



EMV®

3-D Secure

JSON Message Samples

Version 2.1.0

April 2018

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Contents

Introduction.....	4
AReq message samples	5
AReq—01-APP	5
AReq—02-BRW	8
ARes message samples	11
ARes—01-APP—Challenge flow	11
ARes—01-APP—Frictionless flow.....	11
ARes—02-BRW—Challenge flow.....	12
CReq message sample—01-APP	12
CRes message sample—01-APP	13
Error message sample	14
PReq message sample	15
PRes message sample	15
RReq message sample	16
RRes message sample	16

Introduction

This document contains examples of 3-D Secure messages based on the *3-D Secure Protocol and Core Functions Specification V 2.1.0*.

The messages are constructed (not based on real implementation). The values of the data elements are random numbers or string.

AReq message samples

AReq—01-APP

This example is an AReq message between the DS and the ACS. For the AReq message between the 3DS Server and the DS, the Device Information (deviceInfo) data element shall be replaced by its encrypted version the SDK Encrypted Data (sdkEncData).

```
{
  "threeDSRequestorID": "az0123456789",
  "threeDSRequestorName": "Example Requestor name",
  "threeDSRequestorURL": "https://threedsrequestor.adomainname.net",
  "acquirerBIN": "868491",
  "acquirerMerchantID": "mGm6AJZlYotkJJmOk0fx",
  "addrMatch": "N",
  "cardExpiryDate": "1910",
  "acctNumber": "8944988785642183",
  "billAddrCity": "Bill City Name",
  "billAddrCountry": "840",
  "billAddrLine1": "Bill Address Line 1",
  "billAddrLine2": "Bill Address Line 2",
  "billAddrLine3": "Bill Address Line 3",
  "billAddrPostCode": "Bill Post Code",
  "billAddrState": "CO",
  "email": "example@example.com",
  "homePhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "mobilePhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "cardholderName": "Cardholder Name",
  "shipAddrCity": "Ship City Name",
  "shipAddrCountry": "840",
  "shipAddrLine1": "Ship Address Line 1",
  "shipAddrLine2": "Ship Address Line 2",
  "shipAddrLine3": "Ship Address Line 3",
  "shipAddrPostCode": "Ship Post Code",
  "shipAddrState": "CO",
  "workPhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "deviceChannel": "01",
  "deviceRenderOptions": {
    "sdkInterface": "03",
    "sdkUiType": [ "01", "02", "03", "04", "05" ]
  }
},
```

```
"mcc": "5411",
"merchantCountryCode": "840",
"merchantName": "UL TS BV",
"messageCategory": "01",
"messageType": "AReq",
"messageVersion": "2.1.0",
"purchaseAmount": "101",
"purchaseCurrency": "978",
"purchaseExponent": "2",
"purchaseDate": "20170316141312",
"sdkAppID": "dbd64fcb-c19a-4728-8849-e3d50bfdde39",
"sdkMaxTimeout": "05",
"sdkEphemPubKey": {
  "kty": "EC",
  "crv": "P-256",
  "x": "WWcpTjbOqiu_1aODllw5rYTq5oLXE_T0huCPjMIRbkI",
  "y": "Wz_7anIeadV8SJZUfr4drwjzuWoUbOsHp5GdRZBAAiw"
},
"sdkReferenceNumber": "3DS_LOA_SDK_PPFU_020100_00007",
