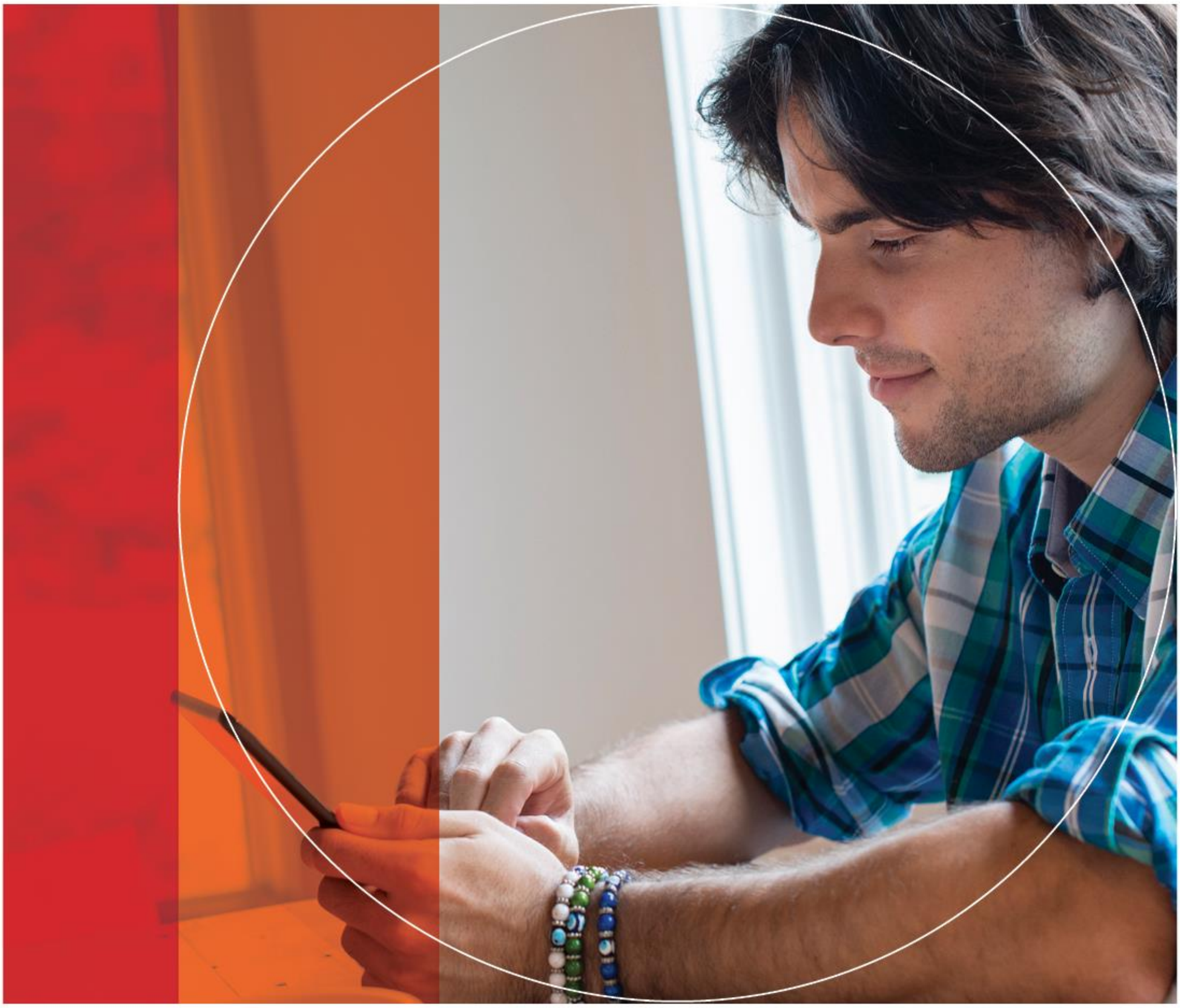


Authentication Guide for Europe

V1.1

mastercard

Table of Contents

Section 1 – Naming convention

In this document, the following naming convention will be used to refer to flags/indicators in authentication, authorization and clearing messages.

Authentication
All authentication fields will be highlighted in italic and underlined.

Authorization (fields starting with "DE")

Reference	Data element	Data element- Full name
Transaction Amount	DE04	Transaction Amount
POS Entry Mode	DE22	POS Entry Mode
DE32	DE32	Acquiring Institution ID Code
RC	DE39	Response Code
Merchant name	DE43	Card Acceptor Name and Location
SLI	DE48 SE 42 SF1	DE48 (Additional Data – Private Use), sub-element 42 (Electronic Commerce Indicators), sub-field 1 (Electronic Commerce Security Level Indicator and UCAF Collection Indicator)
AAV	DE48 SE43	DE 48 (Additional Data), sub-element 43 (UCAF)
Trace ID	DE48 SE63	DE 48 (Additional Data), sub-element 63 (Trace ID)
Program Protocol	DE48 SE66 SF1	DE 48 (Additional Data), sub-element 66 (Authentication Data), sub-field 1 (Program Protocol)
DS Transaction ID	DE48 SE66 SF2	DE 48 (Additional Data), sub-element 66 (Authentication Data), sub-field 2 (Directory Server Transaction ID)
	DE61 SF4	DE 61 (POS Data), sub-field 4 (POS Cardholder Presence).
	DE63 SF1	DE 63 (Network Data), sub-field 1 (Financial Network Code)

Clearing (fields starting with “PDS”)

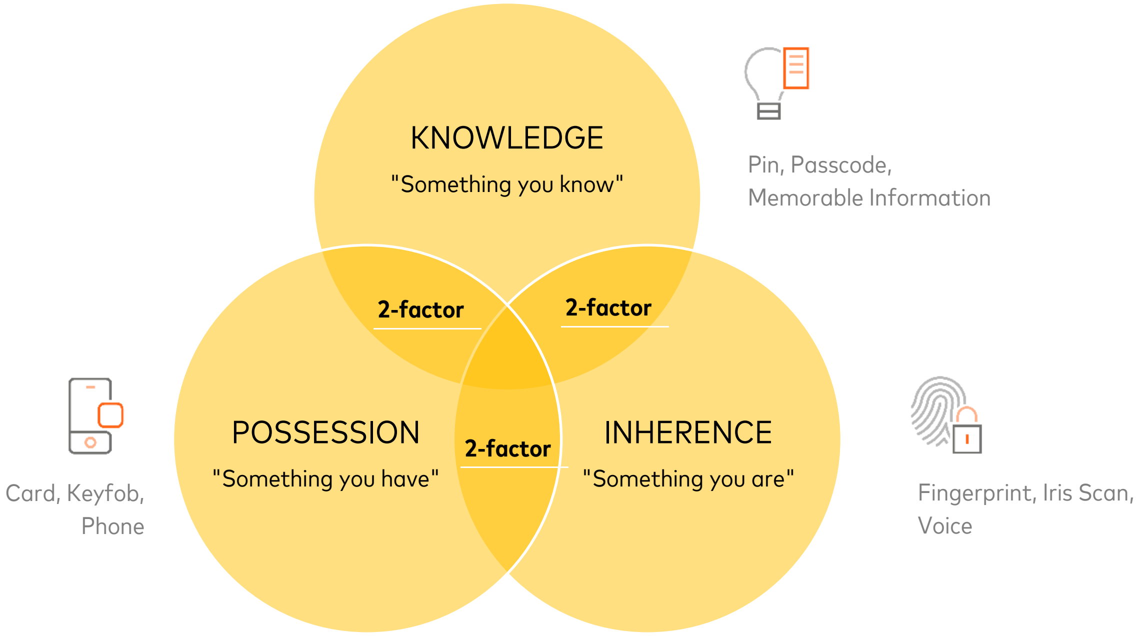
Reference	Data element	Data element – Full name
SLI	PDS0052	Electronic Commerce Security Level Indicator
DS Transaction ID	PDS0184	Directory Server Transaction ID
Program Protocol	PDS0186	Program Protocol

Section 2 - General authentication requirement

2.1 Strong Customer Authentication (SCA)

Strong Customer Authentication (SCA) can be performed using two-factor authentication, i.e. two of the following three factors have to be systematically used during the authentication experience:

- Knowledge – something only the Cardholder knows: password, PIN
- Possession – something only the Cardholder has: mobile phone
- Inherence – something the Cardholder is: finger, face, voice, behavioral biometrics



Mastercard has developed the Mastercard Identity Check ™ Program to support stronger authentication methods and ban at the same time methods that **alone** (i.e. not combined with other methods such as SMS OTP) have proved to be too weak: static passwords, security questions, Knowledge-Based Authentication or KBA.

> Refer to the following document for more information on banned authentication methods as well as recommended authentication methods (e.g. biometry, Risk-Based Authentication/RBA): ***Mastercard Identity Check ™ Program Guide (20 November 2018)***

Mastercard strongly recommends that Issuers roll-out authentication or mobile banking apps with biometrics by April 2019 unless other specific dates have been defined for their country (refer to Appendix-A for the list of those countries) to meet the Mastercard biometric mandate.

Most common SCA mechanisms in the Europe region and as per research include:

- **Biometry** (fingerprint, facial recognition) on consumer devices (e.g. mobile phones), and sometimes PIN on consumer devices.
- **One-time password** (OTP) sent via SMS. This authentication method is considered as a valid solution as per the Mastercard Identity Check™ Program Guide.
  SMS OTP is a one-factor (possession of the SIM card) and combined with a knowledge factor or inherence factor (e.g. a security question or PIN code or behavioral biometrics) qualifies as SCA meeting PSD2 requirements in some markets. In some other markets (e.g. United Kingdom), SMS OTP with card data meets the requirements of the local competent authorities.
  SMS OTP is defined as an acceptable alternative to biometry in the Mastercard Identity Check™ Program.
  If and when needed by local competent authorities, the following options can be used to add a second factor to SMS OTP solutions (which use possession as the first factor, i.e. the OTP confirms that the Cardholder is in possession of the SIM card to which the SMS was sent):
  1. Behavioral biometrics[1] provided that these comply with PSD2 RTS, specifically the requirement that the probability is low that a non-authorized user is authenticated; behavioral biometrics are explicitly allowed as an authentication factor in the PSD2 RTS and the EBA Opinion.

