "segments": [{
                                                        "departureAirport": "NCE",
                                                        "departureDate": "20200415",
                                                        "departureTime": "0930",

                                                        "arrivalAirport": "CDG",
                                                        "arrivalDate": "20200415",
                                                        "arrivalTime": "1030",
                                                        "operatingCarrier": "7S"
                                                },
                                                {

                                                        "departureAirport": "CDG",
                                                        "departureDate": "20200415",
                                                        "departureTime": "1130",
                                                        "arrivalAirport": "LHR",
                                                        "arrivalDate": "20200415",


                                                        "arrivalTime": "1150",
                                                        "operatingCarrier": "7S"
                                                }
                                        ]
                                }
                        },
                        "car": {
                                "companyInfo": {
                                        "name": "ABC Car Hire",
                                        "email": "email@emailaddress.com",
                                        "phone": {
                                                "cc": "44",
                                                "subscriber": "2087654321"
                                        }
                                },
                                "reservationInfo": {
                                        "currencyMismatchIndicator": "Y",
                                        "amount": "10000",
                                        "currency": "123",
```

```json
                            "pickUpDate": "20200415",
                            "pickUpTime": "1300",
                            "pickUpLocation": {
                                    "addrLine1": "123 Airport Road",
                                    "addrCity": "Longford",
                                    "addrPostCode": "TW61AP",
                                    "addrCountry": "826"
                            },
                            "returnDate": "20200416",
                            "returnTime": "1230",
                            "returnLocation": {
                                    "addrLine1": "123 Airport Road",
                                    "addrCity": "Longford",
                                    "addrPostCode": "TW61AP",
                                    "addrCountry": "826"
                            },
                            "cars": [{
                                    "carRentalType": "01",
                                    "carRentalInsuranceType": "01"
                            }]
                    }
            },


            "hotel": {
                    "propertyInfo": {
                            "name": "EMV London Hotel",
                            "chainCode": "CHAIN123",
                            "propertyCode": "EMVLH",
                            "referenceCode": "REF123",
                            "addrLine1": "3 Domain Street",
                            "addrLine2": "Suite 100",
                            "addrCity": "London",
                            "addrPostCode": "SE10UG",
                            "addrCountry": "826",
                            "email": "email@emailaddress.com",
                            "phone": {
                                    "cc": "44",
                                    "subscriber": "2012345678"
                            }
                    },
                    "reservationInfo": {
                            "currencyMismatchIndicator": "Y",
                            "amount": "30000",
                            "currency": "123",
                            "checkInDate": "20200415",
                            "checkInTime": "1500",
                            "checkOutDate": "20200416",
                            "checkOutTime": "1100",
                            "rooms": [{
                                    "bedType": "01",
```

```
                                    "roomOccupancy": "2",
                                    "roomType": "05"
                            }]
                    }
            },
            "travellers": [{
                            "airlineLoyaltyStatus": "03",
                            "airlinePassengerIndicator": "Y",
                            "carRentalDriverIndicator": "Y",
                            "carRentalLoyaltyStatus": "02",
                            "hotelGuestIndicator": "Y",
                            "hotelLoyaltyStatus": "03",
                            "name": "John Smith",
                            "type": "ADT"
                    },
                    {

                            "airlineLoyaltyStatus": "02",
                            "airlinePassengerIndicator": "Y",
                            "carRentalDriverIndicator": "N",
                            "carRentalLoyaltyStatus": "01",
                            "hotelGuestIndicator": "Y",
                            "hotelLoyaltyStatus": "01",
                            "name": "Jane Smith",
                            "type": "ADT"
                    }


            ],
            "version": "2.0"
        }
    }
  ]
}
```

3.2.4   A2.3DSS.FUN.ThreeDSRequestor.004 3DS Server Response to ThreeDSRequestor

API Response will be sent by 3DS Server to ThreeDSRequestor.

pArs: 3DS Server to ThreeDSRequestor transaction initiation response for 2.0

```
{
    "messageVersion": "2.1.0",
    "p_messageVersion": "2.1.0",
    "messageType": "pArs",
    "threeDSServerTransID": "5e56dd9b-9eae-4977-a2ea-230a1bb205ca",
    "acsTransID": "93f0d055-2610-48f2-8eee-324af4ec2da5", "dsTransID":
    "828ba429-cf6b-405c-bda3-4d7d5e0b9367", "merchantTransID": "54c8fefe-
    e694-3569-7864-d4329ce60971", "eci": "05",
    "authenticationValue": "AABBCCDDEEFFAABBCCDDEEFFAAA=",
    "transStatus": "Y",

    "acsChallengeMandated": "Y",
    "acsDecConInd":"N",
    "whiteListStatus":"Y",
    "whiteListStatusSource":"03",
```

```
    "messageExtension": [
      {
        "name": "name",
        "id": "id", "criticalityIndicator": false,
        "data": {
          "valueOne":"value1",
          "valueTwo":"value2"
        }
      }
      ],

      "authenticationUrl": "https://3ds2-api-3dsserverdemo.pc.enstage-
sas.com/3dsserverapi/v5/pRqFrq/indblr-blrrel/6111/54c8fefe-e694-3569-7864-
d4329ce60971",
      "merchantCancelChallengeAuthUrl": "https://3ds2-api-3dsserverdemo.pc.enstage-
sas.com/3dsserverapi/v5/pRqCn/indblr-blrrel/6111/54c8fefe-e694-3569-7864-d4329ce60971 ",

