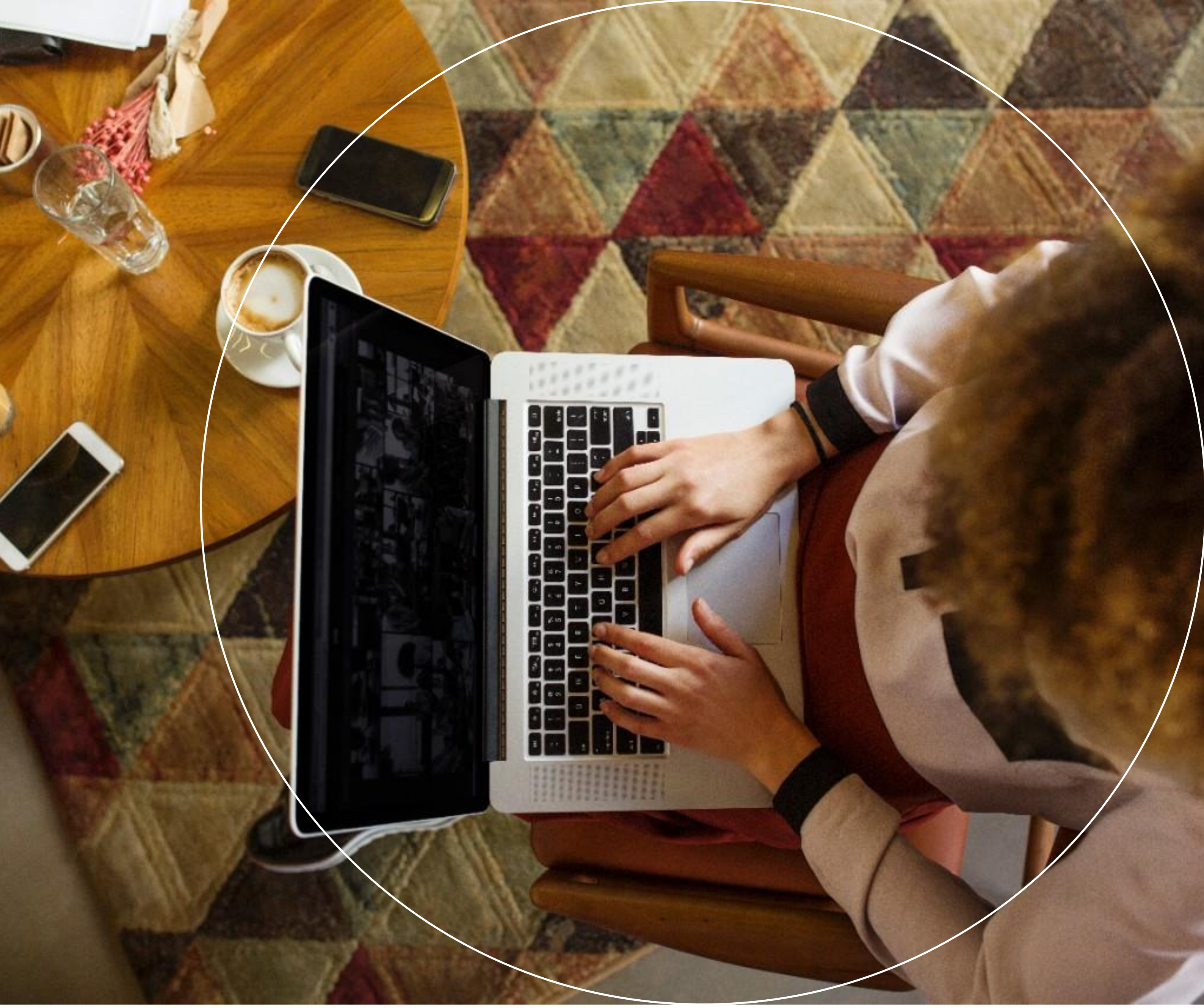

Mastercard® Authentication Best Practices

V1.5

October 2020

This Best Practice guide has been prepared to provide clarification relating to the latest developments on the Mastercard authentication network and provides direction relating to; correct flagging, avoiding unnecessary declines and step-ups, and optimizing the end consumer experience.