     Mastercard also believes that an authentication solution based on card data, OTP and EMV 3DS behavior-based information complies with PSD2.

  2. Although concerns may be raised on transaction speed and consumer experience, Security questions, e.g. from a list of multiple questions; it is recommended that banks re-use existing security questions and answers used for other services (e.g. call center authentications) when available or information they already have which only the Cardholder knows.
  3. PIN code, but this is the least recommended option as static passcodes are likely to be forgotten. An electronic PIN (ePIN) related to remote electronic/e-commerce transactions should be used and not the real card PIN.

Strong customer authentication should be designed to offer an ideal consumer experience while optimally securing payments.

[1] Behavioral biometrics: field related to the measure of patterns in a human behavior or activities that allow to uniquely identify that human. It includes keystroke dynamics, mouse dynamics and signature analysis

2.2 Authentication versus authorization amount policy

Where possible, the authentication amount should be equal to the authorization amount. This may require whenever possible to delay the authentication until the final transaction amount is known.

To reduce fraud and to comply with PSD2 RTS' Dynamic Linking requirements (refer to section on "Dynamic Linking Requirements"), Merchants are recommended to authenticate for an amount equal or greater than the total transaction amount.

Mastercard recommendation:

The total Transaction amount of all authorizations that relate to an intra-EEA Remote Electronic Transaction should not exceed the authentication amount for the Transaction. If the transaction amount is not known in advance, the authentication amount must be an amount that the Cardholder would reasonably expect, i.e. within an acceptable tolerance (recommended 20% tolerance in Europe). In this case, if the authorization amount exceeds the authenticated amount, it is recommended that Merchants treat the incremental amount compared to the authenticated amount as a separate transaction. For transactions subject to PSD2 RTS these may require a separate strong customer authentication unless an exemption applies or unless they are handled as Merchant Initiated Transactions (MIT). If the transaction amount exceeds the Cardholder's 'reasonable expectations', the refund right for authorized transactions under Articles 76-77 PSD2 may apply.

> Refer to sections on "Acquirer Exemptions", "Merchant-Initiated Transactions (MIT)" and "Recurring Payments".

This recommendation applies to one-off payment transactions, not for adding a card to card-on-file or for initiating recurring payments.

As a single authentication may result in multiple authorizations (e.g. travel bookings combining for example hotel and flight, market place purchases where items are ordered from multiple Merchants), Issuers must ensure that the total (possibly accumulated) transaction amount, i.e. the sum of the individual authorizations, does not exceed the authenticated amount. Also in this case, if the transaction amount is not known in advance, the authentication amount must be an amount that the Cardholder would reasonably expect (recommended 20% tolerance in Europe).

As delays may be experienced between the authentication and the final authorization, the authentication code (called Accountholder Authentication Value or AAV) has to remain valid till the final authorization.

2.3 Accountholder Authentication Value (AAV) validity and extension

In the current Mastercard rules, there is no limit on the validity of an AAV. It should be valid for at least 90 days. Some Issuers may be able to validate an AAV older than 90 days, which is why a Merchant could try to use an AAV for more than 90 days. If an authorization with a potentially expired AAV (i.e. more than 90 days old) is declined, the Merchant could re-send the authorization without the AAV and UCAF data but the merchant becomes liable in case of fraud (lost of liability shift).

Mastercard is looking to set the AAV validity period to 90 days in 2020. An extension to the AAV validity period can be requested as follows:

- Renew the AAV by using the 3RI-PA mechanism available with EMV 3DS 2.2.
- When one-authorization-multiple-clearing model is used, the Merchant can extend the authorization and refer to the original authorization using the Trace ID of this latter.

Note: for recurring transactions/MITs, the AAV check is not performed for subsequent transactions. Refer to section on "Recurring Payments".

In case of the agent model (see section "Agent Model") where a single authentication is linked to multiple authorizations, the same authentication code/AAV as per PSD2 RTS could be used for multiple transactions.

2.4. Issuer Authentication Value (IAV)

The IAV is pertinent to Issuers who perform themselves the validation of the authentication code (self-validation). It is included in the AAV of the authorization message that is generated using the Secure Payment Application (SPA) number 2 (SPA2).

Mastercard only validates the Mastercard portion of the SPA2 AAV (or any AAV) only when the Issuer enrols the card range for the OBS 05 service through their regional CIS team for the OBS service in MPS. Mastercard will not validate the IAV part of the SPA2 AAV. SPA1 key share is currently required. Once enrolled, all transactions with AAVs are validated.

> Refer to the following document for more information on this topic: ***SPA2 AAV for the Mastercard Identity Check Program***

2.5 DS Transaction ID

The Directory Server (DS) Transaction ID will be the universal transaction identifier used to map authentications to authorizations. This is a mandatory element in EMV 3DS specifications, Mastercard authorization's Customer Interface Specifications (CIS) and Mastercard clearing's Integrated Product Messages (IPM) specifications as from 6 November 2018:

EMV 3DS	dsTransID
CIS	DE48 SE66 SF2
IPM	PDS0184

As this identifier will allow the mapping of authentication, authorization and clearing transactions, it is a critical element that should be managed carefully.

Merchants/Acquirers must provide the DS Transaction ID in authorization and clearing messages.

Refer to the following document for more information on this topic: ***AN 1630 - AAV Verification Service Enhancement***

If the DS transaction ID is not provided in authorization or clearing message, transactions should not be systematically blocked. The mapping can still be done using systemic reconciliation processes.

2.6 Program Protocol

The Program Protocol is the version of the 3DS specifications being supported: 1 for 3D Secure Version 1.0 (3DS 1.0), and 2 for EMV 3-D Secure (EMV 3DS, aka 3DS 2.x).

This is a mandatory element in Mastercard authorization's CIS and Mastercard clearing's IPM specifications as from 6 November 2018:

CIS	DE48 SE 66 SF1
IPM	PDS0186

Refer to the following document for more information on this topic: ***AN 1630 - AAV Verification Service Enhancement***

2.7 Merchant names

The Merchant name used during the authentication experience and during the authorization process should ideally correspond to meet a strict interpretation of the PSD2 Dynamic Linking requirements by Issuers (refer to section on "Dynamic Linking requirements"). However, Mastercard will not reject transactions based on the non-mapping of Merchants names.

The Merchant names are captured as follows:

EMV 3DS	*MerchantName*
CIS	DE43

Mastercard's position for Europe:

The Merchant name has to be unique, consistent and as descriptive/representative as possible to avoid confusion in the identification of Merchants. The Merchant name should correspond in authentication and authorization to strictly meet the PSD2 SCA dynamic linking requirements.

It is the responsibility of Acquirers and Merchants to ensure:

- the uniqueness and consistency of Merchant names in authentications and authorizations
- Merchant names in authentication and authorization correspond (with the exception of the agent model, where a single authentication results in multiple authorizations, for example for certain travel bookings and market place transactions, but also payment facilitators). Refer to section "Agent Model".

Acquirers should also ensure that Merchant names accurately describe their online Merchant and actually belong to the Merchant in order:

- for Cardholders to recognize the Merchant name during the authentication
- to avoid fraud for example if Merchants try to re-use the name of a large and trusted Merchant as Issuers' Access Control Servers and fraud prevention tools often rely on the Merchant's name to assess the fraud risk.

Position	The Merchant name used during the authentication experience and during the authorization process will need to correspond. As of 1 July 2020, Acquirers must ensure that their online Merchants always use the same Merchant name in the authentication message. The Merchant name in authentications should uniquely identify the Merchant in all countries and for all activities (e.g. Merchant.com) or per activity (e.g. MerchantBooks.com, MerchantMusic.com) or per country (e.g. Merchant.fr, Merchant.co.uk). Acquirers must ensure that the Merchant name used by the Merchant actually belongs to the Merchant and is registered for using the Identity Check Program™.
Rationale	To comply with some specific PSD2 RTS requirements, such as Dynamic Linking requirements which requires the Merchant name to be shown to the Cardholder during authentication and the Issuer to ensure that the authentication code (AAV) is linked to the Merchant. Refer to section on "Dynamic Linking requirements". Using unique Merchant names will also reduce authentication abandonments if the trusted beneficiary (Merchant Whitelisting) exemption is used, because many Issuers will identify whitelisted Merchants by their Merchant name used during the authentication. Refer to section on "Merchant Whitelisting".

Note: as the authentication network does not support special characters out of the printable ASCII characters (for example additional letters in Nordic countries), these make it difficult to mirror Merchant names in authentication and authorization.

Mastercard will provide Acquirers, Issuers and their ACS's with a table listing Merchant names and Whitelisting Merchant names. This will allow:

- Merchant Whitelisting (refer to section on "Merchant Whitelisting") via Issuer online banking or ACS (Access Control Server) portal. It would allow Issuers which want to offer whitelisting in their online banking services to show Merchant names as used during the authentication experience and to pass it on to the ACS which manages the Whitelisting and stores the card number/Whitelisting Merchant names. During the initial setup of Merchants on the Mastercard Directory Server via the ISSM tool on MastercardConnect.com, each Merchant with its Merchant Name can be associated to a Whitelisting Merchant Name to allow multiple Merchant names to be grouped together for whitelisting (i.e. one of these Merchant Names being whitelisted will result in all the Merchant Names under that Whitelisting Merchant Name to be exempt from SCA). The Whitelisting Merchant Name will be available in ISSM as from Q4-2019.

- Acquirers and Merchants to ensure that their Merchant names are unique and consistent, and correspond in authorization and authentication messages to strictly meet the PSD2 SCA dynamic linking requirements.