      "acsChallengeReqUrl": "ACS challenge Request URL ",

      "acsChallengeReqFormData":{
          "creq":""
      },

      "sdkTransID": "5f27d9d4-95c1-4b74-ab41-906859312847",
      "sdkAppID": "34c8fefe-f694-4569-9869-c4029ce60971",
      "acsSignedContent":
"eyJ4NWMiOlsiTUlJRmpqQ0NBM2FnQXdJQkFnSUdBV0dacEZEN01BMEdDU3FHU0liM0RRRUJDd1VBTUh3
eEN6Q
UpCZ05WQkFZVEFrNU1NU2t3SndZRFZRUUtEQ0JWVENCVWNtRnVjMkZ2ZEdJRldV04xY21sMGVTTFQ
mthWFp
wYzJsdmJqQRWdNQjRHQTFVUN3d1hWVXdnVkZNN00wUXRVMlZqZFhKbBlGSlBUMFFnUTBFeElEQWVCZ05
WQkFNT
UYxVk1JJRlJJUSURRORURUxWTmxZM1Z5WlNCQwOVVJRU5CVUI0WERURRNNREl4TlRFME1qVXpPRm9YRFRF
NU1ESXh
OVEUwTWpVek9Gb3dnWUF4Q3pBSkJSkJnTlZCQVlUQWs1TU1Ta3dKd1lEVlFVRllK-
8l6cHRRnTjNmiFyODDOzi4EslBikT0-jOIN8mpZ9h7YjNgBHIj7zHqdGLqZ4XL4c3iSbQBk6Y-
TcW6GwAQ_ZYCWRmyTqsZxtskpSynjWBHfTlLINkQc-JA-FVL3U86NfIRGBft80L5Nk5nJQ-
HIfEJktbmXdmURUcrPC7UyI1-NT_-vVmMoTpyKcQy3arLgXk2XzjwWMTGgFvoASb-gO6L-q4i-
JvQFyEf50hYU9DdTRgsrMwnB1RilSuOWH85M8t2svb5V4hpWnaLejSvGSzWB6ik7iKQmTxbJsJm0mTmbfSP
s5m IWeNhevdpGDp8FPyQAaYAceCIwxbCrBtEZQ",
      "acsRenderingType": { "acsInterface":
          "01",
          "acsUiTemplate": "02"
      },
      "errorCode":"000",
      "errorDesc":""

}
```

3.2.5 A2.3DSS.FUN.ThreeDSRequestor.005 ThreeDSRequestorFinal Authentication Status Request to 3DS Server

For Challenge Browser flow ThreeDSRequestor will initiate below request to fetch Authentication value, eci and Transaction status of the transaction with 3DS Server.

pRqFrq URL format:

URL Attribute	Example
HTTP Verb	POST
URL Format 2.0	<a href="https://<Host>/3dsserverapi/v5/pRqFrq/indblr-blrrel/<acquirerID>/<merchantID&gt" class="bare">https://<Host>/3dsserverapi/v5/pRqFrq/indblr-blrrel/<acquirerID>/<merchantID&gt;
sample URL 2.0	https://3ds2-api-3dsservercrt.enstage-uat.com/3dsserverapi/v5/pRqFrq/ indblr-blrrel/8126/54c8fefe-e694-3569-7864-d4329ce60971

pRqFrq 2.0 : ThreeDSRequestor to 3DS Server request for fetching CAVV and eci

```
{
      "messageType": "pRqFrq",
      "messageVersion": "2.1.0",
      "p_messageVersion": "2.1.0",
      "threeDSServerTransID": "b6fcf6b8-cca6-4df6-8e6f-95e1776934e7",
      "acsTransID": "6c4cb56a-b92f-11eb-8bed-f9aee3c6fdfa", "dsTransID":
      "4b7b0d46-5556-4cb5-a1f6-4d185f08f741", "sdkTransID": "5f942d8f-ad1a-
      4a93-afa8-460e3fc07092", "merchantTransID": "54c8fefe-e694-3569-7864-
      d4329ce60971", "signatureHashIdentifier": "02",
      "acquirerID": "8126",
      "acsAuthResponse":
"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjIwZWMwNDI0LWE0MDEtNDBjNS1hN2M2LTc1MzcxMjdiNGJjNiI
sI
mFjc1RyYW5zSUQiOiIxM2Q0ZmUwMy1iMmU2LTExZWItOGJlZC01OTM0NjdhYmVhMmEiLCJtZXNzYWdlV
HlwZSI
6IkNSXMiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiYWNzVWlUeXBlIjoiMDEiLCJjaGFsbGVuZ2VDb21wb
GV0aW9uSW5kIjoiWSIsImlzc3VlckltYWdlIjp7ImhpZ2giOiJodHRwczovL2FjY29yYS1pdnMuczMuYXAtc29
1dGgtMS5hbWF6b25hd3MuY29tL2FjY29yYS1pdnMvdjEvcGFydGljaXBhbnQvaHNiY2IvaW1hZ2VzL2hzYmNi
X
2xvZ28uanBnIiwiZXh0cmFIaWdoIjoiaHR0cHM6Ly9hY2Nvc2EtaXZzLnMzLmFwLXNvdXRoLTEuYW1hem9uY
Xd  zLmNvbS9hY2Nvc2EtaXZzL3YxL3BhcnRpY2lwYW50L2hzYmNiL2ltYWdlcy9oc2JjYl9sb2dvLmpwZyIsIm1lZ
Gl1bSI6Imh0dHBzOi8vYWNjb3NhLWl2cy5zMy5hcC1zb3V0aC0xLmFtYXpvbmF3cy5jb20vYWNjb3NhLWl2cy
9
2MS9wYXRpY2lwYW50C9oc2JjYi9pbWFnZXMvaHNiY2JfbG9nby5qcGcifSwicHNbWFnZSI6eyJoaWdoIjoia
HR0cHM6Ly9hY2Nvc2EtaXZzLnMzLmFwLXNvdXRoLTEuYW1hem9uYXdzLmNvbS9hY2Nvc2EtaXZzL3YxL2Vt
di9
2aXNhL2ltYWdlcy92aXNhX3xvZ28uanBnIiwiZXh0cmFIaWdoIjoiaHR0cHM6Ly9hY2Nvc2EtaXZzLnMzLmFwL
XNvdXRoLTEuYW1hem9uYXdzLmNvbS9hY2Nvc2EtaXZzL3YxL2Vtdi92aXNhL2ltYWdlcy92aXNhX3xvZ28uan
B
nIiwibWVkaXVtIjoiaHR0cHM6Ly9hY2Nvc2EtaXZzLnMzLmFwLXNvdXRoLTEuYW1hem9uYXdzLmNvbS9hY2N
vc      2EtaXZzL3YxL2Vtdi92aXNhL2ltYWdlcy92aXNhX3xvZ28uanBnIn0sInRyYW5zU3RhdHVzIjoiTiIsImFjc0N
vdW50ZXJBdG9TIjoiMDAwIiwicmVzZW5kRmxhZyI6Ik4ifQ=="
}
```

3.2.6 A2.3DSS.FUN.ThreeDSRequestor.006 3DS Server Final Authentication Response to ThreeDSRequestor

API Response will be initiated by 3DS Server to ThreeDSRequestor which includes Authentication details CAVV, Transaction status and ECI.

pRsFr: 3DS Server final auth response to ThreeDSRequestor

