Mastercard® Authentication Best Practices

January 2021

About this Guide

This Best Practice guide is intended for customers that support ecommerce transactions from anywhere within the UK or the EU.

The purpose is to provide the latest developments on the Mastercard authentication network and offer guidance to meet the new Strong Consumer Authentication (SCA) requirements, avoid unnecessary declines and step-ups, and optimize the end consumer experience.

This guide should be used alongside the main Authentication Guide for Europe, which can be found on MC Connect, and not as a replacement. The Authentication Guide for Europe will be periodically updated with learnings contained in the Best Practices Guide, but the Best Practices guide will be published more frequently (on a monthly basis) to ensure the most up-to-date learnings are constantly available.

Contents

Key Best Practices in January 2021 5
General Guidance on EMV 3DS and PSD2 SCA 6
EMV 3DS 2.1+ is mandated 6
EMV 3DS 2.2+ is supported 6
Fallback to 3DS1 6
How to Achieve PSD2 Compliance with 3DS1 6
Rejected Authentications Cannot be Sent to Authorization 8
Soft Decline Processing – Response Code 65 8
SCA Requirements during Soft Enforcement 9
Mastercard PSD2 Testing Programs 9
Guidance for Acquirers, Merchants and 3DS Servers 10
3DS Servers to Correct Information from Merchants 10
Merchant App Flow Performance 10
Missing or Inaccurate Data in Key EMV 3DS fields 12
Address Match Indicator 12
Merchant Name 13
Merchant Enrollment 13
Acquirer Country Code 13
Acquirer Authorization Processing 13
KPI - Invalid DS Transaction ID 14
KPI - Missing Exemption Indicator 14
MIT/RP - Invalid POS Cardholder Presence: 15
KPI - MIT/RP - Missing Trace ID 15
Mitigating non-3DS Declines 16
Guidance for Issuers and ACS's 17
Challenge Indicator 17
AAV Leading Indicators 17
On-behalf AAV Validation (OBS5) Results 18
KPI - Invalid AAV 18
KPI - Mismatching Amount 19
Amount tolerance 19
Guidance on Mixed Features for ACS's, 3DS Servers and SDKs 21
ISO Codes 21

Method URL 21
ACSCounter and SDKCounters 22
ACSSignedContent and sdkEphemPubKey 22
Displaying Info Texts 22
APPENDIX-A: Successful Identity Check Migration 23
APPENDIX-B: DS Transaction ID 25
APPENDIX-C: AAV Leading Indicators 29

Key Best Practices in January 2021

The following table summarizes the major lessons learned and best practices resulting from the Mastercard's heightened awareness process in January 2021:

About:	Guidelines include:
Approval Strategy	- Issuers must consider and develop a risk-based PSD2 SCA compliant strategy to maximize frictionless authentication and avoid incremental abandonment due to challenge failures. - Issuers must not apply incremental decline logic for transactions that are (most likely) compliant with PSD2 SCA regulation. - Issuers must be prepared to authorize the various Acquirer exemptions and exclusions. - As MIT and Recurring Payment excluded/exempted authorizations are not obtaining great approval rates. Issuers must correct their approval process/logic to avoid unnecessary declines.

Soft Declines	- Issuers must not systematically Soft Decline Acquirer exemption requests or exclusions.
	- Issuers must not Soft Decline authorization requests:
	  - When EMV 3DS is not yet supported
	  - When EMV 3DS is supported but with low authentication success rate
	  - That are fully authenticated
	  - That are attempted
	- Merchants and Acquirers must expect Soft Declines on all Acquirer exemption requests (Transaction Risk Analysis, Low-Value Payment, Secure Corporate Payment) or exclusions that the Issuer cannot justify.
	- Acquirers should not (yet) use SCA delegation or the Outage exemption since not yet applicable. Merchants and Acquirers must expect Soft Declines in those cases.
	- When Merchants are going straight to authorization, the support of Soft Declines is critical to absorb Issuer (regulatory) requirement for SCA.

App-based Transactions	- Merchant and Issuers must come together to improve the app flow performance. Only one strategy works: test, analyze and correct.
EMV 3DS Registration	- 3DS Servers and Merchants must align with Acquirers to ensure Merchants are properly and timely registered on ID Check
Info quality	- 3DS Servers must ensure that field values and presence conditions are respected even when those are introduced by Merchants. - ACS Providers must review and correct EMV 3DS errors at the soonest. Most common errors are invalid "eci" and authentication value in RREQ - Merchants and Acquirers must avoid errors during authorization processing. These errors may cause incremental declines specifically post-effective date.
Increased Volumes	- ACS Providers must expect and be prepared for the increasing EMV 3DS authentication volumes: capacity and resilience measures need to be taken. Consider Smart Authentication Direct to assist reducing the volume.

General Guidance on EMV 3DS and PSD2 SCA

EMV 3DS 2.1+ is mandated

EMV 3DS 2.1+ (EMV 3DS 2.1 + Mastercard PSD2 Message Extension) is the corner stone of the Mastercard roadmap, allowing Customers to leverage all PSD2 features as from day-one (Acquirer exemptions, trusted Merchant listing status, secure corporate payment, SCA delegation). EMV 3DS 2.1+ (or alternative technical SCA solutions) must be supported by all Customers as of mid-2020 (1 July 2020).

EMV 3DS 2.2+ is supported

EMV 3DS 2.2 with the Mastercard PSD2 Message Extension (EMV 3DS 2.2+) must be supported for all features in the extension that are not supported in the core EMV 3DS 2.2 specifications (Acquirer exemptions and Trusted Merchant Listing status). The support of EMV 3DS 2.2+ is not mandated before summer 2021.

EMV 3DS 2.2 must be supported if supported for other payment scheme (principle of parity).

Mastercard now supports EMV 3DS 2.2 compliance testing. It is now covered in the Mastercard Identity Check Program Guide now supports v2.2 testing. Please refer to the announcement AN 3773 “Mastercard Identity Check EMV 3DS 2.2.0 Implementation and Test Strategy Update” for latest updates on this topic.

Fallback to 3DS1

SCA can be performed in EMV 3DS only if the Issuer is enrolled in EMV 3DS. If the Issuer has not yet migrated to EMV 3DS, a fall back to 3DS 1.0 can be used by merchants.

