



# **EMV®**

## **3-D Secure**

---

### **Device Acknowledgement Message Extension**

Version 3.0

August 2022

## Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

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

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

## Contents

Legal Notice .....	2
Contents .....	3
Tables .....	3
Introduction .....	4
Supporting Documentation .....	4
Device Acknowledgement Message Extension Data Elements .....	5
Message Format .....	12
Device Acknowledgement Message Extension Samples .....	14

## Tables

Table 1: Device Acknowledgement Message Extension Data Elements .....	5
Table 2: Data .....	6
Table 3: AReq Message Extension Data Elements .....	12
Table 4: ARes Message Extension Data Elements .....	13

# Introduction

This document provides the EMV® 3-D Secure Device Acknowledgement Message Extension v3.0 and describes, in the context of the *EMV 3-D Secure Protocol and Core Functions Specification v2.1.0* and *v2.2.0*, how:

- the 3DS Server that interfaces with a Split-SDK can provide the Split-SDK-related data to the ACS for use in risk-decisioning
- the ACS can acknowledge data received in 3-D Secure Device Information, particularly for Device Information Data Version 1.3 or higher.

The Device Acknowledgement Message Extension is only present in the AReq message version 2.1.0 or 2.2.0 when the 3DS Requestor uses a Split-SDK for the App flow.

The Device Acknowledgement Message Extension is only present in the ARes message version 2.1.0 or 2.2.0 if the ACS:

- acknowledges the supported Device Information, AND/OR
- provides additional data to the Split-SDK in the case of a challenge (Transaction Status = C)

## Supporting Documentation

The following documents are specific to the EMV 3-D Secure protocol and should be used in conjunction with this specification. These documents, as well as the *EMV® 3-D Secure Frequently Asked Questions*, are located on the EMVCo website.

- *EMV® 3-D Secure—Protocol and Core Functions Specification v2.3.1.0*
- *EMV® 3-D Secure—Split-SDK Specification v2.3.1.0*
- *EMV® Specification Bulletin No. 255—EMV® 3-D Secure Specification Version Configuration*

# Device Acknowledgement Message Extension Data Elements

**Table 1: Device Acknowledgement Message Extension Data Elements**

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Assigned Extension Group Identifier  Field Name: <code>id</code>	A unique identifier for the extension.	3DS Server ACS	Length: 14 characters  JSON Data Type: String  Value accepted: <ul style="list-style-type: none"><li>• A000000802-001</li></ul>	AReq = R  ARes = R
Criticality Indicator  Field Name: <code>criticalityIndicator</code>	A Boolean value indicating whether the recipient must understand the contents of the extension to interpret the entire message.	3DS Server ACS	JSON Data Type: Boolean  Value accepted: <ul style="list-style-type: none"><li>• false</li></ul>	AReq = R  ARes = R
Data  Field Name: <code>data</code>	The data carried in the extension.	3DS Server ACS	Length: Variable, maximum 8059 characters  JSON Data Type: Object  Values accepted: <ul style="list-style-type: none"><li>• Refer to Table 2 for data elements</li></ul>	AReq = R  ARes = R
Extension Name  Field Name: <code>name</code>	The name of the extension data set as defined by the extension owner.	3DS Server ACS	Length: 19 characters  JSON Data Type: String  Value accepted: <ul style="list-style-type: none"><li>• Dev Ack - Split-SDK</li></ul>	AReq = R  ARes = R

**Table 2: Data**

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Extension Version Number Field Name: version	Version number of the message extension.	3DS Server ACS	Length: 3 characters JSON Data Type: String Value accepted: <ul style="list-style-type: none"><li>• 3.0</li></ul>	AReq = R ARes = R
Default-SDK Type Field Name: defaultSdkType	Indicates the characteristics of a Default-SDK.  SDK Variant: SDK implementation characteristics  Wrapped Indicator: If the Default-SDK is embedded as a wrapped component in the 3DS Requestor App  Example: <pre>"defaultSdkType": {     "sdkVariant": "01",     "wrappedInd": "Y" }</pre>	3DS Server	JSON Data Type: Object sdkVariant Length: 2 characters JSON Data Type: String Values accepted: <ul style="list-style-type: none"><li>• 01 = Native</li><li>• 02–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)</li><li>• 80–99 = Reserved for DS use</li></ul> wrappedInd Length: 1 character JSON Data Type: String Value accepted: <ul style="list-style-type: none"><li>• Y = Wrapped</li></ul> Only present if value = Y	Required if SDK Type = 01