```
{
    "messageVersion": "2.1.0",
    "p_messageVersion": "2.1.0",
    "messageType": "pRsFr",
    "threeDSServerTransID": "5e56dd9b-9eae-4977-a2ea-230a1bb205ca",
    "acsTransID": "93f0d055-2610-48f2-8eee-324af4ec2da5", "dsTransID":
    "828ba429-cf6b-405c-bda3-4d7d5e0b9367", "sdkTransID": "5f27d9d4-95c1-
    4b74-ab41-906859312847",
    "merchantTransID": "54c8fefe-e694-3569-7864-d4329ce60971", "eci":
    "05",
    "authenticationValue": "AABBCCDDEEFFAABBCCDDEEFFAAA=",
    "transStatus": "Y",
    "errorCode":"000",
    "errorDesc":""
}
```

6.1 JSON Request Field Details: pVrq

JSON Request Field Details:

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description
messageType	String	Variable, 5–8 characters	R	pVrq	Identifies the Message Type
deviceChannel	String	2 characters	R	01 = App-based (APP) 02 = Browser (BRW) 03 = 3DS Requestor Initiated (3RI)	
p_messageVersio n	String	Variable, 5–8 characters	R	2.1.0	Customer Protocol version
merchantTransI D	String	36 characters	R	UUID Format	Unique Transaction Identifier for merchant / PG
acctNumber	String	Variable, 13 -19 characters	R		Card number
acquirerBIN	String	6 character; Numeric	R		Acquirer BIN assigned by Scheme
acquirerID	String	4 character; Numeric	R		Acquirer Identifier assigned by 3DS Server / MPI
threeDSRequesto rMethod NotificationResp URL	String	Length:2048 characters	C	URL	Merchant URL that will receive the notification of 3DS Method completion from the ACS.

6.2   JSON Request Field Details: pVrs

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description
messageType	String	Variable, 5–8 characters	R	pVrs	Identifies the Message Type
deviceChannel	String	2 characters	R	01 = App-based (APP) 02 = Browser (BRW) 03 = 3DS Requestor Initiated (3RI)	
p_messageVersion	String	Variable, 5–8 characters	R	2.1.0	Customer Protocol version
acsStartVersion	String	Variable, 5–8 characters	R	2.1.0	Earliest Bin supported EMVCo Protocol Version at ACS
acsEndVersion	String	Variable, 5–8 characters	R	2.1.0	Latest Bin supported EMVCo Protocol Version at ACS.
dsStartVersion	String	Variable, 5–8 characters	O	2.1.0	Earliest Bin supported EMVCo Protocol Version at DS
dsEndVersion	String	Variable, 5–8 characters	O	2.1.0	Latest Bin supported EMVCo Protocol Version at DS
scheme	String	Variable, 5–8 characters	O	Visa, Master, Amex, Diner	Identifies the Card Scheme

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description
directoryServerID	String	Variable,250 characters	O	2.1.0	Directory Server ID of the Scheme of Public Key for device encryption by the SDK
acsInfoInd	Json String Array	2 characters	O	Will be available with DS 2.2 version accepted values are - [”01", “02”, “03”, “04”]	Provides the information of ACS - • 01 =Authentication Available at ACS • 02 = Attempts Supported by ACS or DS • 03 = Decoupled Authentication Supported • 04 = Whitelisting Supported • 05–79 = Reserved for EMVCo future use (Values invalid until defined by EMVCo) • 80–99 = Reserved for DS use
merchantTransID	String	Length: 36 characters	R	UUID Format	Unique Transaction Identifier for merchant / PG
threeDSServerTransID	String	Length: 36 characters	R	UUID format	3DS Server Unique Transaction ID
threeDSServerPaRqURL	String	Length:2048 characters	R	URL to post pArq URL	URL to post pArq request
threeDSACSMethodURL	String	Length:2048 characters	C	Required for 2.1.0 and above. URL to initiate ACS Method URL	URL to initiate ACS Method URL

Field Nam e	Data Type	Length	Message Inclusion	Field Value	Field Description
threeDSJSBrowserDetailFetchURL	String	Length:2048 characters	C	Required for 2.1.0 and above. URL to fetch Browser Details	URL to fetch Browser Details
threeDSMethodDataFormPost	Object		C	Required for 2.1.0 and above. 3DS Server ACS method URL form data	3DS Server ACS method URL form data
threeDSMethodDataFormPost.threeDSMethodData	String		C	Required for 2.1.0 and above. Base64 URL encoded value of threeDSMethod Data, which will be posted by Merchant to ACS to fetch Browser details by ACS.	Base64 URL encoded value of threeDSMethod Data to be posted to ACS.
errorCode	String	R	3 characters, numeric	000- Success 001-Message Signature Hash failed	000- Success 001-999 error codes will be sent basis the validation.
error Desc	String	O	Variable, maximum 2048 characters		Error Description

6.3 JSON Request Field Details: pArq

Fiel d Na me	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
messageType	String	Variable, 5–8 characters	R	pArq	Identifies the Message Type	R	R
deviceChannel	String	2 characters	C	01 = App-based (APP) 02 = Browser (BRW) 03 = 3DS Requestor Initiated (3RI)	Required for 2.1.0 and above		R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
p_messageVersion	String	Variable, 5–8 characters	R	2.1.0		R	R
merchantTransID	String	36 characters	R	UUID Format	Unique Transaction Identifier for merchant / PG	R	R
sdkAppID	String	36 characters	C		Universally unique ID created upon all installations and updates of the 3DS Requestor App on a Consumer Device. This will be newly generated and stored by the 3DS SDK for each installation or update.		R (only for SDK)