Given the multitude of ramp-up plans in the EEA countries, it is likely that issuers not yet enrolled in EMV 3DS are in progress and, in the interim, approve EMV 3DS attempted transactions in authorization. Therefore, Mastercard suggests that merchants decide whether to proceed with attempted EMV 3DS authorizations or fallback to 3DS1 based on the conversion rate. Merchants can check which card ranges are enrolled in EMV 3DS by sending EMV 3DS Preparation Request (PReq) messages, which the Mastercard Directory Server (DS) answers by providing enrolled card ranges in the EMV 3DS Preparation Response (PRes) messages.

How to Achieve PSD2 Compliance with 3DS1

1. Based on EBA's paper published on 21 June 2019, Mastercard understands that 3DS1 can comply with dynamic linking, for example, if the OTP is used as authentication code. For Issuers using SMS OTP we recommend that dynamic linking is ensured during OTP validation. Issuers should decline transactions for which the final amount is higher than the authenticated amount (see point on 'Amount Tolerance' below). Issuers may chargeback if the transaction amount is higher than the value agreed by the cardholder. Note that this does not apply to countries where hard enforcement of the PSD2 SCA regulation has not yet started (e.g. the UK on 14 September 2021).
2. Options for Issuers that need to know if a 3DS1 fully authenticated authorization was frictionless or challenged
    a. Always challenge 3DS1 if amount above Issuer TRA threshold
        1. Achieves PSD2 compliance
        2. Reduces unnecessary step-up (e.g. TRA threshold of €100 means only around 18% must be challenged)
        3. Reset Low Value Counters in fully authenticated 3DS1 authorization
    b. Use Authentication Method byte in SPA1 AAV: value 0=frictionless, other values=challenge (AAV = Accountholder Authentication Value)
        1. Both ACS and authorization processor may have to code to support this; Acquirers and Merchants are not impacted
        2. Mastercard on-behalf AAV validation will still work (only validates MAC in last 5 bytes)
        3. Testing recommended

Important clarification:

While we recommend that post-PSD2 Issuers accept 3DS1 authentications and subsequent authorizations (by ensuring PSD2 compliance e.g. with the best practices provided in this document), some Issuers may decline 3DS1 transactions.

It is therefore crucial that Merchants urgently migrate to EMV 3DS, already required by Mastercard Safety and Security Roadmap. EMV 3DS provides several advantages over 3DS1:

- It is fully PSD2 compliant for all devices and transaction types
- it provides a better user experience
- it outperforms 3DS1 in terms of authentication and authorization performance. Note that 3DS1 will be sunset on 14 October 2022. Please refer to AN 3391 "AN 3391 Mastercard Customer Roadmap to Transition from 3DS 1.0 to EMV 3DS (2.0)" for more information on this topic.

The Appendix-A provides guidance on best options for a successful Identity Check migration.

Rejected Authentications Cannot be Sent to Authorization

The Merchant must not retry with 3DS 1.0 or send the transaction to authorization if an EMV 3DS authentication request fails with Transaction Status "R" (Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and request that authorization not be attempted) or CRes = "N". In case of transaction declined or cancelled by the cardholder, the transaction cannot be sent to authorization. This will avoid that declined or cancelled authentications are billed to cardholders.

Soft Decline Processing – Response Code 65

If Issuers require SCA because authorization was not preceded by an authentication, then the

1. Issuer should decline the authorization with reason code 65/soft decline SCA is required (in DE 39)
2. Merchant should retry with EMV 3DS and Challenge Indicator 04/SCA mandated or 3DS1 if EMV 3DS is not supported by Merchant or Issuer
3. if authentication successful Merchant should send another authorization with 3DS data. It appears that some Merchants do not send another authorization with 3DS Data even if the authentication was successfully performed after receiving a reason code 65.
4. Issuer should not automatically decline this fully authenticated authorization.

If the authentication (e.g. for €70) is followed by an authorization (e.g. €100) with a higher amount, then Issuers should decline with reason code 13/invalid amount, not reason code 65/soft decline when SCA is required. This will inform the Merchant to perform another authentication with the correct amount or split the transaction in 2 (e.g. one for €70 fully authenticated, one for €30 with Acquirer exemption applied and without 3DS, if applicable). Note that this does not apply to countries where hard enforcement of the PSD2 SCA regulation has not yet started (e.g. the UK on 14 September 2021).

Issuers should not apply soft decline for other reasons than when SCA is required, e.g. in case of:

- A "Fully authenticated" (SLI 212) transaction except if one of LVP counters is reached;
- An "Exempted" (SLI 216) transaction;
- An "Attempted" (SLI 211) transaction except if the transaction is high risk.

Soft declines cannot be used for device-based Digital Secure Remote Payment (DSRP) transactions, such as Apple Pay, Google Pay or Samsung Pay. Wallet-based DSRP transactions are fully authenticated using Consumer Device Cardholder Verification Method (CDCVM), with the exception of Merchant-initiated DSRP transactions used for recurring payments. DSRP transactions will not carry a SCA delegation flag in DE48 sub-element 22 sub-field 1. For more information on DSRP transactions, please refer to the "MDES Issuer Implementation Guide".

SCA Requirements during Soft Enforcement

In several countries of the EEA, the support of EMV 3DS and compliance to PSD2 SCA requirements will be ensured by a gradual migration/ramp-up through the usage of soft declines for non-compliant transactions above a certain amount threshold that will decrease over time down to zero.

This is well understood by all stakeholders on the authentication value chain. However, it seems some Merchants have understood that all scenarios that require SCA are subject to the amount thresholds milestones in the soft enforcement migration/ramp-up plans. That is not the case: all COF, MIT or RP agreement set-up or soft decline retry transactions must be SCAed through 3DS regardless of the amount.

Mastercard PSD2 Testing Programs

Mastercard reminds all stakeholders on the authentication value chain that the following Mastercard testing platforms are available free of charge:

Mastercard PSD2 Merchant Testing:

Mastercard offers a PSD2 Merchant Testing platform. The landing page of Mastercard's test ACS partner provides all details on the capabilities and registration requirements:

https://3dss.netcetera.com/mastercard psd2 testing/

Mastercard strongly recommends Merchants that operate a Merchant app to participate and test their app using this platform.