The Merchant names table will only be used for dynamic linking and whitelisting (Whitelisting Merchant Name), as well as to comply with our Merchant name rules (i.e. check if a Merchant name already exists, ensure Merchant names in authentication and authorization correspond).

Acquirers should ensure they comply with GDPR, which means that their Merchants should be informed that their name will be shared with other Acquirers and Issuers.

If Merchant names differ in authentication and authorizations, transactions should still be processed and Mastercard will not reject such transactions. Mastercard aims at putting in place a close monitoring of those transactions where merchant names in authentication and authorization are different.

2.8 Biometric authentication support

Issuers are mandated to offer Cardholders biometric authentication in most European countries as of 1 April 2019 unless other specific dates have been defined for their country (refer to Appendix-A for the list of those countries).

The reference announcement specifying the mandate or recommendation and mentioning the mandate effective date is provided in Appendix-B.

> Refer to the following document for more information on this topic: ***Mastercard Biometric Authentication—Europe Region (11 January 2018)***

2.9 Auto-enrollment

Issuers need to make sure that their Mastercard branded portfolios (using Bank Identification Numbers/BINs and card ranges) are enabled to support EMV 3DS and the Mastercard Identity Check™ Program, including SCA and biometry enablement (or alternative technical SCA solutions). SCA enablement will require the activation of two-factor authentication.

Issuers should auto-enroll Cardholders in the Mastercard Identity Check™ Program when and where possible. This may require the amendment of related T&Cs. Mastercard recommends that “Mastercard Identity Check™ Program enrolment by default” is available for all existing and new issued cards. This implies that new cards would be activated only after the cardholder enrolled in the Mastercard Identity Check™ Program.

Issuers will need to make sure that they can collect the missing information necessary for auto-enrollment, e.g. mobile phone numbers to drive push notifications for example. For knowledge factors, additional registration requirements may be needed.

Depending on the Issuer country, the support of auto-enrollment is mandated or strongly recommended in Europe. The effective date was 1 October 2018 unless other specific dates have been defined for a specific country (refer to Appendix-A for the list of those countries).

The reference announcement specifying the mandate or recommendation and mentioning the mandate effective date is provided in Appendix-B.

> Issuers should start auto-enrolling their Cardholders as soon as they have enabled the Mastercard Identity Check™ Program. This means that the missing information, such as mobile phone numbers, is collected, e.g. for new Cardholders, and that terms and conditions include authentication. The enrollment is part of the adoption by the Issuer of the Mastercard Identity Check™ Program to be completed by April 2019 unless other specific dates have been defined for their country (refer to Appendix-A for the list of those countries).

2.10 Non-payment authentications for Card Add

Non-payment authentications for Card Add always require step-up authentication, which means that Risk Based Authentication should be turned off for non-payment authentications. A step-up authentication is a strong authentication decided by the Issuer.

This is useful when SCA is required, for example to add a card to Card-On-File (COF) under PSD2 RTS. It's mandatory to use SCA for all new Cards added to COF. Provisioning qualifies as an "action through a remote channel which may imply a risk of payment fraud or other abuses" pursuant to article 97(1)(C) PSD2. No exemptions are provided for these actions. Refer to section on "PSD2 SCA Exemptions and Exclusions".

When a card is added to Card-On-File and a payment is requested at the same time, only one SCA is needed to cover both the payment and the Add Card.

Different use cases apply as follows:

Use Case	Message Category	3D Requestor Challenge Indicator	3D Requestor Authentication Indicator	Cardholder Account Age Indicator	Purchase Amount
Add CoF without a payment	Non-Payment 02-NPA	“03” (Challenge Requested: 3DS Requestor Preference) OR “04’ (Challenge Requested: Mandate) for regulated markets	“04” (Add Card)	N/A	0
Add CoF as part of a payment	Payment 01-PA				>0
Add CoF as part of the first recurring or installment	Payment 01-PA		“02” (Recurring transaction) OR “03” (Instalment transaction)	“02” (During this transaction)	>0

2.11 Liability shift with EMV 3DS

A liability shift for EMV 3DS will apply as of October 2019. EMV 3DS and the Mastercard Identity Check™ Program are mandated as from 1 April 2019 unless other specific dates have been defined for the country (refer to Appendix-A for the list of those countries).

The liability shift applies to 3DS independently of the program protocol version (3DS 1.0 or EMV 3DS). If the Merchant does not support 3DS or uses Data Only (refer to section “Acquirer SCA Exemptions”), liability in case of fraud is with the Acquirer/Merchant. In all other cases, the Issuer is liable if no Acquirer PSD2 SCA exemption applies or if the Issuer has delegated SCA to the Merchant. Refer to section on “PSD2 SCA Exemptions and Exclusions”.

If the Merchant applies an Acquirer exemption through 3DS then the Merchant is liable, even if the Issuer could apply white listing (or another) exemption, as long as no step-up happens.

2.12 Co-existence of 3DS 1.0 and EMV 3DS

Mastercard does not envision the end of the liability shift for 3DS 1.0, and 3DS 1.0 and EMV 3DS will co-exist:

- Merchants not yet upgraded to EMV 3DS will have the possibility to continue using 3DS 1.0 until the Mastercard mandates are in place. The reference announcement specifying the mandates and their effective date is provided in Appendix-B.
- Issuers should not decline transactions only because 3DS 1.0 is used by the Merchant. The Issuer ACS should be capable of handling authentication requests from Merchants in both 3DS 1.0 format and EMV 3DS.

- Merchants should bear in mind that EMV 3DS allows the transport of authentication elements (e.g. device insights) that will allow Issuers to ensure transaction monitoring for every remote electronic transaction.

Before the Mastercard Identity Check™ Program mandate on 1 April 2019 (unless other specific dates have been defined for their country, refer to Appendix-A for the list of those countries), Merchants can only use EMV 3DS if the Issuer is enrolled in EMV 3DS. If not, a fall back to 3DS 1.0 will be needed. 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. The information will be provided in the Card Range Data.

The reference announcement specifying the mandate or recommendation and mentioning the mandate effective date is provided in Appendix-B.

For Acquirers that have been mandated to support EMV 3DS as from 1 April 2019, Merchants will still need to check that the Issuer is in one of the 12 countries (countries flagged as in CEE in Appendix-B) mandated to support EMV 3DS on 1 September 2019. If this is the case and the Issuer has not yet migrated to EMV 3DS, Merchants will need to fall back to 3DS 1.0 until 1 September 2019.

If an Issuer does not support EMV 3DS after the PSD2 effective date, Mastercard is looking at offering in September 2019 a stand-in authentication service (enrollment by default with opt-out option), called Smart Authentication Stand-In. Refer to section on "Authentication Services".

> If the transaction is scored as low risk then the authentication will be approved up to a certain amount to be set by the Issuer (30€ by default[1]). If not (high risk transaction or amount above €30), the authentication response will indicate that the Merchant has to fall back to 3DS 1.0 authentication requests to enable Strong Customer Authentication with step-up (EMV 3DS Authentication Response will have *Transaction Status*=N, *Transaction Reason Code*=82).

If the authentication was approved in authentication stand-in, the authorization request will indicate a fully authenticated transaction (SLI 212) however the AAV will specify that authentication stand-in was applied (AAV will have leading

[1] In early 2020 Mastercard may enhance the service and allow Issuers to change this limit in line with their fraud rate and TRA exemption limit.

indicator kJ or kC). Issuers that cannot apply a TRA or other exemptions and hence rely on low value payment exemption for such authentication stand-in transactions should ensure that the transaction counter (maximum 5) or cumulative value (maximum €100) are not exceeded since the last SCA, as per PSD2 RTS. This counter or cumulative amount validation during the authorization is also needed if the transaction uses an Acquirer exemption for low value payments (Low Transaction Risk Indicator in DE48 SE 22 SF1 = "04" (Low Value Payment) as only the Issuer can track this counter or cumulative amount as per PSD2 RTS.

If during the authorization processing the Issuer decides that SCA is required, for example because the cumulative counter or value is exceeded, then the authorization response should use response code 65 (RC65). Merchants are then required to go through 3DS authentication to enable the Issuer to apply SCA. Refer to section "Soft decline or decline-as-SCA-required".

Issuers supporting 3DS 1.0 must only implement and accept them when requested by Acquirers/Merchants.

2.13 Friendly fraud and Cardholder challenge

Friendly fraud (the consumer conducts a transaction and then files it as false chargeback using believable reasons) is a type of fraud that will require Issuer awareness and clear guidelines and best practices for their customer support / helpdesk staff.

When friendly fraud is suspected, the Cardholder should be challenged using various techniques through his/her first line interview, including but not limited to:

- The comparison of shipment address and device insights with EMV 3DS provided data.
- (possibly) The challenge of the location via geolocation information provided by the Merchant (eg if Merchant app was used).

Questions of this type should be captured in the script to be run by the Issuer's first line of support/helpdesk.

The Mastercard Claims Manager has a collaboration layer where Issuers can communicate with Merchants directly to share insights prior to sending a formal chargeback.

2.14 General Data Privacy Regulation (GDPR)

Customers are strongly encouraged to consult with their legal counsel with regards to their GDPR compliance obligations.

Key principles

- Legal ground. Merchants and Customers may rely on other legal basis than consent, including legal obligation (PSD2), contract and legitimate interest for disclosing personal data in the context of EMV 3DS and for performing Risk-Based Authentication (RBA) based on profiling.
- Purpose limitation. Mastercard and Issuers will not use EMV 3DS data for other purposes than fraud prevention and authentication, or as provided in Mastercard Rules. It excludes the usage of personal data for other purposes, such as sales, marketing and data mining (other than fraud prevention as purpose) activities. Merchants/Acquirers need to make sure their terms and conditions (especially their privacy notices) are amended to account for the capture of additional data.
- Transparency. Individuals must be provided with detailed information about how their data is collected, used and processed. This can be ensured via a Privacy Notice including at a minimum the types of data being processed, the purposes of their processing, data uses, etc.