"sdkTransID": "b2385523-a66c-4907-ac3c-91848e8c0067",
"transType": "01",
"threeDSServerURL": "https://threedssserver.adomainname.net",
"threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
"threeDSServerRefNumber": "3DS_LOA_SER_PPFU_020100_00008",
"threeDSRequestorAuthenticationInd": "03",
"threeDSRequestorAuthenticationInfo": {
  "threeDSReqAuthMethod": "02",
  "threeDSReqAuthTimestamp": "201711071307",
  "threeDSReqAuthData": "validlogin at UL TS BV"
},
"threeDSRequestorChallengeInd": "02",
"threeDSRequestorPriorAuthenticationInfo": {
  "threeDSReqPriorRef": "d7clee99-9478-44a6-b1f2-391e29c6b340",
  "threeDSReqPriorAuthMethod": "02",
  "threeDSReqPriorAuthTimestamp": "201710282113",
  "threeDSReqPriorAuthData": "cKTYtrvvKU7gUoiqbb07Po"
},
"threeDSServerOperatorID": "1jpeeLAWgGFgS1Ri9tX9",
"acctType": "03",
"acctInfo": {
  "chAccAgeInd": "03",
  "chAccDate": "20140328",
  "chAccChangeInd": "04",
  "chAccChange": "20160712",
  "chAccPwChangeInd": "02",
  "chAccPwChange": "20170328",
  "shipAddressUsageInd": "04",
  "shipAddressUsage": "20160714",
  "txnActivityDay": "1",
  "txnActivityYear": "21",
  "provisionAttemptsDay": "0",
  "nbPurchaseAccount": "11",
  "suspiciousAccActivity": "01",
  "shipNameIndicator": "02",
  "paymentAccInd": "04",
```

```
        "paymentAccAge": "20160917"
      },
      "acctID": "personal account",
      "dsReferenceNumber": "DS_LOA_DIS_PPFU_020100_00010",
      "dsTransID": "1jpe0dc0-i9t2-4067-bcb1-nmt866956sgd",
      "dsURL": "https://dsserver.domainname.com",
      "payTokenInd": true,
      "purchaseInstalData": "024",
      "merchantRiskIndicator": {
        "shipIndicator": "02",
        "deliveryTimeframe": "01",
        "deliveryEmailAddress": "deliver@email.com",
        "reorderItemsInd": "01",
        "preOrderPurchaseInd": "02",
        "preOrderDate": "20170519",
        "giftCardAmount": "337",
        "giftCardCurr": "840",
        "giftCardCount": "02"
      },
      "messageExtension": [ {
        "name": "msgextname",
        "id": "501341592B_0001_4568",
        "criticalityIndicator": false,
        "data": {
          "valueOne": "messageextensiondata",
          "valueTwo": "moremessageextensiondata"
        }
      }
    ],
    "recurringExpiry": "20180131",
    "recurringFrequency": "6",
    "broadInfo": { "message": "TLS 1.x will be turned off starting summer 2019"
  },
  "deviceInfo": "ew0KCSJEViI6ICiXlJjAiLA0KCSJERCI6IHsNCgkJIkMwMDEiOiAiQW5kc
m9pZCIsDQoJCSJDMDAYIjogIkhUQyBPbmVfTTgiLA0KCQkiQzAwNCI6ICIlLjAuMSIsDQoJCSJDMD
AlIjogImVuX1VTIiwNCgkJIkMwMDYiOiAiRWFzdGVybiBTdGFuZGFyZCBUaW1lIiwNCgkJIkMwMDc
iOiAiMDY3OTc5MDMTZmI2MS00MWVvLk0YzItNGQyYjc0ZTI3ZDE4IiwNCgkJIkMwMDkiOiAiSm9o
bidzIEFuZHZHJvaWQgRGV2aWNlIiw0K0CX0sDQoJIKRQTkEiOiB7DQoJCSJDMDewIjogIlJFMDEiLA0KC
QkiQzAxMSI6ICJSRTAzIiw0K0CX0sDQoJIlNXIjogWyJTVzAxIiwgIlNXMDQiXQ0KfQ0K"
}
```