sdkEphemPubKey	JSON Data Type: Object JWK	Variable, maximum 256 characters	C	Required for an SDK App Transaction for 2.1.0 and above	Public key component of the ephemeral key pair generated by the 3DS SDK and used to establish session keys between the 3DS SDK and ACS. In AReq, this data element is present as its own object. In ARes, this data element is contained within the ACS Signed Content JWS Object.		R (only for SDK)
sdkEphemPubKey.kty	String		C	Required for an SDK App Transacti on for 2.1.0 and above			R (only for SDK)

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
sdkEph emPubKey.crv	String		C	Required for an SDK App Transaction for 2.1.0 and above			R (only for SDK)
sdkEphemPubKey.x	String		C	Required for an SDK App Transaction for 2.1.0 and above			R (only for SDK)
sdkEphemPubKey.y	String		C	Required for an SDK App Transaction for 2.1.0 and above			R (only for SDK)
sdkTransID	String	36 characters	C	Required for an SDK App Transaction for 2.1.0 and above	Unique SDK Transaction ID		R (only for SDK)
sdkReferenceNumber	String	Variable maximum 32 characters	C	Required for an SDK App Transaction for 2.1.0 and above	Identifies the vendor and version for the 3DS SDK that is integrated in a 3DS Requestor App, assigned by EMVCo when the 3DS SDK is approved.		R (only for SDK)

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
sdkMaxTimeout	String		C	Required for an SDK App Transaction for 2.1.0 and above	Indicates maximum amount of time (in minutes) for all exchanges.		R (only for SDK)
sdkEncData	String		C	SDK Encrypted Data. Required for an SDK App Transaction for 2.1.0 and above	Required 3DS Server to DS but will not be present DS to ACS.		R (only for SDK)
messageVersion	String	Variable, 5–8 characters	R	2.1.0	EMVCo Protocol Version Number of the specification	R	R
messageCategory	String	2 characters, numeric	R	01 = PA (Payment Authentication) 02=NPA (Non-Payment Authentication)	Merchant must pass the necessary data 01 = PA (Payment Authentication) 02=NPA (Non-Payment Authentication)	R	R
threeDSServerTransID	String	Length: 36 characters	R	UUID format	3DS Server Unique Transaction ID, required in-case 3DS Requestor has initiated Version request	R	R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorID	String		C	Required for 2.1.0 and above	DS assigned 3DS Requestor identifier. Each DS will provide a unique ID to each 3DS Requestor on an individual basis.		R
threeDSRequestorName	String		C	Required for 2.1.0 and above	DS assigned 3DS Requestor name. Each DS will provide a unique name to each 3DS Requestor on an individual basis.		R
thre eDSRequestorURL	String		R		Fully qualified URL of 3DS Requestor website or customer care site. This data element provides additional information to the receiving 3-D Secure system if a problem arises and should provide contact information.	R(merchantUrl)	R
acctNumber	String	Variable, 13 -19 characters	R		Card Number	R	R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorAuthenticationInd	String	2 characters, numeric	C	Required for 2.1.0 and above. • 01 = Payment transaction • 02 = Recurring transaction • 03 = Instalment transaction • 04 = Add card • 05 = Maintain card • 06 = Cardholder verification as part of EMV token ID&V • 07–79 = Reserved	Indicates the type of Authentication request		R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSCompInd	String	1 character	C	Required for 2.1.0 and above. Values accepted: • Y = Successfully complete d • N = Did not successfully complete • U = Unavailable —3DS Method URL was not present in the PRes message data for the card range associate d with the Cardholder Account Number.	Indicates whether ThreeDS Requestor has completed the Method URL call.		R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorAuthenticationInfo	JSON Data Type: Object		O	Information about how the 3DS Requestor authenticated the cardholder before or during the transaction			R
thre eDS Req uest orA uthe ntic atio n Info .thr eeD SRe qAu thM etho d	String	2 characters, numeric	O	Mechanis m used by the Cardhold er to authentic ate to the 3DS Requesto r	Values accepted: • 01 = No 3DS Requestor authentication occurred (i.e. cardholder "logged in" as guest) • 02 = Login to the cardholder account at the 3DS Requestor system using 3DS Requestor's own credentials • 03 = Login to the cardholder account at the 3DS Requestor system using federated ID • 04 = Login to the cardholder account at the 3DS Requestor system using issuer credentials • 05 = Login to the cardholder account at the 3DS Requestor system using third-party authentication • 06 = Login to the cardholder account at the 3DS Requestor system using FIDO Authenticator • 07 = Login to the cardholder account at the 3DS Requestor system using FIDO Authenticator (FIDO assurance data signed) • 08 = SRC Assurance Data • 09–79 = Reserved for		O

					EMVCo future use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use		

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorDecReqInd	String	1 character	O	Indicates whether the 3DS Requestor requests the ACS to utilize Decouple d Authentication and agrees to utilize Decouple d Authentication if the ACS confirms its use	Values accepted: • Y = Decoupled Authentication is supported and preferred if challenge is necessary • N = Do not use Decoupled Authentication		O