2.15 EMV 3DS and Data Collection

EMV 3DS requires that Merchants collect much more data during the checkout experience. The Appendix-D provides the list of EMV 3DS 2.1 fields that are required, conditional or optional by the EMVCo and by Mastercard.

It appears that some of the mandatory EMV 3DS data is not always collected, e.g. the title/prefix, surname, the shipping address or the house number. Here is a web resource addressing the matter and providing examples:

> https://www.uxmatters.com/mt/archives/2008/06/international-address-fields-in-web-forms.php

When this is the case, some dummy values or processes to copy data from other fields may be required. The following provides some guidance on these:

- Title/prefix should be "M." if not captured from the cardholder.
- House number should be extracted from the street name (included number) if not captured separately or set to a default value (e.g. "99999" or similar).

- Additional address info should be space-filled if not captured.
- Shipping address should by default be equal to the billing address and vice versa, if not provided separately.

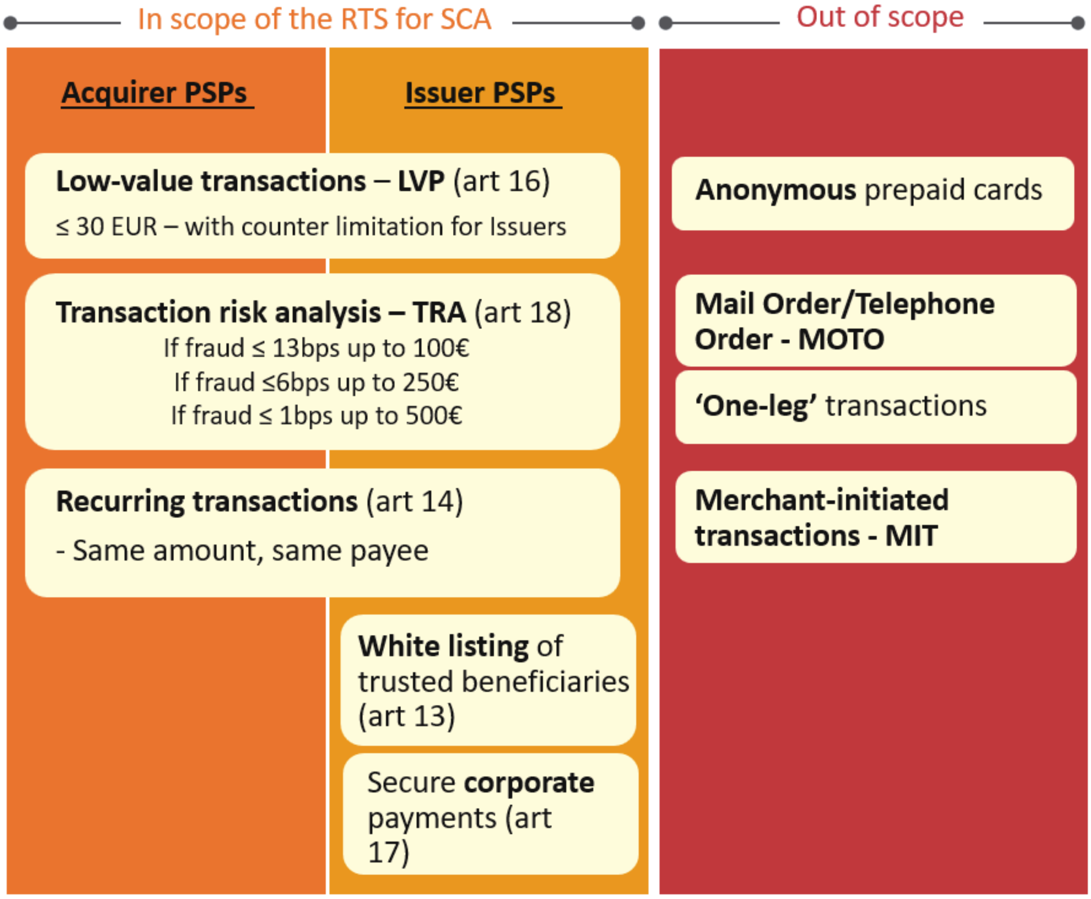
2.16 Staged Wallets

In the case of staged wallets where an initial funding transaction is followed by payment transactions, the following points are important:

- If a wallet provider provides SCA services to an Issuer, the Issuer should ensure that SCA delegation to that wallet provider has been agreed upon. Mastercard is currently working on a program that will facilitate SCA delegation. More information on this will be communicated when available.
- As Merchant-Initiated Transactions are out of scope of the PSD2 RTS on SCA for card payments, these would apply to funding transactions which means that no SCA would be required.

Section 3 - PSD2 SCA Exemptions and Exclusions

An important aspect of the PSD2 RTS is the set of exemptions that will apply in various circumstances. The following diagram depicts the areas in-scope of the PSD2 RTS but exempted (left-hand side), and the areas out-of-scope of the PSD2 RTS (right-hand side).


In scope of the RTS for SCA
Out of scope
Acquirer PSPs
Issuer PSPs
Low-value transactions – LVP (art 16)
≤ 30 EUR – with counter limitation for Issuers
Transaction risk analysis – TRA (art 18)
If fraud ≤ 13bps up to 100€
If fraud ≤6bps up to 250€
If fraud ≤ 1bps up to 500€
Recurring transactions (art 14)
- Same amount, same payee
White listing of trusted beneficiaries (art 13)
Secure corporate payments (art 17)
Anonymous prepaid cards
Mail Order/Telephone Order - MOTO
'One-leg' transactions
Merchant-initiated transactions - MIT

3.1 EMV 3DS support of the PSD2 RTS on SCA

The EMV 3DS 2.2 specifications are including a set of features to support the PSD2 RTS on SCA:

- Acquirer SCA exemptions through the 3DS Requestor Challenge Indicator
- Whitelisting through the Whitelist Status
- MOTO transactions through the 3RI Indicator and message flow for payments (EMV 3DS 2.1 supports 3RI but only for non-payments)

This data is not available in the current EMV 3DS 2.1 specifications. As the timeline for rollout of EMV 3DS 2.2 is not yet decided and there is an urgent need to provide a platform allowing compliance by the PSD2 effective date of 14 September 2019, Mastercard has defined a new Mastercard PSD2 Message Extension to the current EMV 3DS 2.1 specifications that will support some of the EMV 3DS 2.2 features listed above but also introduce new data elements that will help to support the PSD2 RTS on SCA and that are not covered by the EMV 3DS 2.1 nor the EMV 3DS 2.2. The Mastercard PSD2 Message Extension will be available in September 2019.

Here is the list of those data elements. Shaded cells indicate when the feature is already supported in the EMV 3DS 2.2 specifications.

Feature	EMV 3DS 2.1 – PSD2 Mastercard Message Extension	EMV 3DS 2.2
Acquirer SCA exemption **(in ARes and RReq)**	PSD2 Mastercard Message Extension **AReq Field 1 = 3DS Requestor Challenge Indicator** 05 = No challenge requested transactional risk analysis is already performed). **05 will be used for the following Acquirer exemptions: low-value payment, TRA, recurring payment AND MIT (refer to section on "Merchant-Initiated Transactions")** 06 = No challenge requested (Data share only) 07 = No challenge requested (strong consumer authentication is already performed under Issuer delegation)	Already supported in specs Field threeDSRequestorChallengeInd) = Same values as in previous column
Merchant Fraud Rate **(in AREq)**	PSD2 Mastercard Message Extension AReq Field 2 = Merchant fraud rate in bps taking into account all Merchant sites and card volumes, calculated as per PSD2 RTS Article 19 1= fraud level <=1 bps 2= fraud level >1 and <= 6 bps 3= fraud level >6 and <= 13 bps 4= fraud level >13 and >= 25 bps 5= fraud level >25 bps The merchant fraud rate is optional and has to be calculated by the Acquirer as per PSD2 RTS (EEA volumes, remote electronic transactions excluding out of scope items (MOTO, MIT, etc), for all schemes)	Same as in previous column

Feature	EMV 3DS 2.1 – PSD2 Mastercard Message Extension	EMV 3DS 2.2
Acquirer Country Code **(in AReq)**	PSD2 Mastercard Message Extension AReq Field 3 = numeric ISO country code of the Acquirer if in the EEA. If the ISO country code is in the EEA, then related transactions are in scope of the PSD2 RTS on SCA.	Same as in previous column

Secure Corporate Payment
(in AReq)
	PSD2 Mastercard Message Extension
	AReq Field 4 = Whether the electronic payment transaction uses dedicated payment processes or protocols under PSD2 RTS Article 17's Secure Corporate Payment Exemption which the Issuer can apply
	Y = yes
	N = no
		Same as in previous column

Whitelist Status **(in ARes)**	PSD2 Mastercard Message Extension ARes Field 1 = Y = 3DS Requestor is whitelisted by cardholder N = 3DS Requestor is not whitelisted by cardholder E = Not eligible as determined by Issuer P = Pending confirmation by cardholder R = Cardholder rejected U = Whitelist status unknown, unavailable, or does not apply	Already supported in specs Field whiteListStatus = same values as in previous column

What if one of these fields is not populated in the message extension?

- NO Acquirer SCA exemption: an Acquirer exemption cannot be requested before EMV 3DS 2.2.
- NO Merchant Fraud rate: the data point is not provided to the ACS/Issuer to increase its level of confidence in the ongoing transaction. Also, Issuers may use it to decide if a Merchant should be eligible for the white listing exemption.
- NO Acquirer Country Code: an ACS/Issuer could flag the ongoing transaction as a one-leg transaction out of scope of the PSD2 RTS on SCA.
- NO Secure Corporate Payment: the Merchant will not be capable of highlighting the existing agreement and potential exemption to the ACS/Issuer.
- NO Whitelist Status: the Merchant will not be informed if it is whitelisted in the ongoing transaction.