AReq—02-BRW

```
{
  "threeDSCompInd": "Y",
  "threeDSRequestorID": "az0123456789",
  "threeDSRequestorName": "Example Requestor name",
  "threeDSRequestorURL": "https://threedsrequestor.adomainname.net",
  "acquirerBIN": "868491",
  "acquirerMerchantID": "mGm6AJZ1YotkJJmOk0fx",
  "addrMatch": "N",
  "cardExpiryDate": "1910",
  "acctNumber": "8944988785642183",
  "billAddrCity": "Bill City Name",
  "billAddrCountry": "840",
  "billAddrLine1": "Bill Address Line 1",
  "billAddrLine2": "Bill Address Line 2",
  "billAddrLine3": "Bill Address Line 3",
  "billAddrPostCode": "Bill Post Code",
  "billAddrState": "CO",
  "email": "example@example.com",
  "homePhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "mobilePhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "cardholderName": "Cardholder Name",
  "shipAddrCity": "Ship City Name",
  "shipAddrCountry": "840",
  "shipAddrLine1": "Ship Address Line 1",
  "shipAddrLine2": "Ship Address Line 2",
  "shipAddrLine3": "Ship Address Line 3",
  "shipAddrPostCode": "Ship Post Code",
  "shipAddrState": "CO",
  "workPhone": {
    "cc": "123",
    "subscriber": "123456789"
  },
  "deviceChannel": "02",
  "browserAcceptHeader": "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
  "browserIP": "192.168.1.11",
  "browserJavaEnabled": true,
  "browserLanguage": "en",
  "browserColorDepth": "48",
  "browserScreenHeight": "400",
  "browserScreenWidth": "600",
  "browserTZ": "0",
  "browserUserAgent": "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0",
  "mcc": "5411",
```



```
"merchantCountryCode": "840",
"merchantName": "UL TS BV",
"messageCategory": "01",
"messageType": "AReq",
"messageVersion": "2.1.0",
"purchaseAmount": "101",
"purchaseCurrency": "978",
"purchaseExponent": "2",
"purchaseDate": "20170316141312",
"transType": "01",
"threeDSServerURL": " https://threeDSserver.adomainname.net ",
"threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
"threeDSServerRefNumber": "3DS_LOA_SER_PPFU_020100_00008",
"threeDSRequestorAuthenticationInd": "03",
"threeDSRequestorAuthenticationInfo": {
  "threeDSReqAuthMethod": "02",
  "threeDSReqAuthTimestamp": "201711071307",
  "threeDSReqAuthData": "validlogin at UL TS BV"
},
"threeDSRequestorChallengeInd": "02",
"threeDSRequestorPriorAuthenticationInfo": {
  "threeDSReqPriorRef": "d7clee99-9478-44a6-b1f2-391e29c6b340",
  "threeDSReqPriorAuthMethod": "02",
  "threeDSReqPriorAuthTimestamp": "201710282113",
  "threeDSReqPriorAuthData": "cKTYtrvvKU7gUoiqbb07Po"
},
"threeDSServerOperatorID": "1jpeeLAWgGFgSlRi9tX9",
"acctType": "03",
"acctInfo": {
  "chAccAgeInd": "03",
  "chAccDate": "20140328",
  "chAccChangeInd": "04",
  "chAccChange": "20160712",
  "chAccPwChangeInd": "02",
  "chAccPwChange": "20170328",
  "shipAddressUsageInd": "04",
  "shipAddressUsage": "20160714",
  "txnActivityDay": "1",
  "txnActivityYear": "21",
  "provisionAttemptsDay": "0",
  "nbPurchaseAccount": "11",
  "suspiciousAccActivity": "01",
  "shipNameIndicator": "02",
  "paymentAccInd": "04",
  "paymentAccAge": "20160917"
},
"acctID": "personal account",
"dsReferenceNumber": "DS_LOA_DIS_PPFU_020100_00010",
"dsTransID": "1jpe0dc0-i9t2-4067-bcb1-nmt866956sgd",
"dsURL": "https://dsServer.domainname.com",
"payTokenInd": true,
"purchaseInstalData": "024",
"merchantRiskIndicator": {
  "shipIndicator": "02",
  "deliveryTimeframe": "01",
```

```
        "deliveryEmailAddress": "deliver@email.com",
        "reorderItemsInd": "01",
        "preOrderPurchaseInd": "02",
        "preOrderDate": "20170519",
        "giftCardAmount": "337",
        "giftCardCurr": "840",
        "giftCardCount": "02"
    },
    "messageExtension": [ {
        "name": "msgextname",
        "id": "501341592B_0001_4567",
        "criticalityIndicator": false,
        "data": {
            "valueOne": "messageextensiondata",
            "valueTwo": "moremessageextensiondata"
        }
    } ],
    "recurringExpiry": "20180131",
    "recurringFrequency": "6",
    "broadInfo": { "message": "TLS 1.x will be turned off starting summer 2019"
  }, ,
}
```