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorDecMaxTime	String	5 characters	O	Indicates the maximum amount of time that the 3DS. Requestor will wait for an ACS to provide the results of a Decouple d Authentication transaction (in minutes).	Numeric values between 1 and 10080 accepted.	R	R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
thre eDS Req uest orA uthe ntic atio n Info .thr eeD SRe qAu thTi mes tam p	String	12 characters	O	Date format = YYYYMM DDHHM M	Date forma t = YYYY MMD DHH MM		O
threeDSReq uestorAuthe nticationInfo .threeDSRe qAuthData	String	maximum 2048 bytes	O	Data that document s and supports a specific authentication process.			O

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
threeDSRequestorChallengeInd	String	2 characters	O	Indicates whether a challenge is requested for this transaction.	Values accepted: • 01 = No preference • 02 = No challenge requested • 03 = Challenge requested (3DS Requestor preference) • 04 = Challenge requested (Mandate) • 05 = No challenge requested (transactional risk analysis is already performed) • 06 = No challenge requested (Data share only) • 07 = No challenge requested (strong consumer authentication is already performed) • 08 = No challenge requested (utilize whitelist exemption if no challenge required) • 09 = Challenge requested (whitelist prompt requested if challenge required) • 10–79 = Reserved for EMVCo future use (values invalid until		O

					defined by EMVCo) • 80–99 =Reserved for DS use		
acctType	String	2 characters	C	Indicates the type of account. Values accepted: • 01 = Not Applicable • 02 = Credit • 03 = Debit	Required if 3DS Requestor is asking Cardholder which Account Type they are using before making the purchase. Required in some markets (for example, for Merchants in Brazil). Otherwise, it is optional.		C
add rMatch	String		R				R
acct Info	String		O				O

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
acctInfo.chAccAgeInd	String		O				O
acctInfo.chAccDate	String		O				O
acct Info.chAccChangeInd	String		O				O
acctInfo.chAccPwChange	String		O				O
acctInfo.shipAddressUsageInd	String		O				O

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
acctInfo.shipAddressUsage	String		O				O
acctInfo.txnActivityDay	String		O				O
acctInfo.txnActivityYear	String		O				O
acctInfo.provisionAttemptsDay	String		O				O
acctInfo.nbPurchaseAccount	String		O				O
acctInfo.sus piciousAccActivity	String		O				O
acctInfo.shipNameIndicator	String		O				O
acctInfo.paymentAccInd	String		O				O
acctInfo.paymentAccAge	String		O				O
acctID	String		O		Additional information about the account optionally provided by the 3DS Requestor.		O
merchantRiskIndicator	String		O	Merchant 's assessment of the level of fraud risk for the specific authentication for both the cardholder and the authentication being conducted.			O
merchantRiskIndicator.shipIndicator	String		O				O
merchantRiskIndicato r.deliveryTi meframe	String		O				O
merchantRiskIndicator.deliveryEmailAddress	String		O				O
merchantRiskIndicator.reorderItemsInd	String		O				O
merchantRiskIndicator.preOrderPurchaseInd	String		O				O
merchantRiskIndicator.preOrderDate	String		O				O
merchantRiskIndicator.giftCardAmount	String		O				O
merchantRi skIndicator.giftCardCu rr	String		O				O
mer chantRiskIndicator.giftCardCount	String		O				O
billAddrPostCode	String		O				O
billAddrCountry	String		O				O
cardExpiryDate	String		R	YYMM format	Expiry Date of the PAN or token supplied to the 3DS Requestor by the Cardholder.	R	R

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
purchaseCurrency	String	3 characters; Numeric	R	Currency in which purchase amount is expressed.	ISO 4217 three-digit currency code	R	R
shipAddrCity	String		O				O
shipAddrLin e1	String		O				O
mcc	String	4 characters	R	Merchant 's type of business, product or service.	Optional but strongly recommended to include for 02- NPA if the merchant is also the 3DS Requestor. For PA it is required field, for NPA it is optional		R
acquirerMerchantID	String	Variable, maximum 35 characters	R	Acquirer-assigned Merchant identifier	Acquirer-assigned Merchant identifier.	R	R
purchaseExponent	String	1 character	R	Minor units of currency as specified in the ISO 4217 currency exponent.	For Payment Transaction its Mandatory, For NPA, Required for 02- NPA if 3DS Requestor Authentication Indicator = 02 or 03.		R
billAddrState	String		O				O
merchantName	String	Variable, maximum 40 characters	R		Merchant name assigned by the Acquirer or Payment System. Required for payment transaction. Optional for non-payment but strongly recommended to include for 02- NPA if the merchant is also the 3DS Requestor.	R	R
shipAddrPostCod e	String		O				O

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
purchasAmount	String		R	Purchase amount in minor units of currency with all punctuation removed.	Required for Payment. For non-payment, Required for 02- NPA if 3DS Requestor Authentication Indicator = 02 or 03.	R	R
cardholderName	String		C	Name of the Cardholder.	Required unless market or regional mandate restricts sending this information.		C
bill AddrLine3	String		C		Required unless market or regional mandate restricts sending this information.		C