In response to an Acquirer exemption (Field 1="05"), the ACS should respond with an ECI=6 with leading indicators of kN keeping the liability to the Merchant:

- For an EMV 3DS v2.1, an ACS response of *Transaction Status* = "N" with a new Transaction Status Reason Code of "81".
- For an EMV 3DS v2.2, an ACS response of *Transaction Status* = "I" with any value in the Transaction Status Reason Code.

The Directory Server will reject the ARes with ECI=6 if the above flagging is not used.

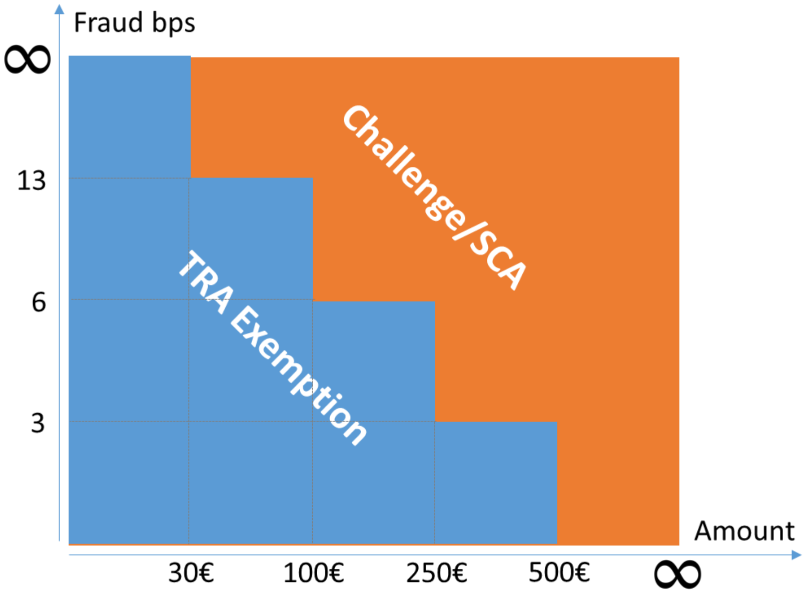
3.2 Acquirer SCA exemptions

An Acquirer can apply SCA exemption only if PSD2 RTS conditions are met:

- An Acquirer exemption is available for:
  - Low-value payments when the payment is not higher than €30. The Issuer must check if the transaction counter (maximum 5) or cumulative amount (maximum €100) since the last SCA is not exceeded as per PSD2 RTS.

    Refer to the section 'Low-Value Payments (LVP) and management of counters" for more information on this.
  - Transaction Risk Analysis (TRA) due to low fraud rate (art 18 – see fraud thresholds for transaction value ranges below). Mastercard aims at monitoring compliance by checking if the Acquirer and Merchant fraud rate are below the fraud level in bps.

    * 1 bps = 1 % divided by 100 = 1 out of 10,000



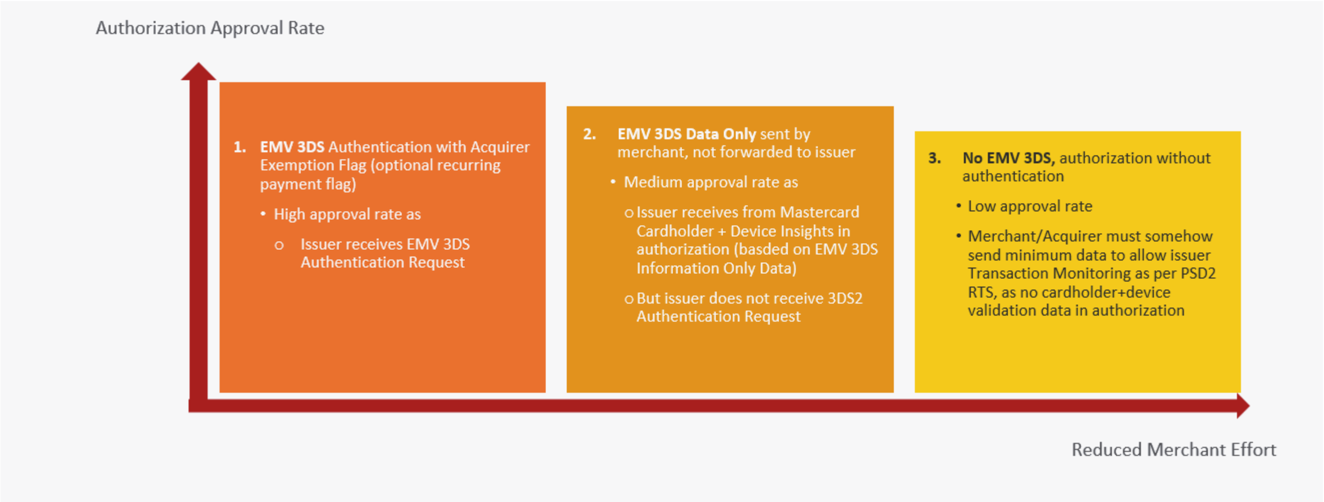
- ○ Recurring Payment✪ if the amount is the same. When the amount varies, the transaction may fall under **Merchant Initiated Transactions**. Refer to section on "Merchant-Initiated Transaction (MITs)".

✪ Merchant-Initiated Transactions (MITs), when the Cardholder is off-session and the Merchant initiates the payment without any involvement of the Cardholder in triggering the transaction(s) (such transactions are out of scope from PSD2 RTS) are not exempted but excluded, i.e. out of scope of the PSD2 RTS on SCA.

Decoupled authentications can also be applied (refer to section "Decoupled authentication").

- The Acquirer / Merchant is liable in case of fraud if the Issuer does not apply SCA.
- Transaction monitoring has to be applied by the Issuer and the Acquirer.

For Recurring Payments and Acquirer TRA exemptions, Mastercard proposes the following 3 options for Merchants/Acquirers to provide the required information to the Issuer:



1. **EMV 3DS** Authentication with Acquirer Exemption Flag (optional recurring payment flag)
   - High approval rate as
     - o Issuer receives EMV 3DS Authentication Request

2. **EMV 3DS Data Only** sent by merchant, not forwarded to issuer
   - Medium approval rate as
     - o Issuer receives from Mastercard Cardholder + Device Insights in authorization (basded on EMV 3DS Information Only Data)
     - o But issuer does not receive 3DS2 Authentication Request

3. **No EMV 3DS,** authorization without authentication
   - Low approval rate
   - Merchant/Acquirer must somehow send minimum data to allow issuer Transaction Monitoring as per PSD2 RTS, as no cardholder+device validation data in authorization

The highly recommended option 1 will drive the highest authorization approval rate as a full EMV 3DS authentication request with all required data will be provided to the Issuer for an optimal "decisioning" process.

The option 2 is an intermediate option allowing the Merchant to provide additional data but without going through the authentication process. The Issuer will receive cardholder and device insights in the authorization message. The anticipated approval rate of those transactions will be lower than fully authenticated transaction (option 1) but higher than no-EMV 3DS (option 3).

Mastercard sets minimum quality standards (minimal authorization approval rate and a maximum abandonment rate) whenever EMV 3DS is used.

> The Mastercard Identity Check™ Program already requires a minimum authorization approval rate of 90% for fully authenticated transactions. As EMV 3DS allows a lot more data to be exchanged, fraud detection should improve vs 3DS 1.0 which is expected to lead to reduced false declines and higher authorization approval rates. EMV 3DS is also expected to reduce authentication abandonments.

Mastercard will monitor on an ongoing basis the Key Performance Indicators (KPIs) of authorization approval rate, authentication abandonment rate and fraud rate. This latter is important to leverage the TRA exemption.

> Refer to section on "Authentication Quality".

Mastercard's position for Europe:

An authorization in the European Economic Area (EEA) zone (Acquirer and Issuer in an EEA country) without authentication (i.e. no EMV 3DS or EMV 3DS Data Only) is only allowed if an Acquirer exemption or MIT applies as per PSD2 RTS, or if another SCA compliant method is used. 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 DE48 SE22 SF1 in the authorization message.

> Issuers are recommended to NOT systematically decline authorizations without authentications when these use an Acquirer SCA exemption as per the PSD2 RTS. Additional information provided to the Issuer, through the EMV 3DS Data Only channel for example, should lead to increased confidence in the transaction to the Issuer. Another option is the use of a soft decline or "decline-as-SCA-required" (refer to section on "Soft Decline") by the Issuer when SCA is requested. This will suggest the Merchant to re-submit the request but now with EMV 3DS.

The position above has been translated as a requirement for Acquirers to set the Acquirer exemption indicator in the authorization.

Position

As of 14 September 2019 in the authorization request/0100 message for an intra-EEA Remote Electronic Transaction that is subject to PSD2 RTS, authentication can only be skipped if an Acquirer exemption to strong Cardholder authentication applies or if another Strong Customer Authentication compliant method was used (e.g. delegation to the Merchant, Secure Corporate Payment exemption applied with the Merchant's knowledge). 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 Data Element 48, 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

As of 14 September 2019 EEA Issuers must be able to process Data Element 48, sub-element 22, subfield 1 in the authorization message and they should only apply Strong Customer Authentication (SCA) on such transactions when Transaction Monitoring under PSD2 RTS suggests a high fraud risk.

As of 1 November 2019 Acquirers in the EEA which allow their online Merchants to request a Transaction Risk Analysis (TRA) exemption under PSD2 RTS must set the TRA exemption flag for such Merchants when registering them for the Identity Check Program in the Identity Solutions Services Management (ISSM) tool.

In order to optimize authorization approval rates for transactions using an Acquirer exemption under PSD2 RTS, it is recommended that Merchants send an EMV 3DS authentication request with Acquirer exemption flag.

It is mandated that EEA Acquirers and Issuers ensure as of 1 November 2019 that the "Acquirer exemption" flag (used for all Acquirer exemptions, ie low value payment and TRA exemption and recurring payment) can be supported in EMV 3DS authentication requests:

- In version 2.1 PSD2 message extension Field 1 with value 05/No SCA Requested, Transaction Risk Analysis performed
- and as of v2.2 Challenge Indicator value 05/No SCA Requested, Transaction Risk Analysis performed.