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
SDK Authentication Type  Field Name: sdkAuthenticationType	Authentication methods preferred/supported by the 3DS SDK in order of preference.	3DS SDK	Size: 1–99 elements  JSON Data Type: Array of String  String: 2 characters  Values accepted: <ul style="list-style-type: none"><li>• 01 = Static Passcode</li><li>• 02 = SMS OTP</li><li>• 03 = Key fob or EMV card reader OTP</li><li>• 04 = App OTP</li><li>• 05 = OTP Other</li><li>• 06 = KBA</li><li>• 07 = OOB Biometrics</li><li>• 08 = OOB Login</li><li>• 09 = OOB Other</li><li>• 10 = Other</li><li>• 11 = Push Confirmation</li><li>• 12–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)</li><li>• 80–99 = Reserved for DS use</li></ul>	Required if SDK Type = 02

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
SDK Server Signed Content  Field Name: sdkServerSignedContent	Contains the JWS object (represented as a string) created by the Split-SDK Server for the AReq message.	3DS SDK	Length: Variable  JSON Data Type: String  Values accepted: <ul style="list-style-type: none"><li>• The body of the JWS object (represented as a string) will contain the following data elements as defined in Table A.1:<ul style="list-style-type: none"><li>◦ SDK Reference Number</li><li>◦ SDK Signature Timestamp</li><li>◦ SDK Transaction ID</li><li>◦ Split-SDK Server ID</li></ul></li></ul>	Conditional based on DS rules. Only present if SDK Type = 02
SDK Signature Timestamp  Field Name: sdkSignatureTimestamp	Date and time indicating when the 3DS SDK generated the Split-SDK Server Signed Content converted into UTC.	3DS SDK	Length: 14 characters  JSON Data Type: String  Date format accepted: <ul style="list-style-type: none"><li>• YYYYMMDDHHMMSS</li></ul>	See SDK Server Signed Content
SDK Type  Field Name: sdkType	Indicates the type of 3DS SDK.  This data element provides additional information to the DS and ACS to determine the best approach for handling the transaction.	3DS Server	Length: 2 characters  JSON Data Type: String  Values accepted: <ul style="list-style-type: none"><li>• 01 = Default-SDK</li><li>• 02 = Split-SDK</li><li>• 03–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)</li><li>• 80–99 = Reserved for DS use</li></ul>	

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Split-SDK Type  Field Name: splitSdkType	<p>Indicates the characteristics of a Split-SDK.</p> <p>Split-SDK Variant: Implementation characteristics of the Split-SDK client</p> <p>Limited Split-SDK Indicator: If the Split-SDK client has limited capabilities</p> <p>Example:</p> <pre>"splitSdkType": {     "sdkVariant": "01",     "limitedInd": "Y" }</pre>	3DS Server	<p>Length: Variable</p> <p>JSON Data Type: Object sdkVariant</p> <p>Length: 2 characters</p> <p>JSON Data Type: String</p> <p>Values accepted:</p> <ul style="list-style-type: none"> <li>• 01 = Native Client</li> <li>• 02 = Browser</li> <li>• 03 = Shell</li> <li>• 04–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)</li> <li>• 80–99 = Reserved for DS use</li> </ul> <p>limitedInd</p> <p>Length: 1 character</p> <p>JSON Data Type: String</p> <p>Value accepted:</p> <ul style="list-style-type: none"> <li>• Y = Limited</li> </ul> <p>Only present if value = Y</p>	Required if SDK Type is present and = 02
Split-SDK Server ID  Field Name: splitSdkServerID	<p>DS-assigned Split-SDK Server identifier.</p> <p>Each DS can provide a unique ID to each Split-SDK Server on an individual basis.</p>	Split-SDK Server	<p>Length: Variable, maximum 32 characters</p> <p>JSON Data Type: String</p> <p>Value accepted:</p> <ul style="list-style-type: none"> <li>• Any individual DS may impose specific formatting and character requirements on the contents of this field.</li> </ul>	See SDK Server Signed Content