threeDSServerOperatorID	String		O				O
purchaseDate	String	14 characters	R	YYYYMM DDHHM MSS	Date and time of the purchase, expressed in UTC.	R	R
recurringExpiry	String	8 characters	C	Format accepted: YYYYMM DD	Required for Installment and Recurring Transactions.	R	C R
recurringFrequency	String	Variable, maximum 4 character	C	Indicates the minimum number of days between authoriza tions	Required for Installment and Recurring Transactions.	R	C
mobilePhone	Json Object		C		Required (if available) unless market or regional mandate restricts sending this information.		C
mobilePhone.cc	String		C				C

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
billAddrCity	String		O				O
workPhone	String		O				O
workPhone.cc	String		O				O
workPhone.subscriber	String		O				O
billAddrLine1	String		O				O
billAddrLine2	String		O				O
shipAddrCountry	String		O				O
email	String		O				O
shipAddrLine2	String		O				O
merchantCountryCode	String	3 characters	R		Country Code of the Merchant.	R	R
homePhone	Json Object		O				O
homePhone.cc	String		O				O
homePhone.subscriber	String		O				O
acquirerBIN	String	maximum 11 characters	R	Acquiring institution identification code as assigned by the DS	Acquiring institution identification code as assigned by the DS	R	R
shipAddrLine3	String		O				O
tran sTy pe	String		C	Values accepted: • 01 = Goods/ Service Purchase • 03 = Check Acceptan ce • 10 = Account Funding • 11 =	Identifies the type of transaction being authenticated. This field is required in some markets (e.g. for Merchants in Brazil). Otherwise,		C

Field	Type	Length/Format		Description	Description		
					Quasi- Cash Transacti on • 28 = Prepaid Activatio n and Load	optional.		
ship AddrSta te	String		C				C
acq uire rID	String	4 character; Numeric	R		Acquirer Identifier assigned by 3DS Server / MPI	R	R
thre eDS Req uest orPr ior Authen ticat ionI nfo	Object		O	3DS Requesto r Prior Transacti on Authentic ation Informati on	3DS Requestor Prior Transaction Authentication Information.		O
thre eDS Req uest orPr ior Authen ticat ionI nfo. thre eDS Req Prio rRef	String	Maximum 2048 Character	O	3DS Requesto r Prior Transacti on Authentic ation Data	3DS Requestor Prior Transaction Authentication Information.		O
thre eDS Req uest orPr ior Authen ticat ionI nfo. thre eDS Req Prio rAut hMe tho d	String	2 characters	O	Values accepted: • 01 = Frictionle ss authentic ation occurred by ACS • 02 = Cardhold er challenge occurred by ACS • 03 = AVS verified • 04 = Other issuer methods	3DS Requestor Prior Transaction Authentication Information.		O
thre eDS Req uest orPr ior Authen ticat ionI nfo. thre eDS Req Prio rAut hTi mes tam p	String	12 characters	O	Date format = YYYYMM DDHHM M	3DS Requestor Prior Transaction Authentication Timestamp		O

thre eDS Req uest orPr iorA uthe ntic atio n Info .thr eeD SRe qPri orA uth Dat a	String	maximum 2048 bytes	O		Data that document s and supports a specific authentic ation process	Data that documents and supports a specific authentication process		O
thre eRII nd	String	2 characters	O		Values accepted: • 01 = Recurring transactio n • 02 = Instalme nt transactio n • 03 = Add card • 04 = Maintain card informati on • 05 = Account verificati on	Indicates the type of 3RI request		O
thre eDS Req uest or Fina lAut hRe spU RL	String	Variable, maximum 2048 characters	C		Values accepted: Fully qualified Merchant URL of the system that receives the CRes / PaRes message from ACS	Required if transactionStatus ="C"		
stric tReg iona l Aut hen ticat ion Rule s	Boolean	2 characters	O		Identifier to know whether strict Authentic ation rules are enabled in the region	Values accepted: true or false		O
whi teLi stSt atus	String	1 characters	O		Enables the communi cation of trusted beneficia ry/whiteli st status between the ACS, the DS and the 3DS Requesto r.	Values accepted: • Y = 3DS Requestor is white listed by cardholder • N = 3DS Requestor is not white listed by cardholder • E = Not eligible as determined by		O

					issuer • P = Pending confirmation by cardholder • R = Cardholder rejected • U = Whitelist status unknown, unavailable, or does not apply			
mer cha ntD SPas swo rd	String	20 characters	O		Merchant 1.0 Directory Server Registered password	Merchant 1.0 Directory Server Registered password		O
whi teLi stSt atus Sou rce	String	2 characters	O		This data element will be populate d by the system setting Whitelist Status.	Values accepted: • 01 = 3DS Server • 02 = DS • 03 = ACS • 04-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80-99 = Reserved for DS use.		O
mes sage Exte nsio n	JSON Data Type: Array	Variable, maximum 81920 bytes	C		// Sample Message Extension Tag "message Extension ": [{ "name": "extensio nField1" "id": "ID1", "criticalit yIndicato r": true, "data":{ "valueOn e":"value" }, {Travel industry fields. Please refer the section 4.3.0}]	Data necessary to support requirements not otherwise defined in the 3-D Secure message are carried in a Message Extension.		C
bro wse rAcc ept Hea der	String	Variable, maximum 2048 characters	C			Exact content of the HTTP accept headers as sent to the 3DS Requestor from		R (only for Browser based)

					the Cardholder's browser.		