It is mandated that EEA Acquirers with online Merchants accepting corporate cards, as well as that corporate card Issuers ensure as of 1 November 2019 that the "dedicated processes and protocol" flag (which indicates if the conditions for the secure corporate payment exemption are met and hence if the exemption can be applied by Issuers) can be supported in EMV 3DS authentication requests as of version 2.1 in the PSD2 message extension field 4.

For EMV 3DS Data Only messages, the AReq uses Message Category = "80". For EMV 3DS Data Only, the ARes will return a Transaction Status of "U" (Authentication/ Account Verification Could Not Be Performed; Technical or other problem, as indicated in ARes or RReq) with a Transaction Status Reason Code = "80".

Refer to the following document for more information on this topic: ***AN 2609 - Enhancements to Support the Low-Risk Transaction Indicator for EEA Customers***

3.3 Flagging and liability shift matrix with PSD2

In the following table:

- Columns 1 and 2 define if Merchants will use EMV 3DS or not, and what type of exemption will be requested.
- Columns 3 and 4 clarify how those transactions will be flagged in authentication and authorization.
- Column 5 specifies the type of action that is expected for those transactions.
- Columns 6 and 7 identify the AAV leading indicators and SLI that will appear as a result of those transactions with the expected Issuer action.
- Last by not least, the last column clarifies where the liability stands for those transactions and the expected Issuer action.

In the table below, SLI217 will be optional for European ACS/Issuers in response to an authenticated recurring payment EMV 3DS 2.1. Most will probably continue to use 212 as today. With EMV 3DS 2.2, SLI217 will have to be used by ACS in response to a 3RI authentication request for subsequent payments in a recurring payment arrangement. Acquirers will have to support SLI217 which gives them fraud chargeback protection.

In the table, when "3DS Req Chal Ind = 05" is mentioned, this is for EMV 3DS 2.2 as this value does not exist in EMV 3DS 2.1. For this earlier version, the 3DS Req Chall Ind = 02 and the Field 1 of the PSD2 Mastercard message extension = 05.

Merchant	Exemption	Authentication	Authorization	Expected Issuer action	AAV Leading Indicators	SLI	Liability
No 3DS or Data Only	No exemption			Decline as not compliant			Acquirer
No 3DS or Data Only	LVP		DE48 SE22 SF1 = 4	**Accept exemption** **Check LVP counters**		210	Acquirer
No 3DS or Data Only	Acquirer TRA		DE48 SE22 SF1 = 2	**Accept exemption**		210	Acquirer
No 3DS (STA) or Data Only	RP/MIT first		DE61 SE4 = 4 DE48 SE22 SF1 not set	Not compliant RC65 to step-up			Acquirer
No 3DS (STA) or Data Only	RP/MIT subsequent		DE61 SE4 = 4 DE48 SE22 SF1 = 1 or 3	**Accept exemption**		210	Acquirer

Merchant	Exemption	Authentication	Authorization	Expected Issuer action	AAV Leading Indicators	SLI	Liability
EMV 3DS	No or **Any**	*Based on exemption*	*Based on exemption*	**No 3DS**	kL or kE	211	Issuer
EMV 3DS	LVP	3DS Req Chal Ind = 05*	DE48 SE22 SF1 = 4	**Accept exemption** **Check LVP counters**	kN	216	Acquirer
EMV 3DS	Acquirer TRA	3DS Req Chal Ind = 05	DE48 SE22 SF1 = 2	**Accept exemption**	kN	216	Acquirer
EMV 3DS	No or **Any**	*Based on exemption*	*Based on exemption*	**Issuer TRA** Check LVP counters if LVP exemption	kA or kG	212	Issuer
EMV 3DS	No or **Any**, except RP/MIT first	*Based on exemption*	*Based on exemption*	**Challenge** Reset LVP counters	kB or kH	212	Issuer
EMV 3DS	RP/MIT first	3DS Req Auth Ind = 02	DE61 SE4 = 4	**Challenge**	kB or kH	212	Issuer
		3DS Req Chal Ind = 04	DE48 SE22 SF1 not set	**Required**	kO	217	

3.4 Soft decline or decline-as-SCA-required

In view of an authorization request without authentication (no-3DS or EMV 3DS Data Only), an Issuer may decline the request and indicate at the same time to the Merchant/Acquirer that SCA is required. The Merchant/Acquirer will then initiate a second flow including an authentication request followed by an authorization request.

The Issuer will indicate to the Merchant/Acquirer that SCA is required by returning the value 65 (Exceeds withdrawal count limit) in DE39 of the authorization response. The Merchant receiving a response code of 65 (RC65) will need to go through SCA and will therefore need to flag the:

> *3DS Requestor Challenge Indicator* = "03" (Challenge Requested: 3DS Requestor Preference) or "04" (Challenge Requested: Mandate). "04" for regulated markets.

Until all Issuers support RC65, Merchants are recommended to always send an authentication request following an authorization that was declined for non-financial and non-technical reasons. Besides, it is recommended that the authentication request is sent without asking the consumer to re-enter card details. The Merchant should have a mechanism to re-use card details used for the initial authorization.

As declined authorizations followed by an authentication and another authorization will add an estimated 10 seconds latency, some Cardholders may abandon such transactions.

Merchants are therefore recommended to always send authentication requests, especially with Issuers that decline authorizations without prior authentication.

*Note: If Merchants go straight to authorization, the authorization has to be done **during checkout**, i.e. before goods are actually shipped (clearing has to wait until shipment). Indeed, the Issuer softly declining the authorization will require SCA to occur while the cardholder is still in-session.*

Acquirers are requested not to normalize the error codes to their merchants so that these are aware of RC65.

The Acquirer exemption with authentication will be indicated by SLI 216.

In this case, the AAV will be provided. A new AAV prefix should be used by Issuers in this case to avoid Merchants using the AAV to flag the authorization as fully authenticated and benefit from liability shift.

In this case, the Acquirer will be liable in case of fraud, except if the Issuer decides to step up. If the Issuer decides to step up, the SLI used will be 212, i.e. both the Merchant and the Issuer are UCAF-enabled.

3.5 PSD2 SCA Exemptions and Maestro

Currently we have three special programs enabling ecommerce European Merchants to accept Maestro transactions without 3DS (Transaction Processing Rules Europe Region 5.3)

They are

- Maestro Low Merchant Risk Program (MLRMP)
- Maestro Utility Payment Program (MUPP)
- Maestro Recurring Payment Program (MRPP)

MLRMP, MUPP and MRPP participating Merchants are subject to eligibility and operations requirements that are specified in the Europe Operations Bulletin December 2011 and Europe Region Operations Bulletin March 2016.

Today MLRMP, MUPP and MRPP participating Merchants use specific values:

- SLI 213
- Mastercard-assigned Merchant ID
- static AAV

These specific values are peculiar to these special Maestro programs and they are not used for Mastercard.

From the PSD2 RTS on SCA effective date:

- ecommerce European Merchants who want to accept Maestro transactions without Strong Customer Authentication will be able to do so only if an RTS regulated exemption applies;
- the above Maestro specific values will come to an end (SLI 213, Mastercard-assigned Merchant ID, static AAV);
- Merchants who want to leverage Acquirer exemptions will have to follow the same use cases and specifications for Mastercard and for Maestro.

3.6 Low-Value Payments (LVP) and management of counters

As per the PSD2 RTS, payments are considered as low value if less than or equal to 30 euros or equivalent in other currencies.

The PSD2 RTS also set maxima above which SCA will be required:

- Maximum number of consecutive transactions without SCA = 5
- Maximum cumulative amount of transactions without SCA = 100 euros or equivalent in other currencies.

The LVP exemption can be applied by Issuers but as well by Acquirers.

Because Acquirers are not able to count the number of transactions and cumulative amount since the last SCA, this must be done by the Issuer authorization host system during authorization processing especially when Acquirers apply the LVP SCA exemption without sending an authentication request. When these counters or cumulative amount limits are exceeded, Issuers should respond with response code 65 and Merchants should send an authentication request (refer to section on “Soft Decline”).

A LVP exemption will be indicated by the Merchant/Acquirer by 3DS Requestor Challenge Indicator = “05” in authentication and DE48 SE22 SF1 = “04” in authorization.

3.7 Merchant Whitelisting

Refer to the following document for more information on this topic: **Mastercard Standards for Merchant Whitelisting v1.0**

3.8 Secure Corporate Payments

The PSD2 RTS' Article 17 states that secure corporate or Business-to-Business (B2B) payments over dedicated payment processes and protocols are exempted and that this exemption will apply to "payment processes or protocols that are only made available to payers who are not consumers where competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security" to those achievable with SCA.

Although this leaves the decision with the competent authority of each Member State, Mastercard believes that the lodged and virtual corporate/commercial cards should be exempted:

- Lodged cards: A commercial card that is lodged with a company-approved third party, such as a travel company that books travel and hotels on behalf of the company by secure dedicated payment process and protocol. Use cases include both traditional company travel procurement (via a company-approved travel agency) and broader business-to-business procurement, where commercial cards are lodged securely directly with approved company suppliers.
- Virtual Card Numbers: Virtual card numbers (VCNs) used over dedicated payment processes and protocols ensure a very high level of security. The generation of VCNs is protected with SCA and the virtual PAN itself can also be uniquely linked to the Merchant or other parameters that further control its use (e.g. amount, time).

To identify corporate payment transactions, 2 scenarios are possible:

- Firstly the lodged and virtual cards that could be identified by the Issuers & their ACS based on the product/PAN and where Issuers could indicate to Acquirers (via their ACS) that SCA is not required.

  It is recommended that Issuers inform their ACS of card numbers or card ranges that can use this secure corporate payment SCA exemption (eg because card number is a lodged account or virtual corporate card number) to avoid step-up. ACS services will need to apply a risk-based authentication for these transactions to comply with Transaction Monitoring under PSD2 RTS.

