



EMV®

3-D Secure

Device Acknowledgement Message Extension

Version 2.0

September 2021

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 Acknowledgment Message Extension Data Elements..... 5

Message Format..... 12

Device Acknowledgment Message Extension Samples 13

Tables

Table 1: Device Acknowledgment Message Extension Data Elements 5

Table 2: Data 6

Table 3: AReq Message Extension Data Elements..... 12

Table 4: ARes Message Extension Data Elements 12

Introduction

This document provides the EMV® 3-D Secure Device Acknowledgment Message Extension v2.0 and describes in the context of *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
- ACS can acknowledge data received in 3-D Secure Device Information particularly for Device Information Data Version 1.3 or above

The Device Acknowledgment 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 Acknowledgment 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 EMV 3-D Secure FAQs are located on the EMVCo website.

- *EMV® 3-D Secure—Protocol and Core Functions Specification v2.3.0.0*
- *EMV® 3-D Secure—Split-SDK Specification v2.3.0.0*
- *SB 255—EMV® 3-D Secure Version Configuration*

Device Acknowledgment Message Extension Data Elements

Table 1: Device Acknowledgment 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 Values accepted: <ul style="list-style-type: none">A000000802-001	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">false	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">Refer to Table 2 for data elements	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">Dev Ack - Split-SDK	AREq = R ARes = R

Table 2: Data

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
Extension Version Number Field Name: <code>version</code>	Version number of the message extension.	3DS Server ACS	Length: 3 characters JSON Data Type: String Values accepted: <ul style="list-style-type: none">• 2.0	AReq = R ARes = R

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

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 Value accepted: The body of JWS object (represented as a string) will contain the following data elements as defined in Table A.1: <ul style="list-style-type: none">• SDK Reference Number• SDK Signature Timestamp• SDK Transaction ID• Split-SDK Server ID	Conditional based on DS rules. Only present if SDK Type = 02, 03, 04 or 05
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">• YYYYMMDDHHMM	See SDK Server Signed Content.

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
SDK Type Field Name: <code>sdkType</code>	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 SDK	Length: 2 characters JSON Data Type: String Values accepted: <ul style="list-style-type: none">• 01 = Default SDK• 02 = Split-SDK• 03 = Limited-SDK• 04 = Browser-SDK• 05 = Shell-SDK• 06–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)• 80–99 = Reserved for DS use	
Split-SDK Server ID Field Name: <code>splitSdkServerID</code>	DS assigned Split-SDK Server identifier. Each DS can provide a unique ID to each Split-SDK Server on an individual basis.	Split-SDK Server	Length: Variable, maximum 32 characters JSON Data Type: String Value accepted: Any individual DS may impose specific formatting and character requirements on the contents of this field.	See SDK Server Signed Content.

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
<p>Authentication Method</p> <p>Field Name: authenticationMethod</p>	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	<p>Size: Variable, 1–99</p> <p>JSON Data Type: Array of String</p> <p>String: 2 characters</p> <p>Values accepted:</p> <ul style="list-style-type: none"> • 01 = Static Passcode • 02 = SMS OTP • 03 = Key fob or EMV card reader OTP • 04 = App OTP • 05 = OTP Other • 06 = KBA • 07 = OOB Biometrics • 08 = OOB Login • 09 = OOB Other • 10 = Other • 11 = Push Confirmation • 12–79 = Reserved for future EMVCo use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use <p>If SDK Type = 03, a value of 01 or 06 is not valid.</p>	<p>For ARes, required if the Transaction Status = C or D in the ARes message.</p> <p>For RReq, required in the RReq message if the Transaction Status = Y or N in the RReq message.</p>

Data Element/Field Name	Description	Source	Length/Format/Values	Inclusion
<p>Device Information Recognition Version</p> <p>Attribute Name: deviceInfoRecognisedVersion</p>	Indicates the highest Data Version of the Device Information that the ACS supports.	ACS	<p>Length: 3 characters</p> <p>JSON Data Type: String</p> <p>Value accepted:</p> <p>Any active Device Information Data Version as defined in Table 2 of <i>SB 255—EMV® 3-D Secure Specification Version Configuration</i></p> <ul style="list-style-type: none"> Example: 1.4 	ARes = R
<p>Device User Interface Mode</p> <p>Attribute Name: deviceUserInterfaceMode</p>	Indicates the user interface mode that the ACS will present to the Cardholder for a challenge.	ACS	<p>Length: 2 numeric characters</p> <p>JSON Data Type: String</p> <p>Values accepted:</p> <ul style="list-style-type: none"> 01 = Portrait 02 = Landscape 03 = Voice 04 = Other 	<p>ARes = C</p> <p>Required if Transaction Status = C and if Data Version is greater than or equal to 1.3.</p>

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
SDK Authentication Type	sdkAuthenticationType
SDK Server Signed Content	sdkServerSignedContent
SDK Signature Timestamp	sdkSignatureTimestamp
SDK Type	sdkType
Split-SDK Server ID	splitSdkServerID

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 Recognition Version	deviceInfoRecognisedVersion
Device User Interface Mode	deviceUserInterfaceMode
Extension Name	Name
Extension Version Number	version

Device Acknowledgment 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",
    "splitSdkServerID": "validId",
    "version": "2.0"
  }
}]
```

This is a sample extension that may be included in the ARes message by the ACS. The 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": "2.0"
  }
}]
```