Mastercard PSD2 Issuer Testing:

Mastercard offers a PSD2 Issuer Testing platform. Stakeholders willing to start using this platform should register at: https://validation.wirecard.ro/register.php

During the registration process, if the stakeholder's URL suffix is not recognized, please contact Mastercard at IdentityCheckEurope@mastercard.com to go through the enablement process.

When registered, stakeholders can start using the platform at:

https://validation.wirecard.ro/login.php

Mastercard strongly recommends Issuers to participate and test their app(s) using that platform.

Guidance for Acquirers, Merchants and 3DS Servers

3DS Servers to Correct Information from Merchants

The following are typical errors in EMV 3DS and must be changed by 3DS Server when received from the Merchant according to EMV 3DS specifications, otherwise the Directory Server will reject these with an error:

- E.g. color depth (eg value 30 from Chrome browser must be converted to value 24)
- ISO code value of state code in address fields
- Special characters (eg öüäéèê) in cardholder name(*) are not allowed

Concerning these latter special characters, it is recommended that:

- Merchant gateways or 3DS Servers convert Umlaute or accented characters to standard Latin characters (e.g. ä becomes ae, é and ê become e, etc) for cardholder name(*) before sending these in the EMV 3DS authentication request.
- ACS's do not decline authentication requests only because the cardholder name does not match 100% the one on file, for example due to conversion of special characters (e.g. some 3DS Servers may convert ä to a).

(*) This also applies to merchant names and address fields.

Merchant App Flow Performance

Following an analysis with different Merchants, below are a few recommendations/best practices on how to improve the Merchant app flow performance or success rate, that Issuers and their ACS's can use:

1. Issuers must optimize authentication pages (including responsive design) for mobile devices or other digital/smart consoles (e.g. smart TV);
2. 30%-40% of cardholders who are successfully challenge, then do not press on the "Continue" button on the Merchant app, especially if the challenge is via authentication app; clear messaging of call to action needs to guide cardholders to the right behavior in the flows;
3. Not all fields are present in the CRes from the ACS, causing SDKs to reject or time-out;
4. The ACS rejects the CReq when doing case sensitive editing (charsect=utf-8 is declined, charsect=UTF-8 is accepted);
5. The ACSSignedContent is signed with a wrong/old key. The key should be the most recent Mastercard SDK key. This is causing some problems with the encryption algorithm or with the ACS public key. As a result, the 3DS Server (or Merchant) won't be able to build or send the CREQ

6. ACS's and 3DS Servers should use the correct (decimal) SDKcounter/ ACScounter format/specs by the EMVCo. See the specific section on this at the end of these best practices;
7. Challenge Requests (CReq) are often not sent or rejected by the ACS (e.g. for 3DS Server sending v2.2 CReq for a v2.1 authentication or ACS using wrong SDK encryption key);
8. Challenge Requests (CReq) rejected by the ACS because JSON is used instead of JOSE (Security and Encryption method) method;
9. The Public IP address is not available via SDK (SDK will produce a private IP address), hence the ACS should not try to validate it;
10. ACS's and 3DS Servers have to support UI data element /Challenge info data elements in the CRes (Challenge Response) message. Find below in table A-18 some data elements that may have been omitted and that are key to a successfully performing C-flows. These are guidelines on the mandatory fields for the UI data element /Challenge info data elements in the CRes.

    It seems that ACS's or 3D Servers may not have coded for all EMV 3DS 2.1 specified fields. The source of this issue is that EMVCo has issued bulletins after the initial EMV 3DS 2.1 publication with additional data element definitions and requirements. This concerns the EMVCo February 2020 Bulletin and May 2020 Impact Notice regarding UI Data Elements (Rqmt 387) that were once optional but now mandatory per specification changes. Not all providers may have noticed these bulletins or implemented the additional requirements.

Table A.18: UI Data Elements

Data Element	Field Name	Zone	Portrait Top-down Display Order	Landscape Top-down Display Order	ACS UI Type			
					OTP	Single Select	Multi Select	OOB
Challenge Additional Information Text	challengeAddInfo	3	3	3	N	N	N	O
Challenge Information Header	challengeInfoHeader	3	2	2	M	M	M	M
Challenge Information Label	challengeInfoLabel	3	4	4	M	M	M	O
Challenge Information Text	challengeInfoText	3	3	3	M	M	M	M
Challenge Information Text Indicator	challengeInfoTextIndicator	3	3	3	O	O	O	O
Challenge Selection Information	challengeSelectInfo	3	5	5	N	M	M	N
Expandable Information Label	expandInfoLabel	4	12	12	O	O	O	O
Expandable Information Text	expandInfoText	4	13	13	O	O	O	O
Issuer Image	issuerImage	2	1	1	O	O	O	O
OOB Continuation Label	oobContinueLabel	3	6	6	N	N	N	M
Payment System Image	psImage	2	1	1	O	O	O	O
Resend Information Label	resendInformationLabel	3	8	6	O	N	N	N
Submit Authentication Label	submitAuthenticationLabel	3	7	6	M	M	M	N

11. Some ACS's are blanket rejecting CReq when "A message element required as defined in the 3DS Specifications is missing from the CReq message", while the element is even not present in the CReq specifications:
    - acsOperatorID
    - acsReferenceNumber
    - acsRenderingType
    - acsSignedContent

- Eci
- transStatusReason

ACS Providers are called upon to review their C-flow performance: avoid rejects of data elements that have no relevance nor value to the process.

Missing or Inaccurate Data in Key EMV 3DS fields

Based on the fields marked as high importance by customers, we can see customers are using the following ones as a part of their authentication models:

- Device Info
- Cardholder Account Number
- Browser IP address
- Cardholder Name
- Cardholder Mobile Number
- Billing address (also address match indicator in UK)

It is therefore important that Merchants make sure they send those fields to maximize the chance to get a frictionless authentication and drive higher approval rates.

From experience, many Merchants leave data fields blank, taking away Issuer´s ability to evaluate them for a frictionless authentication. Some other Merchants populate the fields with dummy values or static information, possibly leading to declines due to mismatches.

If conditional or optional fields are not provided, then they should be empty and not space filled (which will be rejected by the Directory Server).