- Secondly the "individual/plastic" corporate cards where the product as such is not exempted but rather the transaction, i.e. bookings via Corporate Travel Agents.

In order to properly identify transactions that are "secure corporate payments" not subject to the PSD2 SCA requirements, Mastercard has defined an EMV 3DS v 2.1 message extension with a Secure Corporate Payment flag (refer to section "2.1.EMV 3DS support of the PSD2 RTS on SCA"). This will allow Merchants to indicate that dedicated processes and protocols were used as required for secure corporate payment exemption, by which the Issuer's ACS could then decide if indeed eligible to apply the exemption.

EMV 3DS 2.1 and EMV 3DS 2.2 – Mastercard Message Extension:

Field #	Field	Field Definition
4	Secure Corporate Payment	Whether the electronic payment transaction uses dedicated payment processes or protocols under PSD2 RTS Article 17's Secure Corporate Payment Exemption which the Issuer can apply

The majority of Corporate Air bookings is made using a Corporate Travel Agent. The Travel Agent often makes the airline booking using a Global Distribution System (GDS). Managing authentication into the process will be needed to meet the SCA mandate at the time of reservation. An option might be that the booking tool triggers 3DS when the cardholder is in session. Further details will be provided in a separate document focusing on Travel Use Cases.

The merchant should send an authentication request, unless the merchant has a way of recognizing the transaction as secure corporate payment exempted, in which case the merchant can send the transaction directly for Authorization. The issuer remains responsible for the validation of the exemption and should not request SCA for secure corporate payment exempted transactions. In case the issuer deems that the transaction is not subject to a secure corporate payment exemption, the issuer should do a soft decline.

Mastercard strongly recommends that Issuers register Lodged and Virtual/Corporate Cards on the Identity Check Authentication Network to avoid merchants refusing to complete the transaction purely because the issuer does not support Mastercard Identity Check.

3.9 Out of the scope of the PSD2 RTS

3.9.1 Anonymous prepaid cards

Due to their very nature, payments made through the use of an anonymous payment instruments, such as anonymous prepaid (e.g. gift) cards, are not subject to the obligation of strong customer authentication.

The Issuer will be the only one able to identify this type of cards. The Acquirer will not be able to identify from the primary account number that the product is an anonymous product. There is indeed no specific Mastercard product code or Mastercard BIN associated to the anonymous nature of the payment instrument.

However, a new account range indicator ("Anonymous indicator") will be introduced in October 2019 (4th Release of Mastercard's core systems). The Anonymous Indicator will signal to Acquirers whether a Mastercard and Maestro prepaid account range is anonymous or non-anonymous.

> Refer to the following document for more information on this topic: ***AN 2509 - Announcing the Prepaid Anonymous Indicator ("Anonymous Indicator")***

Remark: there may be prepaid programs requiring Customer due diligence where the name of the Cardholder (what the Merchant sees) is not mentioned but that are non-anonymous cards in the PSD2. This is the case of some instantly issued types of cards.

Mastercard Rules allow Issuers not to register Anonymous Prepaid Cards on the Identity Check Authentication Network. If there is concern that Merchants refuse cards when the Authentication Request would result in an Attempt due to expectation of lower approval rates then Issuers may need to consider registering these cards anyway.

3.9.2 Mail Order / Telephone Order (MOTO)

The PSD2 RTS is not covering Mail Order/Telephone Order (MOTO) transactions.

In authorization messages, MOTO transactions are flagged by a value of 2 (Cardholder not present - mail/facsimile order) or 3 (Cardholder not present - phone or Automated Response Unit [ARU]) in DE61 SF4.

Flagging MOTO transactions in the correct way is the liability of the Merchant and the PSP/Acquirer.

In EMV 3DS 2.2, specifications, the value 08 (Mail Order) or 09 (Telephone Order) in the 3RI Indicator will indicate a MOTO transaction.

Voice commerce (aka. vCommerce) transactions, leveraging user interaction with voice recognition technology, will generally require SCA (unless an exemption applies).

3.9.3 One-leg transactions (one leg in the EEA, the other out)

The PSD2 RTS is generically referring to Payment Service Providers (PSPs) to identify parties that are either managing the acceptance and/or the issuance of electronic remote card-based payment transactions.

Mastercard is translating this into Acquirer and/or Issuer since these are the legal entities that are Customers of Mastercard.

The locations of the Issuer and Acquirer are relevant to determine if the RTS SCA requirements apply to two-leg transactions. Thus, it is sufficient that the Issuer and the Acquirer are located in the EEA for the RTS to apply.

The location of the cardholder and Merchant is in principle not relevant. However, Mastercard has asked the EBA to confirm that the Issuer is allowed to use the Merchant's location as a proxy (in lieu of the Acquirer's location) to determine whether the Acquirer is located in the EEA. Under PSD2, a card in the EEA must be issued by an Issuer in the EEA. If the card is issued in the EEA, the Issuer is also in the EEA and is subject to the PSD2 SCA requirements.

On the acquiring side, the Acquirer must be licensed in the EEA* to acquire Merchants in the EEA. If the card is issued in the EEA and the Merchant is in the EEA, the Issuer and Acquirer are in the EEA and transactions are "two-leg" transactions.

(*) We understand that certain non-EEA airlines are acquired by an EEA Acquirer. If a non-EEA airline uses an EEA Acquirer, EEA Issuers may decline a no-3DS authorization without Acquirer exemption. To avoid this, these non-EEA airlines are recommended to use 3DS or to flag the authorization with an Acquirer exemption flag if that can be applied.
Airlines Merchants are recommended to use the correct Merchant country code.

If the Issuer is in the EEA and the Merchant is not in the EEA but is acquired by an Acquirer in the EEA, the Merchant country code would give the impression to the Merchant that the transaction is "one-leg" not subject to the PSD2 SCA requirements. As the PSP/Acquirer is in the EEA, PSD2 SCA requirements will apply.

Mastercard's position for Europe:

Position

As of 14 September 2019 if the Issuer and the Acquirer are in the EEA but the Merchant is not, EMV 3DS authentication requests must include the PSD2 Message Extension with Field 3 containing the Acquirer country code. In other cases it is recommended to provide the Acquirer country in the EMV 3DS PSD2 Message Extension Field 3.

The Issuer and its Access Control Server are recommended to use the Acquirer country code in the PSD2 Message Extension Field 3 to determine if Strong Customer Authentication (SCA) is required by PSD2 RTS. If the Acquirer country is not provided, then Issuers are recommended use the Merchant country to determine if SCA is required by PSD2 RTS.

How to recognize Acquirer/Issuer country to apply SCA under PSD2?

In order to properly identify transactions that are "two-leg" subject to the PSD2 SCA requirements, the EMV 3DS specifications have been amended to include the Acquirer country code (refer to section "2.1. EMV 3DS support of the PSD2 RTS on SCA"):

EMV 3DS 2.1 and EMV 3DS 2.2 – Mastercard Message Extension:

Field #	Field	Field Definition
3	Acquirer Country Code	Acquirer country code is required when the Acquirer country differs from the Merchant country and the Acquirer is in the EEA (e.g. an Acquirer in the EEA acquiring an airline Merchant in the US). If both Acquirer and Issuer are in the EEA, PSD2 SCA requirements apply

The following elements apply as well in the identification of the Acquirer and Issuer countries:

- The Issuer country is identified by the BIN related to the PAN being used. The Member Parameter Extract (MPE) table allows to associate the Issuer country related to a BIN.
- Similarly, the Acquirer country is identified by the Mastercard Customer ID hosted in the DE32 of the authorization message. The Member Parameter Extract (MPE) table IP0072T1 (Expanded Member ID Master) maps the Mastercard Customer ID to the Acquirer country.
- Merchants may not have received from their Acquirer(s) an extract of the MPE tables. If this is the case, Merchants can obtain the BIN table, called the BIN Table Resource, from Mastercard.

The BIN Table Resource provides a list of active and valid issuing account ranges to help Merchants and service providers successfully accept Mastercard transactions and prevent valid accounts from being declined.

Value-add to Merchants:

Reliability	Accurate lists are provided directly by Mastercard – the most reliable source for up-to-date information
Efficiency	With direct access to information, there is no need to continually monitor unauthorized lists
Insight	Helps improve routing, fraud "decisioning", information on brand, product and authorization.

The BIN Table Resource will provide authorization parameters ensuring greater BIN information accuracy:

- Acceptance Brand: Identifies whether an account range is used for issuing credit, debit, or private label cards;
- Authorization Only: Identifies accounts from which a private label or prepaid card has been issued to provide Cardholder with prefunded discount or prepaid value only redeemed at select Merchants at checkout;
- Issuing Country Code: Assists in e-commerce fraud management to help detect inconsistencies between the IP address of the originating purchase and the Cardholder billing address that may warrant additional analysis.
- Local Use: Identifies whether cards within the authorization account range may be used outside of the country of issuance;
- Brand Product Code: Identifies the Mastercard accepted brands: Mastercard Credit, Mastercard Debit, Maestro, Cirrus, Mastercard Private Label;
- Series 2 BINs: Range of BINs that begin with "2" and are processed the same as the series "5" BINS.

3.9.4 Merchant-Initiated Transaction (MIT)

Merchant-Initiated Transactions are payments initiated by the Merchant without the interaction of the payer. They are characterized by a lack of involvement of the payer in triggering each individual payment. Such payments require that (1) SCA is applied to the first transaction/action mandating the Merchant to initiate payment(s) and (2) there is an agreement between the payer and the Merchant for the provision of products or services and potential costs associated with these. Such payments can happen in the following cases:

- Recurring Payments for fixed or variable amounts.
- Merchant funded instalments.
- The final amount is higher than the amount used at authentication time. This can happen when additional charges are added to the initially agreed amount.

  E.g. minibar in a hotel or fines with a rented car. The Merchant should anticipate as much as possible these potential additional charges but in some cases, the pre-defined amount may be reached, thus leading to re-authentication for the incremental charge.