browserIP	String	Variable, maximum 45 characters	C		• IPv4 address is represent ed in the dotted decimal format of 4 sets of decimal numbers separated by dots. The decimal number in each and every set is in the range 0 to 255. Example IPv4 address: 1.12.123.2 55 IPv6 address is represent ed as eight groups of four hexadecimal digits, each group representing 16 bits (two octets. The groups	IP address of the browser as returned by the HTTP headers to the 3DS Requestor.		R (only for Brows er based)

Field Name	Data Type	Length	Mes age Inclusion	Field Value	Field Description	1.0	2.0
browserJavaEnabled	JSON Data Type: Boolean	true/false	C	• true • false	Boolean that represents the ability of the cardholder browser to execute Java. Value is returned from the navigator.javaEnabled property.		R (only for Browser based)
browserLanguage	String	1-8 characters	C		Value representing the browser language as defined in IETF BCP47. Returned from navigator.language property.		R (only for Browser based)
browserColorDepth	String	1-2 characters	C	• 1 = 1 bit • 4 = 4 bits • 8 = 8 bits • 15 = 15 bits • 16 = 16 bits • 24 = 24 bits • 32 = 32 bits • 48 = 48 bits	Value representing the bit depth of the color palette for displaying images, in bits per pixel. Obtained from Cardholder browser using the screen.colorDepth property.		R (only for Browser based)
browserScreenHeight	String	1-6 characters	C		Total height of the Cardholder's screen in pixels. Value is returned from the screen.height property.		R (only for Browser based)

Field Name	Data Type	Length	Message Inclusion	Field Value	Field Description	1.0	2.0
browserScreenWidth	String	1-6 characters	C		Total width of the cardholder's screen in pixels. Value is returned from the screen.width property.		R (only for Browser based)
browserTZ	String	1-5 characters	C	Value is returned from the getTimez oneOffset () method.	Time difference between UTC time and the Cardholder browser local time, in minutes.		R (only for Browser based)
browserUserA gent	String	maximum 2048 characters	C		Exact content of the HTTP user- agent header.		R (only for Browser based)
challengeWindowSize	String	2 characters	O	Value accepted: • 01 = 250 x 400 • 02 = 390 x 400 • 03 = 500 x 600 • 04 = 600 x 400 • 05 = Full screen	challengeWindowSize		O
additionalInfo	String		O		BrowseradditionalInfo		O
merchantClassificationA	String	maximum 2048 characters	O	Merchant Classification details like Platform			O
merchantClassificationB	String	maximum 2048 characters	O	Merchant Classification details like Platform			O
merchantClassificationC	String	maximum 2048 characters	O	Merchant Classification details like Platform			O

6.4   JSON Request Field Details:pArs

Field Nam e	Data Type	Message Inclusion	Length	Field Value	Field Description
messageType	String	R	Variable, 5–8 characters	pArs	Identifies the Message Type
p_message Version	String	R	Variable, 5–8 characters	2.1.0	Message Protocol Version Number of the specification
messageVersion	String	R	Variable, 5–8 characters	2.1.0	EMVCo Protocol Version Number of the specification
three DSSe rverT ransI D	String	R	Length: 36 characters	UUID format	3DS Server Unique Transaction ID
acsTr ansI D	String	R	Length: 36 characters	UUID format	ACS Server Unique Transaction ID
dsTr ansI D	String	R	Length: 36 characters	UUID format	DS Server Unique Transaction ID
merc hant Tran sID	String	R	Length: 36 characters	UUID format	Merchant Server Unique Transaction ID
error Code	String	R	3 characters, numeric	000- Success 001- Message Signature Hash failed	000- Success 001-999 error codes will be sent basis the validation
error Desc	String	O	Variable, maximum 2048 characters		Error Description
eci	String	C	Length: 2 characters		As per EMVCo / DS specs

Field Name	Data Type	Message Inclusion	Length	Field Value	Field Description
authentication Value	String	C	Length: 28 characters	Authentication Value needs to be generated for transStatus ="Y"	Payment System-specific value provided as part of the ACS registration for each supported DS.
whiteListStatus	String	O	1 character	Enables the communication of trusted beneficiary/ whitelist status between the ACS, the DS and the 3DS Requestor.	Values accepted: • Y = 3DS Requestor is whitelisted by cardholder • N = 3DS Requestor is not white listed by cardholder • E = Not eligible as determined by issuer • P = Pending confirmation by cardholder • R = Cardholder rejected • U = Whitelist status unknown, unavailable, or does not apply
whiteListStatusSource	String	O	2 characters	This data element will be populated by the system setting Whitelist Status.	Values accepted: • 01 = 3DS Server • 02 = DS • 03 = ACS • 04-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80-99 = Reserved for DS use.

Field Name	Data Type	Message Inclusion	Length	Field Value	Field Description
acsDecConInd	String	1 char acter	C	Indicates whether the ACS confirms utilization of Decoupled Authentication and agrees to utilize Decoupled Authentication to authenticate the Cardholder	Required if Transaction Status = D Values accepted: • Y = Confirms Decoupled Authentication will be utilized • N = Decoupled Authentication will not be utilized Note: if 3DS Requestor Decoupled Request Indicator = N, a value of Y cannot be returned in the ACS Decoupled Confirmation Indicator.registration for each supported DS.