Another important field for risk assessment is the Merchant Category Code (MCC) which should be accurately populated to reflect the Merchant's business. It should ideally be the same as in the authorization.

Address Match Indicator

Some ACS's decline authentication requests when the Address Match Indicator (field name: addrMatch) = "N" (meaning that the billing address differs from the shipping address) as this is a higher risk indicator.

This leads to unnecessary declines as some e-com Merchants set the Address Match Indicator to "N" for digital goods or services that are actually not shipped.

Mastercard recommends to leave the Address Match Indicator blank for digital goods or services that are not subject to shipping to a physical address.

Merchant Name

The Merchant name in authentications must uniquely identify the Merchant in all countries where it operates and for all its activities (for example, Merchant.com) or per its activities (such as, MerchantBooks.com, MerchantMusic.com) or per its countries (such as, Merchant.fr, Merchant.co.uk). Acquirers must ensure that the Merchant name used by the Merchant belongs to the Merchant and is registered for use in the Identity Check Program.

Merchant Enrollment

The announcement AN-1544 published in March 2018 mandated Acquirers to enable their Merchants for EMV 3DS and therefore enroll them into the Identity Solutions Service management (ISSM) tool by 1 April 2019.

Many EMV 3DS authentications are rejected by the Directory Server (error 303) because the Merchant ID and Acquirer BIN combination is not properly enrolled in Identity Check via the ISSM tool.

It is important that Merchants

1. ensure they are enrolled by their Acquirer;
2. provide the correct combination (Acquirer BIN, Merchant ID) to their 3DS Servers or gateways.

3DS Servers can also enroll Merchants into ISSM, including via the API (which does not require Acquirer approval or delegation). 3DS Servers are encouraged to use the API - available on the Mastercard developer zone - to enroll their Merchants when EMV 3DS authentications fail due to enrollment issues. Acquirers will instead be informed electronically and can then disenroll Merchants in case of error.

If a Merchant is acquired by several Acquirers, then all combinations of (Acquirer BIN, Merchant ID) must be enrolled by those Acquirers.

Acquirer Country Code

If the Acquirer is in EEA for Merchants outside EEA, the Acquirer should use EMV 3DS and provide the Acquirer numeric country code in the Mastercard PSD2 Message Extension field 3 (Acquirer Country Code). If the ISO country code is in the EEA, then related transactions are in scope of the PSD2 RTS on SCA.

Acquirer Authorization Processing

Merchants/Acquirers must provide the DS Transaction ID and Program Protocol in authorization and clearing messages. This is very important as otherwise AAV validation will fail which leads to automatic declines by the Issuers.

The Appendix-B provides guidance for European Acquirers on sending DS Transaction ID for EMV 3DS Transactions.

Mastercard's monitoring will report the following KPI:

KPI - Invalid DS Transaction ID

> The Acquirer is sending an authorization transaction with DE48 sub-element 42 (SLI=Security Level Indicator) that indicates an EMV 3DS authentication was performed but without value in DE48 sub-element 66 sub-field 2 (DS Transaction ID).
>
> The root cause of such behavior may be a communication channel between Merchant and Acquirer that is not updated yet to support this value.
>
> Acquirers and Merchants must ensure that they include a correct value in DE48 sub-element 66 sub-field 2 in the authorization message when an EMV 3DS authentication was completed.

The DS Transaction ID must exactly mirror from authentication to authorization. As the EMVCo specifies this field as case sensitive, a lower case letter in the DS Transaction in authentication will not mirror if uppercased in authorization. Also, the usage of a constant dummy value into the DS Transaction ID is not allowed.

As a general measure, the recommendations in the previous paragraph apply to all data shared between authentication and authorization.

When Strong Customer Authentication is not required under PSD2 RTS, or when it is delegated, the Acquirer must provide the reason by populating the appropriate value in DE 48—Additional Data—Private Use, sub-element 22, sub-field 1 in the authorization message: 01=Merchant Initiated Transaction, 02=Acquirer low fraud and Transaction Risk Analysis, 03=Recurring payment, 04=Low value payment, 05=SCA Delegation, 06=Secure Corporate Payment.

As the effective date for the support of DE48 sub-element 22 sub-field1 was 14 September 2020, it is not surprising that most authorizations do not use this field yet.

> It has been brought to the attention of Mastercard that the DE 48 sub-element 22 sub-field 1 is sometimes populated in single tap flows related to card-present contactless transactions. All customers should be reminded that DE 48 sub-element 22 sub-field is only used for card not-present transactions and other sub-fields of DE 48 sub-element 22 should be used for card present transactions.

Mastercard's monitoring will report the following KPI:

KPI - Missing Exemption Indicator

> The Acquirer is sending an authorization transaction with a DE48 sub-element 42 (SLI) that indicates that no authentication was obtained. The authorization is not populated with an exemption or exclusion indicator in DE48 SE22 SF1 which would make this transaction not PSD2 RTS compliant as of 1 January 2021 (in countries where hard enforcement applies).

The root cause of such behavior may be that the Merchant is not (yet) prepared to properly request an exemption/exclusion.

Acquirers and Merchants must ensure that they are prepared to request an exemption or exclusion when no authentication was requested nor obtained. As of 1 January 2021, this is required by the regulation (in countries where hard enforcement applies).

MIT/RP - Invalid POS Cardholder Presence:

The Acquirer is sending an authorization transaction with a DE48 sub-element 22 sub-field 1 (low-risk Merchant indicator) with value "01" (MIT) or "03" (RP) where DE61 sub-element 4 (POS cardholder Presence) does not equal "4" (standing order/recurring transactions).

The root cause of such behavior is an incorrect interpretation or implementation of the specifications.

Acquirers must ensure that they use the correct value "4" for DE61 SE4 in the authorization message when an MIT or Recurring Payment exemption is being requested.

Acquirers must provide the unique Trace ID of the initial recurring payment authorization in DE 48, sub-element 63 (Trace ID) of subsequent recurring payment transaction authorizations to allow the Issuer to validate that SCA occurred on the initial recurring payment authorization, as is required under PSD2 RTS.