Contents

3DS Servers to correct info 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)
- Special characters (eg öüäéèê) in cardholder name are not allowed

Concerning these latter special characters, it is recommended that:

1. Merchant gateways or 3DS Servers convert Umlaute to standard Latin characters (e.g. ä becomes ae, é and ê become e, etc) for cardholder names before sending these in the EMV 3DS authentication request.
2. 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).

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 value agreed by the cardholder.

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

        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

Correct 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.

When Strong Customer Authentication by the Issuer is not required under PSD2 RTS, or when it has been delegated, the Acquirer must provide the reason by populating the appropriate value in DE 48—Additional Data—Private Use, sub-element 22, subfield 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 DE48.22.1 is 14 September 2020, it is not surprising that most authorizations do not use this field yet.

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.

Issuers must not decline authorizations only because the Merchant name does not match in authentication and authorization, provided issuers can ensure that merchant identity remains the same.

According to a recent survey conducted in September 2020, 30% of EEA (excluding UK) issuers will not accept non-3DS authorizations (with acquirer exemption flag) in the beginning of 2021. Merchants/acquirers that plan to skip 3DS when applying an acquirer exemption are therefore advised to

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

Soft decline processing

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
4. issuer should not automatically decline this fully authenticated authorization.

If merchant cannot handle soft decline and retry with an authentication request, then each transaction should be authenticated (especially those with low value payment acquirer exemption which must be challenged if counters are exceeded as per PSD2).

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 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).

Issuers should not apply soft decline for other reasons than when SCA is required. For example, if the amount in authorization is greater than the authenticated amount, then the response code to be used is 13 (Invalid Amount) and not 65.

Processing leading indicators for improved authorization approval rates

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-A 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.

OBS5

The issuer host system has to properly process the OBS5 result codes. Result codes that should be accepted are “A” and “V”:

Code	Description	SPA2 AAV	DS Transaction ID	Amount check (Authorization: Authentication)
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 Found associated with PAN	Not Present in Authorization	20% or > of authentication amt
D	DS Transaction ID Failed	Found associated with PAN		N/A
I	Invalid AAV	Not Found associated with PAN		N/A
K	Key Not on File			
S	DS Transaction ID Present-Balance to Verify	Found associated with PAN	Found associated with PAN & AAV	0% -19.99% of authentication amt
T	Transaction ID Present – Consider the Amount	Found associated with PAN	Found associated with PAN & AAV	20% or > of authentication amt
U	Service Unavailable			
V	Valid – All Data Passes	Found associated with PAN	Found associated with PAN & AAV	< or = authentication amt
X	Security Platform Timeout			

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 payer was made aware of and agreed to when initiating the transaction, the payer’s PSP 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 preauthorization 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.

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

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 Identity Solutions Services Manager (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 in ISSM, including via the API (which does not require acquirer delegation).

If a merchant is acquired by several acquirers, then all combinations of (Acquirer BIN, Merchant ID) have to be enrolled by those acquirers.

To avoid the rejection of merchant IDs, it is recommended that the acquirerMerchantID is filled without leading zeros in authentication messages and in ISSM.

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, whitelisting status, secure corporate payment, SCA delegation). EMV 3DS 2.1+ (or alternative technical SCA solutions) must be supported by all Customers by mid-2020 (1 July 2020).

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 whitelisting 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).

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.

Missing or inaccurate Data in key EMV 3DS fields

Based on the fields of 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 obvious gibberish 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.

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.

Fallback to 3DS1

Merchants can only use EMV 3DS 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 (or to an alternative technical SCA solution) is required. 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.

3DS1 should not be retried in case of non-authenticated or rejected authentications (see next point).

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.

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 PSPs.

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.

Using error messages with EMV 3DS

When issuer declines authentication request or challenge fails, issuer/ACS should provide, and 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

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

*Mastercard will support a new leading indicator for Attempts starting Q3-2020

** Mastercard will support this new leading indicator starting Q3-2020

*** 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"