

resultsResponse EN



Please note that all data elements listed below will be present in **resultsResponse** but might hold an *empty string* based on the *condition*.

	Key	Format	Condition	Description
1	threeDSSTransID	string	M	BNP Payment platform PayID in canonical format as specified in IETF RFC 4122
2	acsTransID	string	M	Universally Unique transaction identifier assigned by the ACS to identify a single transaction
3	acsRenderingType	object	C	Required unless ACS Decoupled Confirmation = true
4	authenticationType	string	C	Required if the Transaction Status = Y or N. Indicates the type of authentication method the Issuer will use to challenge the cardholder. Required if the Transaction Status = C Values accepted: • 01 = static • 02 = dynamic • 03 = oob Future implementation. Protocol Version 2.2.0 onwards - • 04 = decoupled
5	authenticationValue	string	C	Required if Transaction Status = Y or A
6	challengeCancel	string	C	Indicator informing that the authentication has been canceled. Values accepted: • 01 = Cardholder selected "Cancel" • 02 = Reserved for future EMVCo use (values 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—First CReq not received by ACS • 06 = Transaction Error • 07 = Unknown • 08 = Transaction Timed Out at SDK
7	dsTransID	string	M	Universally unique transaction identifier assigned by the DS to identify a single transaction
8	eci	string	C	Payment System-specific value provided by the ACS or DS to indicate the results of the attempt to authenticate the Cardholder. TP specific.
9	interactionCounter	string	M	Indicates the number of authentication cycles attempted by the Cardholder
10	messageCategory	string	M	Identifies the category of the message for a specific use case. Values accepted: • 01 = PA • 02 = NPA
11	messageExtension	string	C	Data necessary to support requirements not otherwise defined in the 3-D Secure message are carried in a Message Extension. Cc
12	messageType	string	C	Identifies the type of message that failed in case of an error. Values accepted: • ARes • RReq
13	messageVersion	string	M	Protocol version identifier
14	sdkTransID	string	M	Future use. Universally unique transaction identifier assigned by the 3DS SDK to identify a single transaction.
15	transStatus	string	M	Indicates whether a transaction qualifies as an authenticated transaction. Values accepted: • Y = Authentication Verification Successful. • N = Not Authenticated /Account Not Verified; Transaction denied. • U = Authentication/ Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq • A = Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided • C = Challenge Required; Additional authentication is required using the CReq/CRes. • D = Challenge Required; Decoupled Authentication confirmed. • R = Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorisation • I = Informational Only; 3DS Requestor challenge preference acknowledged.

16	transStatusReason	string	C	Provides information on why the Transaction Status field has the specified value. Required if the Transaction Status field = N, U, or Values accepted: • 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 not permitted to cardholder • 13 = Cardholder not enrolled in service • 14 = Transaction timed out at the ACS • 15 = Low confidence • 16 = Medium confidence • 17 = High confidence • 18 = Very High confidence • 19 = Exceeds ACS maximum challenges • 20 = Non-Payment transaction not supported • 21 = 3RI transaction not supported • 22 = ACS technical issue • 23 = Decoupled Authentication required by ACS but not requested by 3DS Requestor • 24 = 3DS Requestor Decoupled Max Expiry Time exceeded • 25 = Decoupled Authentication was provided insufficient time to authenticate cardholder. ACS will not make attempt • 26 = Authentication attempted but not performed by the cardholder
17	whiteListStatus	string	C	Future use. Only supported with protocol version 2.2.0 onwards. Enables the communication of trusted beneficiary/whitelist status Values accepted: • Y = 3DS Requestor is whitelisted by cardholder • N = 3DS Requestor is not whitelisted 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
18	whiteListStatusSource	string	C	Future use. Only supported with protocol version 2.2.0 onwards. This data element will be populated by the system setting Whiteli Values accepted: • 01 = 3DS Server • 02 = DS • 03 = ACS

Schema

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "$id": "https://paymentpage.axepta.bnpparibas/schemas/resultsResponse.json",
  "type": "object",
  "properties": {
    "threeDSSTransID": {
      "type": "string",
      "maxLength": 36
    },
    "acsTransID": {
      "type": "string",
      "maxLength": 36
    },
    "acsRenderingType": {
      "type": "object",
      "properties": {
        "acsInterface": {
          "type": "string",
          "enum": ["native", "html", ""],
          "description": "The ACS interface that the challenge will present to the c"
        },
        "acsUiTemplate": {
          "type": "string",
          "enum": ["text", "singleSelect", "multiSelect", "oob", "other", ""],
          "description": "Identifies the UI Template format that the ACS first prese"
        }
      }
    }
  }
}
```

```

        "required": ["acsInterface", "acsUiTemplate"],
        "additionalProperties": false
    },
    "authenticationType": {
        "type": "string",
        "enum": ["01", "02", "03", "04", ""]
    },
    "authenticationValue": {
        "type": "string",
        "maxLength": 28
    },
    "challengeCancel": {
        "type": "string",
        "enum": ["01", "02", "03", "04", "05", "06", "07", "08", ""]
    },
    "dsTransID": {
        "type": "string",
        "maxLength": 36
    },
    "eci": {
        "type": "string",
        "maxLength": 2
    },
    "interactionCounter": {
        "type": "string",
        "maxLength": 2
    },
    "messageCategory": {
        "type": "string",
        "enum": ["01", "02"]
    },
    "messageExtension": {
        "type": "string",
        "maxLength": 81920
    },
    "messageVersion": {
        "type": "string",
        "minLength": 5,
        "maxLength": 8
    },
    "sdkTransID": {
        "type": "string",
        "maxLength": 36
    },
    "transStatus": {
        "type": "string",
        "enum": ["Y", "N", "U", "A", "C", "D", "R", "I", ""]
    },
    "transStatusReason": {
        "type": "string",
        "enum": ["01", "02", "03", "04", "05", "06", "07", "08", "09", "10", "11", "12", "13", "14", "15", "16", "17", "18", "19", "20", "21", "22", "23", "24", "25", "26", ""]
    },
    "required": ["threeDSServerTransID", "acsTransID", "acsRenderingType", "authenticationType", "authenticationValue", "dsTransID", "eci", "interactionCounter", "messageCategory", "messageExtension", "messageVersion", "sdkTransID", "transStatusReason"],
    "additionalProperties": false
}

```

Sample

```
{
  "threeDSServerTransID": "9e944d5d-56f3-461d-a393-80a666d346d1",
  "acsTransID": "1e43b52f-3623-4e5d-8917-41c5c15b7218",
  "acsRenderingType": {
    "acsInterface": "01",
    "acsUiTemplate": "01"
  },
  "authenticationType": "02",
  "authenticationValue": "JAmi21makAifmwqo2120cj1AAA=",
  "challengeCancel": "",
  "dsTransID": "c626e8a0-f2ba-42b3-aa6d-620658421f3a",
  "eci": "05",
  "interactionCounter": "01",
  "messageCategory": "01",
  "messageExtension": "",
  "messageVersion": "2.1.0",
  "sdkTransID": "",
  "transStatus": "Y",
  "transStatusReason": ""
}
```