Mastercard's monitoring will report the following KPI:

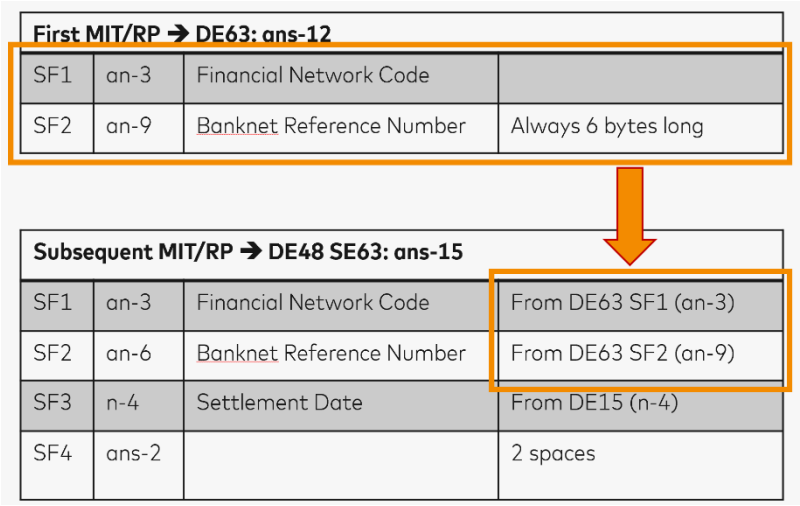
KPI - MIT/RP - Missing Trace ID

The Acquirer is sending an authorization transaction with a DE48 sub-element 22 sub-field 1 (low-risk Merchant indicator) with a value of "01" (MIT) or "03" (RP) where DE61 sub-element 4 (POS Cardholder Presence) does equal "4" but with DE48 sub-element 63 (TraceID) is missing.

The root cause of such behavior is an incorrect interpretation or implementation of the specifications.

Acquirers must ensure that they include a correct value in DE48 SE63 in the authorization message when an MIT or Recurring Payment exemption is being requested.

Note that DE48 SE63 (ans-15) is populated in part by DE63 (Network Data) of the initial/parent MIT/RP as follows:



First MIT/RP ➔ DE63: ans-12			
SF1	an-3	Financial Network Code	
SF2	an-9	Banknet Reference Number	Always 6 bytes long

Subsequent MIT/RP ➔ DE48 SE63: ans-15			
SF1	an-3	Financial Network Code	From DE63 SF1 (an-3)
SF2	an-6	Banknet Reference Number	From DE63 SF2 (an-9)
SF3	n-4	Settlement Date	From DE15 (n-4)
SF4	ans-2		2 spaces

In view of this, the Trace ID of subsequent MITs/RPs has to have a length of at least 13 bytes, so including the settlement date allowing the Issuer to find the parent transaction. DE63 specs may lead to the absence of settlement date in DE48 SE63.

The following best practices come from cases raised by customers since the beginning of 2021 and are worth repeating:

- The parent of a series of MIT/RPs has to be properly flagged and SCAed. It cannot be a TRA or other Acquirer exemption or exclusion for example.
- The parent had to go through authentication using 3DS. The parent cannot be a 0€ authorization (reported case) without authentication (this latter may have been Issuer LVP exempted).
- The Trace ID in subsequent MIT/RPs:
    - Can be a dummy value if grandfathering applies (before 14 September 2020);
    - Has to have a length of at least 13 bytes;
    - Has to link to a valid parent transaction;
    - Has to link to a parent that has been SCAed.

A Trace ID for MIT/RP can be combined with a Trace ID for pre-authorization because both will be referring to the same initial/parent transaction. It is however not possible to have a "grandfathered" dummy value in the Trace ID for a subsequent pre-authorization: whereas the value can be accepted for MIT/RP, it is not possible to accept it for pre-authorization. These latter transactions will be declined with response code RC=77.

Mitigating non-3DS Declines

To limit the impact of Issuers not accepting non-3DS authorizations with Acquirer exemption flag, Merchants/Acquirers that plan to skip 3DS when applying an Acquirer exemption are advised to

- identify Issuers that systematically decline such authorizations and
- always send 3DS for such Issuer card ranges.

Guidance for Issuers and ACS's

Challenge Indicator

The Challenge Indicator (field name: *threeDSRequestorChallengeInd*) can hold one of the following values:

- 01 = No preference
- 02 = No challenge requested
- 03 = Challenge requested: 3DS Requestor Preference
- 04 = Challenge requested: Mandate
- 05–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo)
- 80-99 = Reserved for DS use

An ACS must properly process the Challenge Indicator to identity the best course of action. Issuers should agree with their ACS on the best course of action and possibly review the ACS rules.

For example:

- If the Challenge Indicator has a value of "4", the transaction must be systematically challenged.
- Except for values "3" and "4", the ACS should avoid useless or unnecessary step-ups.
- If Challenge Indicator = 05/Acquirer exemption or 07/SCA delegation (in v2.1 these values are not supported and instead the message extension field *scaExemption* allows values 05/Acquirer exemption or 07/SCA delegation to be used), then the ACS should not step-up more than 5% of such authentication requests and respond with ECI 06 to avoid liability shift (in v2.1 Ares=N with reason code 81; in v2.2 Ares=I).

Merchants should send an authorization request following Ares=N with reason code 81, as this is a correct response in v2.1 to an Acquirer exemption or SCA Delegation.

AAV Leading Indicators

Authorization front-end processors must identify the conditions under which e-commerce transactions (especially the authentication price) have been conducted to act upon them and eventually approve or decline these transactions.

The authentication data received in the authorization message must be properly processed to drive higher approval rates. For example, it is expected that the approval rate related to transactions that are successfully challenged with 2-factor authentication as per PSD2 (leading indicator "kB" of the AAV) has to be higher than the one related to frictionless (leading indicator "kA" of the AAV) transactions. This is because transactions where the cardholder was strongly authenticated with 2 factors have a lower fraud risk than frictionless authenticated transactions.

For the sake of clarity and full transparency, the Appendix-C summarizes the latest information available on the AAV leading indicators. Authorization front-end processors should amend their systems to fine-tune their authorization decisioning processes.

On-behalf AAV Validation (OBS5) Results

The Issuer host system has to properly process the OBS5 result codes. Result codes that should be accepted are “A” and “V” during hard enforcement of the PSD2 SCA regulation. During soft enforcement, some flexibility should allow Issuer host systems to approve “B”, C”, “D”, “S” and “T” result codes after proper risk analysis.