ARes—02-BRW—Challenge flow

```
{
  "messageVersion": "2.1.0",
  "dsTransID": "f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
  "messageType": "ARes",
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "acsTransID": "d7clee99-9478-44a6-b1f2-391e29c6b340",
  "acsReferenceNumber": "3DS_LOA_ACS_PPFU_020100_00009",
  "acsOperatorID": "AcsOpId 4138359541",
  "dsReferenceNumber": "DS_LOA_DIS_PPFU_020100_00010",
  "transStatus": "C",
  "acsChallengeMandated": "Y",
  "acsURL": "https://test.com",
  "authenticationType": "01"
}
```

CReq message sample—01-APP

This example contains data before encryption as a JWE.

```
{
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "acsTransID": "d7clee99-9478-44a6-b1f2-391e29c6b340",
  "messageType": "CReq",
  "messageVersion": "2.1.0",
  "sdkTransID": "b2385523-a66c-4907-ac3c-91848e8c0067",
  "sdkCounterStoA": "001"
}
```

CRes message sample—01-APP

This example contains data before encryption as a JWE.

```
{
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "acsTransID": "d7c1ee99-9478-44a6-b1f2-391e29c6b340",
  "acsUiType": "01",
  "challengeAddInfo": "Additional information to be shown.",
  "challengeCompletionInd": "N",
  "challengeInfoHeader": "Header information",
  "challengeInfoLabel": "One-time-password",
  "challengeInfoText": "Please enter the received one-time-password",
  "challengeInfoTextIndicator": "N",
  "expandInfoLabel": "Additional instructions",
  "expandInfoText": "The issuer will send you via SMS a one-time password.
Please enter the value in the designated input field above and press continue
to complete the 3-D Secure authentication process.",
  "issuerImage": {
    "medium": "https://acs.com/medium_image.svg",
    "high": "https://acs.com/high_image.svg",
    "extraHigh": "https://acs.com/extraHigh_image.svg"
  },
  "messageType": "CRes",
  "messageVersion": "2.1.0",
  "psImage": {
    "medium": "https://ds.com/medium_image.svg",
    "high": "https://ds.com/high_image.svg",
    "extraHigh": "https://ds.com/extraHigh_image.svg"
  },
  "resendInformationLabel": "Send new One-time-password",
  "sdkTransID": "b2385523-a66c-4907-ac3c-91848e8c0067",
  "submitAuthenticationLabel": "Continue",
  "whyInfoLabel": "Why using 3-D Secure?",
  "whyInfoText": "Some explanation about why using 3-D Secure is an
excellent idea as part of an online payment transaction",
  "acsCounterAtoS": "001"
}
```

Error message sample

```
{
  "threeDSServerTransID": "6afa6072-9412-446b-9673-2f98b3ee98a2",
  "acsTransID": "375d90ad-3873-498b-9133-380cbbc8d99d",
  "dsTransID": "0b470d4f-fdf8-429f-9147-505b1a589883",
  "errorCode": "203",
  "errorComponent": "A",
  "errorDescription": "Data element not in the required format. Not
numeric or wrong length.",
  "errorDetail": "billAddrCountry,billAddrPostCode,dsURL",
  "errorMessageType": "AReq",
  "messageType": "Erro",
  "messageVersion": "2.1.0",
  "sdkTransID": "b2385523-a66c-4907-ac3c-91848e8c0067"
}
```

PReq message sample

```
{
  "threeDSServerRefNumber": "3DS_LOA_SER_PPFU_020100_00008",
  "threeDSServerOperatorID": "1jpeeLAWgGFgSlRi9tX9",
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "messageType": "PReq",
  "messageVersion": "2.1.0",
  "serialNum": "66lM7xWInwdqG1SSFk5"
}
```

Pres message sample

```
{
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "dsTransID": "f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
  "messageType": "Pres",
  "messageVersion": "2.1.0",
  "serialNum": "3q9oaApFqmnys47ujRg",
  "dsStartProtocolVersion": "2.1.0",
  "dsEndProtocolVersion": "2.1.0",
  "cardRangeData": [ {
    "startRange": "1000000000000000",
    "endRange": "10000000000005000",
    "actionInd": "A",
    "acsStartProtocolVersion": "2.1.0",
    "acsEndProtocolVersion": "2.1.0",
    "threeDSMethodURL": "https://www.acs.com/script"
  },
    {
    "startRange": "2000000000000000",
    "endRange": "20000000000004000",
    "dsStartProtocolVersion": "2.1.0",
    "dsEndProtocolVersion": "2.1.0",
    "actionInd": "D",
    "acsStartProtocolVersion": "2.1.0",
    "acsEndProtocolVersion": "2.1.0",
    "threeDSMethodURL": "https://www.acs2.com/method"
  }
  ]
}
```

RReq message sample

```
{
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "acsTransID": "d7c1ee99-9478-44a6-b1f2-391e29c6b340",
  "acsRenderingType": {
    "acsInterface": "01",
    "acsUiTemplate": "01"
  },
  "authenticationMethod": "02",
  "authenticationType": "02",
  "authenticationValue": "MTIzNDU2Nzg5MDA5ODc2NTQzMjE=",
  "dsTransID": "f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
  "eci": "05",
  "interactionCounter": "02",
  "messageCategory": "01",
  "messageType": "RReq",
  "messageVersion": "2.1.0",
  "transStatus": "Y"
}
```

RRes message sample

```
{
  "threeDSServerTransID": "8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
  "acsTransID": "d7c1ee99-9478-44a6-b1f2-391e29c6b340",
  "dsTransID": "f25084f0-5b16-4c0a-ae5d-b24808a95e4b",
  "messageType": "RRes",
  "messageVersion": "2.1.0",
  "resultsStatus": "01"
}
```