Authentication Method  Field Name: authenticationMethod	Indicates the authentication types that the Issuer will use to challenge the Cardholder when in the ARes message or what was used by the ACS when in the RReq message.	ACS	Size: Variable, 1–99  JSON Data Type: Array of String  String: 2 characters  Values accepted: <ul style="list-style-type: none"><li>• 01 = Static Passcode</li><li>• 02 = SMS OTP</li><li>• 03 = Key fob or EMV card reader OTP</li><li>• 04 = App OTP</li><li>• 05 = OTP Other</li><li>• 06 = KBA</li><li>• 07 = OOB Biometrics</li><li>• 08 = OOB Login</li><li>• 09 = OOB Other</li><li>• 10 = Other</li><li>• 11 = Push Confirmation</li><li>• 12 = Decoupled</li><li>• 13 = WebAuthn</li><li>• 14 = SPC</li><li>• 15 = Behavioural biometrics</li><li>• 16–79 = Reserved for future EMVCo use (values invalid until defined by EMVCo)</li><li>• 80–99 = Reserved for DS use</li></ul> If SDK Type = 02 and Split-SDK Type/Limited Indicator = Y, a value of 01 or 06 is not valid.	<ul style="list-style-type: none"><li>• Required in the ARes message if Transaction Status = C or D.</li><li>• Required in the RReq message if Transaction Status = Y or N.</li></ul>
--	--	-----	---	---

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Device Information Recognised Version  Field Name: deviceInfoRecognisedVersion	Indicates the highest Data Version of the Device Information supported by the ACS.	ACS	Length: 3 characters  JSON Data Type: String  Value accepted: <ul style="list-style-type: none"><li>• Any active Device Information Data Version as defined in Table 2 of the <i>EMV® Specification Bulletin No. 255—EMV® 3-D Secure Specification Version Configuration</i>.</li></ul> Example: <ul style="list-style-type: none"><li>• 1.4</li></ul>	ARes = R
Device User Interface Mode  Field Name: deviceUserInterfaceMode	Indicates the user interface mode that the ACS will present to the Cardholder for a challenge.	ACS	Length: 2 numeric characters  JSON Data Type: String  Values accepted: <ul style="list-style-type: none"><li>• 01 = Portrait</li><li>• 02 = Landscape</li><li>• 03 = Voice</li><li>• 04 = Other</li></ul>	ARes = C  Required if Transaction Status = C and if Data Version is greater than or equal to 1.3.

# Message Format

**Table 3: AReq Message Extension Data Elements**

Data Element	Field Name
Assigned Extension Group Identifier	id
Criticality Indicator	criticalityIndicator
Data	data
Extension Name	name
Extension Version Number	version
Default-SDK Type	defaultSdkType
SDK Authentication Type	sdkAuthenticationType
SDK Server Signed Content	sdkServerSignedContent
SDK Signature Timestamp	sdkSignatureTimestamp
SDK Type	sdkType
Split-SDK Server ID	splitSdkServerID
Split-SDK Type	splitSdkType

**Table 4: ARes Message Extension Data Elements**

Data Element	Field Name
Assigned Extension Group Identifier	id
Authentication Method	authenticationMethod
Criticality Indicator	criticalityIndicator
Data	data
Device Information Recognised Version	deviceInfoRecognisedVersion
Device User Interface Mode	deviceUserInterfaceMode
Extension Name	name
Extension Version Number	version

# Device Acknowledgement Message Extension Samples

This is a sample extension that may be included in the AReq message by the 3DS Server. The ACS may consume this additional information as part of its risk evaluation process.

```
"messageExtension": [ {  
    "name": "Dev Ack - Split-SDK",  
    "id": "A000000802-001",  
    "criticalityIndicator": false,  
    "data": {  
        "sdkAuthenticationType": ["02", "03", "04"],  
        "sdkServerSignedContent": "xxxxxxxxxx",  
        "sdkSignatureTimestamp": "20200109185123",  
        "sdkType": "02",  
        "splitSdkType": {  
            "sdkVariant": "01",  
            "limitedInd": "Y"  
        }  
        "splitSdkServerID": "validId",  
        "version": "3.0"  
    }  
} ]
```

This is a sample extension that may be included in the ARes message by the ACS. The 3DS SDK may use this additional information as part of its challenge processing.

```
"messageExtension": [ {  
    "name": " Dev Ack - Split-SDK",  
    "id": "A000000802-001",  
    "criticalityIndicator": false,  
    "data": {  
        "authenticationMethod": ["02", "04"],  
        "deviceInfoRecognisedVersion": "1.5",  
        "deviceUserInterfaceMode": "02",  
        "version": "3.0"  
    }  
} ]
```