Code	Description	SPA2 AAV	DS Transaction ID	Amount check
A	AAV & Amount Checked	Found associated with PAN	Not Present in Authorization	< or = authentication amt
B	Balance to Verify	Found associated with PAN	Not Present in Authorization	0%-19.99% of authentication amt
C	Consider the Amount	Found associated with PAN	Not Present in Authorization	20% or > of authentication amt
D	DS Transaction ID Failed	Found associated with PAN	Different from authorization	N/A
I	Invalid AAV	Not Found associated with PAN	N/A	N/A
K	Key Not on File			
M	Currency Mismatch	Found associated with PAN	N/A	Authorization currency <> authentication currency
S	DS Transaction ID Present-Balance to Verify	Found associated with PAN	Found associated with PAN & AAV	0% -19.99% of authentication amt
T	DS Transaction ID Present – Consider the Amount	Found associated with PAN	Found associated with PAN & AAV	20% or > of authentication amt
U	Service Unavailable			
V	DS Transaction ID Present – AAV and Amount Checked	Found associated with PAN	Found associated with PAN & AAV	< or = authentication amt
X	Security Platform Timeout			
Z	Security Platform Processing Error			

Mastercard’s monitoring will report the following KPIs:

KPI - Invalid AAV

Acquirer is sending an authorization transaction with a DE48 SE42 (SLI) that indicates the presence of an AAV where the OBS 05 service finds that this AAV does not match the AAV value that was sent in the authentication response to the Merchant through EMV 3DS. The OBS 05 service will indicate this finding through value “05I” in the authorization to the Issuer.

The result code is taken in account by the Issuer during authorization decisioning and may result in a decline.

The root cause of such behavior can be many:

- Acquirer includes incorrect AAV
- Acquirer damages the AAV value (very common is last two digits being overridden). AAV conversions should be avoided; if needing to convert from hexadecimal, 21 bytes of length (and not 20 as already monitored) must be ensured for SPA2 AAVs starting with “k”.

Merchants and Acquirers must ensure that they use the correct AAV field value from the authentication to insert into the authorization message.

KPI - Mismatching Amount

An Acquirer is sending an authorization transaction with a DE48 sub-element 42 (SLI) where the OBS 05 service finds that the amount of the transaction is higher than the amount that was sent through EMV 3DS. The result code is taken in consideration by the Issuer during authorization decisioning and may result in a decline.

The root cause of such behavior can be many:

- Acquirer includes incorrect amount
- Acquirer or Merchant performed an incorrect value conversion
- Merchant authenticated for a higher amount than what is being presented for authorization

Within EEA (excluding the UK), Merchants and Acquirers must ensure that they do not request authorization for an amount that exceeds the authorization amount.

Amount tolerance

The EBA set out the following principles for transactions for which the final amount is unknown:

1. The final transaction amount cannot be higher than the authenticated amount. According to the EBA, "if the final amount is higher than the amount the end consumer was made aware of and agreed to when initiating the transaction, the Merchant shall apply SCA to the final amount of the transaction or decline the transaction".
2. The final transaction amount may be lower than the authenticated amount. According to the EBA, "[i]f the final amount is equal to or lower than the amount agreed in accordance with Article 75(1) of PSD2, the transaction can be executed and there is no need to re-apply SCA, as the authentication code would still be valid in accordance with Article 5(3)(a) of the [RTS]".

There are three options when the authorization amount is higher than the authentication amount. These are compliant with the PSD2:

1. Use of Merchant Initiated Transaction (MIT) for the payment amount (MIT is excluded from PSD2 but requires SCA when setting up with cardholder, liability with Merchant);
2. A: Regular payment for expected amount (SCA required for expected amount with liability with Issuer unless Acquirer exemption applies), if needed followed by

   B: 2nd payment for incremental amount (no SCA either with exemption or MIT, if applicable, and liability with Merchant if Acquirer exemption or MIT applies)

3. Regular SCA for expected amount plus margin similar to pre-authorization value being used at hotel check in (Cardholder could be informed that SCA does not block the total amount)

The 20% tolerance will be kept in the Mastercard documentation for the UK and zero amount tolerance (authorization amounts can always be lower than authentication amounts) will be applicable to all EEA countries.

Guidance on Mixed Features for ACS's, 3DS Servers and SDKs

ISO Codes

When an ISO code is used in EMV 3DS authentication messages to identify a country or currency, the ISO 3166-1 and ISO 4217 standards have to be used. If a country code or currency code does not use values mentioned in these standards or appear on the list of excluded code values in Table A.5 of the EMV 3DS 2.1 specifications (Table A.5: Excluded Currency Code and Country Code Values), then an error code 304 will be returned.

Country codes in EMV 3DS specifications that are using the ISO 3166-1 standard:

EMV 3DS Data Element	EMV 3DS Field Name
Cardholder Billing Address Country	*billAddrCountry*
Cardholder Shipping Address Country	*shipAddrCountry*
Merchant Country Code	*merchantCountryCode*

Currency codes in EMV 3DS specifications that are using the ISO 4217 standard:

EMV 3DS Data Element	EMV 3DS Field Name
Purchase Currency	*purchaseCurrency*

When referring to state information, the ISO 3166-2 standard applies. There is a number of countries where the official concept of "state" does not apply. Hard edits on state fields (*shipAddrState* or *billAddrState*) should be removed whenever they are not applicable in certain countries. 3DS Servers and Acquirers must convert special characters and validate (possibly with softened validation rules) state information at time of entry.

Method URL

The 3DS Method is a scripting call placed on the website on which the Cardholder is interacting, such as a Merchant checkout page in a payment transaction. The purpose of the 3DS Method is for an ACS to gather additional browser information prior to the receipt of the AReq message to help facilitate risk-based decisioning. The use of the 3DS Method by an ACS is optional.

The 3DS Method URL is the ACS URL that will be used by the 3DS Method. It is optional but if supported by the ACS, it is indicated in the Card Range Data sent in the PRes message data for the card range associated with the Cardholder Account Number.

The 3DS Method Completion Indicator indicates whether the 3DS Method successfully completed: Y (yes), N (no), U (3DS Method URL was not present in the PRes message data for the card range associated with the Cardholder Account Number).