acsRenderingType	JSON Data Type: Object	C			
acsRendering Type.acsInterface	String	C	2 characters	01 = Native UI 02 = HTML UI	
acsRenderingType. acsUiTemplate	String	C	2 characters	01 = Text 02 = Single Select 03 = Multi Select 04 = OOB 05 = HTML Other (valid only for HTML UI)	

Field Nam e	Data Type	Message Inclusion	Length	Field Value	Field Description
acsSignedContent	JSON Data Type: Object	C	Length: Variable	Required only for SDK InApp transaction s v2.0.1 and above	As per EMVCo specs
transStatus	String	R	Length: 1 character		As per EMVCo spec
acsChallengeReqUrl	String	C	Variable, maximum 2048 characters	Values accepted: Fully qualified ACS URL, where in Merchant needs to post the Challenge request to ACS	Fully qualified ACS URL, where in Merchant needs to post the Challenge request to ACS
authenticationUrl	String	C	Variable, maximum 2048 characters	Values accepted: Fully qualified 3DS Server URL for fetching Authentication Value, eci	Fully qualified 3DS Server URL for fetching Authentication Value, eci.
merc hant Canc elCha lleng eAut hUrl	String	Varia ble, maxi mum 2048 char acter s	C	Values accepted: Fully qualified 3DS Server URL for cancelling the challenge by Merchant	
mess ageE xtens ion	JSON Data Type: Array	Varia ble, maxi mum 8192 0 bytes	C	// Sample Message Extension Tag "messageEx tension": [{ "name": "extensionF ield1" "id": "ID1", "criticalityI ndicator": true, "data":{ "valueOne": "value" }]	Data necessary to support requirements not otherwise defined in the 3-D Secure message are carried in a Message Extension.

Field Name	Data Type	Message Inclusion	Length	Field Value	Field Description
acsChallengeR eqFormData	JSON Object Map		C	Required for Browser Ecom 1.0.2 and above ThreeDSRe questor needs to post the data as Form Post to the ACS URL obtained from acsChalleng eReqUrl, form data Name and Value needs to be picked from the Json Object Map.	Required for Browser Ecom 1.0.2 and above ThreeDSRequestor needs to post the data as Form Post to the ACS URL obtained from acsChallengeReqUrl, form data Name and Value needs to be picked from the Json Object Map.

6.5   JSON Request Field Details:pRqFrq

Field Name	Data Type	Message Inclusion	Length	Field Value	Field Description
messageType	String	R	Variable, 5–8 characters	pRqFr	Identifies the Message Type
p_message Version	String	R	Variable, 5–8 characters	2.1.0	Message Protocol Version Number of the specification
messageVersion	String	R	Variable, 5–8 characters	2.1.0	EMVCo Protocol Version Number of the specification
threeDSSer verTransID	String	R	Length: 36 characters	UUID format	3DS Server Unique Transaction ID
acsTransID	String	R	Length: 36 characters	UUID format	ACS Server Unique Transaction ID
dsTransID	String	O	Length: 36 characters	UUID format	DS Server Unique Transaction ID
merchantTransID	String	R	Length: 36 characters	UUID format	Merchant Server Unique Transaction ID
sdkTransID	String	C	36 characters	UUID format Required for an APP Transaction	SDK Server Unique Transaction ID, field is required only for SDK In App transaction for 2.0.1 version and beyond
acquirerID	String	R	4 characters; Numeric		Acquirer Identifier assigned by 3DSS / MPI
acsAu thRes ponse	String		C	Values accepted: Base64 URL Encoded PaRes or cRes data received from ACS.	Base64 URL Encoded PaRes or cRes data received from ACS.

Field Name	Data Type	Message Inclusion	Length	Field Value	Field Description
messageExtension	JSON Data Type:Array	Variable, maxi mum 81920 bytes	C	// Sample Message Extension Tag "messageExtension" : [{ "name": "extensionField1" "id": "ID1", "criticalityIndicator ": true, "data":{ "valueOne":"value" },{ "name": "Travel Industry", "id": "A000000802-002", "criticalityIndicator ": false, "data"{data fields mentioned in the section 4.3.0 below for 2.0 transactions}]	Data necessary to support requirements, not otherwise defined in the 3-D Secure message is carried in a Message Extension.

6.6   JSON Request Field Details: pRsfr

Field Nam e	Data Type	Message Inclusion	Field Length	Field Value	Field Description
messageType	String	R	Variable, 5–8 characters	pRsFr	Identifies the Message Type
p_messageVersion	String	R	Variable, 5–8 characters	2.1.0	Message Protocol Version Number of the specification
messageVersion	String	R	Variable, 5–8 characters	2.1.0	EMVCo Protocol Version Number of the specification
threeDSServerTransID	String	R	36 characters	UUID format	3DS Server Unique Transaction ID
acsTransID	String	C	36 characters	UUID format	ACS Server Unique Transaction ID
dsTransID	String	O	36 characters	UUID format	DS Server Unique Transaction ID
merchantTransID	String	R	36 characters	UUID format	Merchant Server Unique Transaction ID
sdkTransID	String	C	36 characters	UUID format Required for an APP Transaction	SDK Server Unique Transaction ID
eci	String	C	2 characters		As per EMVCo / DS specs
authenticationValue	String	C	28 characters		Payment System-specific value provided as part of the ACS registration for each supported DS.
transStatus	String	R	1 character		As per EMVCo spec
errorCode	String	R	3 characters, numeric	000- Success 001- Message Signature Hash failed	000- Success 001-999 error codes will be sent basis the validation