The support of the 3DS Method URL is a mandate for 3DS Servers.

ACSCounter and SDKCounters

ACSCounter and SDKCounter:

- Should be octet/decimal and not octal. EMVCo specs mention “Oct” that could be interpreted by ACS’s or SDK’s as octal. In this case, the counter would be reset after “007” and not after “256”.
- When some Merchants detect the counter being out of sync, they send an Erro message to the SDK as per EMVCo specs. The problem is that some SDK’s then increase the Counter again based on the Erro message.

  In short, it should be clarified that Erro messages should not increase the SDK/ACS Counters (only CReq/Cres should).

  But if EMVCo clarifies anyway that SDK/ACS Counters should use octet/decimal (not octal) then it may help to clarify or remind for the avoidance of doubt that these Erro messages should not increase these counters.

ACSSignedContent and sdkEphemPubKey

When building the ACSSignedContent, an ACS must use the correct value of the sdkEphemPubKey. An incorrect value of the key may lead to transaction failure at the SDK side.

The conclusion of this is:

- (SDK side) Some SDKs do not check the value of the sdkEphemPubKey in the returned ACSSignedContent. It does not necessarily create an issue in the field since the SDK knows the correct value for sdkEphemPubKey, as generated by the SDK itself.
- (ACS side) The sdkEphemPubKey returned in the ACSSignedContent must be the correct key, as SDKs may check the key value when provided. The ACS Test Plan should check that the sdkEphemPubKey returned in the ACSSignedContent matches the one sent in AReq.

Displaying Info Texts

When ACSs decline authentication requests or challenge fails, they should provide, and the Merchant should display, potential error messages / cardholder communication:

- Cardholder Info in AReq
- Challenge Info Text in Cres

This will allow cardholder to act (e.g. enroll, unblock card etc by contacting Issuer) and retry authentication.

APPENDIX-A: Successful Identity Check Migration

Guidance for European Acquirers on Sending DS Transaction ID for EMV 3DS Transactions

Why is it critical to send the Directory Server Transaction ID (DS Transaction ID)

Acquirers not sending the DS Transaction ID correctly will :

(1) **Negatively impact authorization approval rates**

(2) Result in **financial penalties under Mastercard's Data Integrity Monitoring Program** (see Announcement 2401 for more details)

(3) **Prevent the unique mapping between authentication and authorization** messages required to meet the PSD2 SCA dynamic linking requirements.

Merchants/Acquirers must send the DS Transaction ID in authorization. The DS Transaction ID field cannot be populated with dummy values or upper-case characters.

Guidance for Sending Data Element 48, Subelement 66 (DE 48 SE 66)

(1) **DE 48 SE 66 Subfield 1 (SF 1) = Program Protocol**

- Acquirers must send Program Protocol (DE 48 SE 66 SF 1) on both Secure Code (3DS1.0) & EMV 3DS (3DS2.0) transactions

(2) **DE 48 SE 66 Subfield 2 (SF 2) = DS Transaction ID**

- Acquirers must send the DS Transaction ID (DE 48 SE 66 SF 2) in Authorization for all 3DS2.0 transactions
- DS Transaction ID is not present on 3DS1.0 transactions so acquirers should omit this value

Example of correct string for DE 48 SE 66:
66450101202 36ffffa2b1-6afb-4d82-817e-a079e922cb92

Breakdown:
66 45 01 01 2 02 36 ffffa2b1-6afb-4d82-817e-a079e922cb92

Value	66	45	01	01	2	02	36	ffffa2b1-6afb-4d82-817e-a079e922cb92
Definition	Data Element	Field Length	Subfield 1	Subfield Length	Program Protocol	Subfield 2	Subfield Length	Directory Server Transaction ID

For more information on Identity Check, contact your Mastercard representative or IdentityCheckEurope@mastercard.com

APPENDIX-B: DS Transaction ID

Mastercard Identity Check Migration

Why should merchants migrate from SecureCode (3DS1.0) to EMV 3DS now?
Mastercard has announced a sunset date for 3DS1 of Oct 2022, and will be taking several actions as part of the phasing out process. In accordance with this upcoming deadline, Mastercard recommends merchants migrate to the new protocol EMV 3DS (3DS2.0) for the following reasons:

- EMV 3DS transaction performance is better than 3DS1 in terms of authentication and authorization approval rates. EMV 3DS performance will continue to improve as Issuers retrain their fraud models with the richer data provided by EMV 3DS and optimize their usage of Mastercard intelligence solutions (Smart Authentication and Digital Transaction Insights).
- Liability shift for 3DS1 Attempts will end as of October 2021.
- As of 1 January 2021, 3DS1 will be more expensive than EMV 3DS - 3DS1 transactions fee will double and new monthly 3DS1 only fees will go into effect (see AN3821).
- EMV 3DS will be the primary protocol utilized to comply with PSD2 SCA requirements and will enable issuers to support exemptions allowed under the new regulation.
- While 3DS1 is limited to browser flows, EMV 3DS supports both in-app and mobile payment transactions.

Where is the market in terms of readiness?
We expect the share of EMV 3DS to reach 90% and 3DS1 to fall to 10% by September 2021.

What are the potential benefits of the new EMV 3DS standards for the ecosystem ?

Benefits of new EMV 3DS standards		
Supports two-factor authentication for greater security and convenience	Supports new payment needs such as in-app and mobile payments for a better UX	Supports additional use cases such as Card on File, wallets, tokenization, etc.

Merchants/ Wallets

- Helps drive revenue by **reducing cart abandonment** and **increased approval rates**
- Helps merchants gain category share through a **more seamless checkout experience**
- Facilitates exchange of 10X more data for enhanced decisioning and reduced fraud

Cardholders

- **Eliminates the frustration** of managing and remembering passwords
- **Minimizes unnecessary friction**
- **Offers greater choice** in authentication methods

[1]

How can Issuers confirm in authorisation if a 3DS1 transaction was fully authenticated via a frictionless or challenge flow?

Mastercard recommends two options for Issuers:

1. Always challenge a 3DS1 transaction if the amount is above the Issuer TRA threshold as this will:
    - Achieve PSD2 compliance
    - Reduce unnecessary friction due to step up – e.g. TRA threshold of €100 means only around 18% must be challenged
    - Reset Low Value Counters for fully authenticated 3DS1 authorization only if amount above TRA threshold

2. Use the authentication method byte in SPA1 AAV (value 0=frictionless, other values=challenge)
    - Both ACS and authorization processor may have to code to support this, while acquirers and merchants will not be impacted
    - Mastercard on-behalf AAV validation will still work (only validates MAC in last 5 bytes

    Please note testing is recommended for this option.

4	Authentication Method	Indicates how the cardholder was authenticated to the ACS: 0 = No Cardholder Authentication Performed (This is only valid for an AAV created using control byte value x'86' – Attempts processing.) 1 = Password 2 = Secret Key (e.g. Chip Card) 3 = PKI (pending further discussions) **MasterCard reserves the right to add additional values to this field at any time.** For additional information, refer to section 2.2 - SPA AAV Control Byte and Authentication Method Initialization	½ (4 bits)	Byte 11, 1st hex digit

Please find more details in "SPA Algorithm for the MasterCard Implementation of 3-D Secure" (dated 27 May 2004)

SecureCode (3DS1) and Dynamic Linking

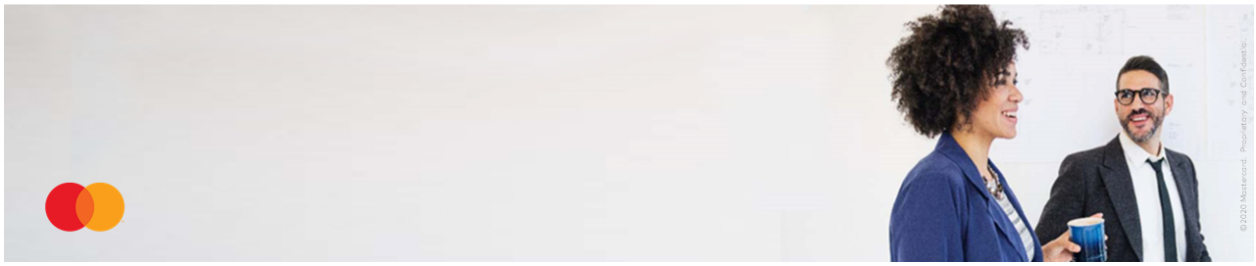
Is 3DS1 compliant with PSD2?
Mastercard understands that 3DS1 is compliant with PSD2 and dynamic linking. For example, if the OTP is used as the authentication code, the OTP validation can ensure dynamic linking. Given that many Issuers use SMS OTP, we recommend that dynamic linking is enabled during OTP validation.

For EEA Issuers that will follow the EBA's Q&A 5133 guidance (no higher amount permitted), how will Issuers prevent a transaction authorization amount from going above authentication amount?
To comply with PSD2's dynamic linking, issuers will not be able to utilize Mastercard's AAV validation service (OBS 5) for 3DS1 as the service does not validate the amount for 3DS1 (OBS5 validates for 3DS1 only that the issuer/ACS or Mastercard generated the AAV via cryptography; OBS5 also validates the amount for EMV 3DS that uses the SPA2 algorithm).

Does 3DS1 support Dynamic Linking?
Unfortunately, Mastercard does not offer a solution for dynamic linking and 3DS1.
The Mastercard on-behalf AAV validation service compares the PAN, the amount, the DS Transaction ID and the SPA2 AAV in authentication and authorization (please refer to Authentication Guide v1.3, page 82 for more details). However, this is not available for 3DS1, which uses SPA1. Please note that our AAV validation does cover 3DS1 transactions, but without amount validation.

It is important to note that for all 3DS1 transactions, Issuers can initiate a chargeback request if the transaction amount is higher than what the cardholder agreed to during authentication.

For more information on Identity Check, contact your Mastercard representative or IdentityCheckEurope@mastercard.com



APPENDIX-C: AAV Leading Indicators

Scenario	Txn Stat.	SPA2 ind. with SHA:		ECI	SLI	Liability
		256	1			
Transaction successfully authenticated by ACS - **Frictionless**	Y	kA	kG	2	212	Issuer
Transaction successfully authenticated by ACS - **Challenge**	Y	kB	kH	2	212	Issuer
Transaction successfully authenticated by Mastercard Smart Authentication **Stand-In - Frictionless (low risk)**	Y	kC	kJ	2	212	Issuer
Transaction successfully authenticated by Mastercard Smart Authentication **Stand-In - Frictionless (non-low risk)**	A	kE	kL	1	211	Issuer
Transaction could not be authenticated by either the ACS or Mastercard Mastercard Smart Authentication **Stand-In - Attempts**	A	kE kF	kL	1	211	Issuer
Transaction was not authenticated by either ACS or Mastercard as **Acquirer SCA Exemption** was applied	I***	kN	N/A	6	216	Merchant
Recurring transaction successfully authenticated by ACS - **Frictionless**	Y	kO	N/A	7	217	Issuer
Recurring transaction successfully authenticated by ACS - **Challenge**	Y	kP	N/A	7	217	Issuer
Recurring transaction successfully authenticated by Mastercard Smart Authentication **Stand-In - Frictionless (low risk)**	Y	kC	kJ	2	212	Issuer
Recurring transaction successfully authenticated by Mastercard Smart Authentication **Stand-In - Frictionless (non-low risk)**	A	kE	kL	1	211	Issuer
Recurring transaction could not be authenticated by either the ACS or Mastercard Mastercard Smart Authentication **Stand-In - Attempts**	A	kE kF	kL	1	211	Issuer
Data Only transaction (Message category 80). No Authentication performed by either the ACS or Mastercard Mastercard Smart Authentication	U, RC=80	No AAV		4	214	Merchant
AAV Refresh transaction successfully authenticated by ACS	Y	kQ		2	212	Issuer
Transaction could **not** be **authenticated**. Attempts doesn't apply	N	No AAV		0	210	Merchant
Transaction **rejected** by Issuer. Authorization should not be attempted	R	No AAV		0	N/A	N/A
*** Txn Status = I is only supported with version 2.2 of EMV 3DS. For version 2.1 "Txn Status = N" with "Txn Status Reason = 81"						