Merchants will bear liability for MITs. However, the liability shifts to the Issuer if:

- 3DS is used and serves Issuer transaction monitoring purposes (see below)
- 3RI is used in EMV 3DS 2.2 for subsequent recurring payments (SLI217)

As confirmed by the EBA, MITs are out of scope of the PSD2 RTS on SCA, under the following conditions:

- the transaction is triggered by the Merchant and the cardholder is off-session and
- the transaction could not have triggered during cardholder checkout, because
  - The final amount was impossible to determine during the checkout (e.g. online groceries shopping) or
  - An event triggered the transaction after the checkout (e.g. miscellaneous rental or service charges, staged-wallet funding transaction) or
  - The transaction is part of a recurring payment arrangement or
  - The transaction is broken down into different payments happening at different times (e.g. instalments, travel bookings, market places).

To set-up an MIT, Strong Customer Authentication is required, as well as an agreement between Merchant and cardholder specifying the reason for the payment and the payment amount (or an estimate when the precise amount is not known).

The EMV 3DS specifications are supporting MITs as follows:

EMV 3DS 2.1	*3DS Requestor Challenge Indicator* = "02", AND PSD2 Mastercard Message Extension Field1 "Acquirer SCA exemption" = "05" / No challenge requested (transactional risk analysis is already performed)
EMV 3DS 2.2	*3DS Requestor Challenge Indicator* = "05" / No challenge requested (transactional risk analysis is already performed)

A Merchant-Initiated Authorization Request will be flagged by the Merchant/Acquirer by DE48 SE22 SF1 = "01" of the authorization request.

Mastercard recommends that Merchants send EMV 3DS (with 3DS Requestor Challenge Indicator = "02" so that Issuers are instructed not to step-up) as it provides the data to the Issuer to check e.g. if device authenticators are compromised (which is required under Transaction Monitoring).

Issuers are required to not systematically decline MIT with no-3DS authorization and not step-up if EMV 3DS is used. As MIT is not part of PSD2 RTS and given the importance of MIT, Mastercard will start monitoring Issuer behavior when handling MIT.

Mastercard's position for Europe:

Position	MIT should be flagged by populating Data Element 48, sub-element 22, subfield 1 in the authorization message with 01=Merchant Initiated Transaction. As of 1 November 2019 when setting-up an MIT includes an authorization request (or Account Status Inquiry), its Trace ID has to be provided by the EEA Acquirer in subsequent related authorizations in DE 48 sub-element 63 (Trace ID). If the initial authorization happened before 14 September 2019 and its Trace ID is not available (eg was not stored), then the Trace ID must have the following values: Positions 1–3 = « MCC » Positions 4–9 = « 999999 » Positions 10–13 = 1231 Positions 14–15 = blank filled As of 1 November 2019 EEA Issuers must be able to process the Trace ID provided in authorizations in DE 48 sub-element 63 (Trace ID), for example to validate if an initial SCA took place to set-up the MIT as required under PSD2 RTS.

Section 4 - Specific Use Cases under PSD2

4.1 General flow for all use cases

The following general flow is applicable to all use cases that are listed under "Use Cases for in-session payments" and "Use cases for off-session payments". The specifics of each of these use cases will be provided in the related section.

- The Merchant sends an EMV 3DS authentication request for an amount that is called the authentication amount. The amount to be indicated will depend on the use case that will be described in the following sections.
    - In case of Recurring Payment, the 3DS Requestor Prior Transaction Reference will capture the DS Transaction ID of the initial Recurring Payment Agreement authentication. This reference is required to complete the authentication process successfully.
    - In case of an MIT, the 3DS Requestor Prior Transaction Reference will capture the DS Transaction ID of the initial MIT Agreement authentication. This reference is required to complete the authentication process successfully and must be provided in subsequent authentications where the Merchant is looking for an Issuer authentication when consumer is out-of-session.
- The ACS decides to go for a challenge or risk-based authentication (RBA requiring Issuer exemption) and generates an authentication code (AAV).
    - The Cardholder needs to be in-session in case of challenge.
    - If not, subsequent Merchant-Initiated Transactions may be leveraged or a decoupled authentication may be applied (refer to section on "Decoupled authentication").
- The Acquirer presents the authorization (possibly delayed) including
    - The AAV.
    - In case of Recurring Payment or MIT, DE48 SE63 will capture the Trace ID of the initial Recurring Payment Agreement or MIT.
    - The DS Transaction ID.
- In the case where EMV 3DS is used, Mastercard injects Digital Transaction Insights (refer to section on "Digital Transaction Insights") into the authorization request to provide the Issuer with an assessment of the EMV 3DS provided data.
- The Issuer authorizes the transaction upon

- Retrieving the original authentication using the 3DS Transaction ID
- Validating the original AAV (see remark above for Recurring Payments)
- Dynamic Linking of authentication vs. authorization by
  - (for non-Recurring Payments) Comparing the authorization transaction amount (possibly accumulated) to be less than or equal to the authentication amount. If not possible (e.g. the amount has changed), the AAVs in authentication and authorization will be compared.
  - Matching Merchant names

4.2 Amounts to be used

The following table presents various use cases and the amount to be used. The use case descriptions and specifics are provided in the following sections.

Use Case (refer to sections below)	Authentication (aka AuthE) Amount
Plain vanilla e-commerce	AuthE Amount = Purchase amount
Delayed delivery/charge/free trial	AuthE Amount = Purchase amount
Partial/split shipment	AuthE Amount = Purchase amount + capped partial shipment costs
Agent Model	AuthE Amount = Total amount
Unknown/undefined final amount before Purchase	AuthE Amount = Pre-agreed purchase amount plus the typical margin in business
Recurring payment with fixed amounts	AuthE Amount = Subscription amount (*)
Recurring payment with variable amounts	AuthE Amount = Maximum expected amount of the Recurring Payment Agreement (*)
Recurring payment combined with one time purchase	AuthE Amount = Purchase amount + subscription amount
Instalments	AuthE Amount = Total of all instalments including fees and interest

(*) In case of recurring MITs, an authentication for a zero amount may be used. The Merchant will still need to inform the cardholder about the expected amount in agreement.

A zero amount will reduce the abandonment risk but increase the chargeback risk because the cardholder could claim that the transaction amount was not authorized. An estimate of the final amount may increase the abandonment rate but decrease the chargeback rate.

4.3 Use Cases for In-Session Payments

In-Session Payments are conducted when the Cardholder is available behind his device to perform SCA.

This is including:

- Regular eCommerce transactions
- Delayed Delivery / Charge
- Partial/Split Shipment
- Agent Model
- Unknown Amount before purchase

4.3.2 Delayed Delivery / Charge / Free Trial

This is a use case when for example there is a trial of a product and payment is made after the trial period, or could be a pre-order of a product with payment before delivery.

Global recommendation: Mastercard highly recommends that transaction is authenticated while the Cardholder is in-session and sent to authorization or pre-authorization. Clearing is delayed till the time of delivery of product. This will ensure a smoother process without requiring multiple authorizations or pre-authorizations or holding AAVs for extended periods. If the delay is longer than 7 days or 30 days, respectively applicable for Maestro and Mastercard, then the pre-authorization will need to be extended for another month. This latter process can be repeated if and when needed. As from the second pre-authorization, the AAV will not be included but the Trace ID of the initial pre-authorization will need to be provided.

There is still the option of sending the authorization after the trial period is over (an Account Status Inquiry✪ or ASI in authorization following the authentication may be envisaged). The transaction is fully authenticated, with chargeback protection in case of fraud. A Merchant will need to refresh the AAV when the 30 days retention period has been exceeded and the transaction has not been authorized nor cleared yet.

✪ *An AAV should not be included in the ASI. These transactions may be declined by Issuers. The Merchant has included the AAV in the first authorization message.*

4.3.2 Partial / Split Shipment

This is a use case when for example ordered products are not all available at the same time and the Merchant decides to ship them separately.

Global recommendation: Mastercard highly recommends that the transaction is authenticated for the full amount (purchase amount + capped partial shipment costs) while the Cardholder is in-session and sent to authorization for the full amount. Multiple clearing transactions are sent based on each of the shipments with the proper partial/ final presentment message reason codes. This is in line with the best practices in the Mastercard CIS manual.

When Merchants are from various geographies and only part of the basket is in regulation (e.g. part of the split transaction is within the EEA), then the PSD2 RTS on SCA applies unless an exemption can be leveraged.

4.3.3 Agent Model

This is a use case when for example an agent manages orders of both hotel and airline from different Merchants. The authenticator is the agent but payments are managed by Merchants. In such use cases there will be one authentication but multiple authorizations, one for each of the Merchants.

Note: An agent may occasionally manage payments on-behalf of Merchants.

Global requirement: The AAVs in both authorizations will be the same and must match the AAV in the authentication.

> Void original authorization and reauthorize use case: if an authorization response times out and another authorization is sent for the same transaction, then the AAV from the authentication linked to that transaction should be used.
>
> To avoid expired authorizations, Merchants have to perform pre-authorizations/incremental authorizations to extend the validity period using the Trace ID.

European requirement: Merchant name - Acquirers shall ensure that the Merchant name in authentication and authorization correspond, except for the agent model, where the authentication and purchase is made on a combined site (like a combined travel booking of airline and hotel) but the authorizations are for separate Merchants.

> If and when needed, the Merchant can initiate an authentication request that, when referring to the (SCA) authentication request of the agent, could be managed as an MIT (provided the Cardholder gave a mandate to this end).

> *Note: The name in clearing can be different and should not be changed to comply with current rules.*

European recommendation for dynamic linking: It is recommended that Merchant names in the clearing message contains the agent name and a reference to the individual Merchant(s) of the different transactions so that the transaction can be easily recognized by the Cardholder and dispute resolution is not initiated for transactions not recognized by the Cardholder.

4.3.4 Unknown/undefined final amount before purchase

This is a use case when for example payments are made on a travel turnstile or when fines are assessed after days/ months of car rental. This includes as well examples of groceries where fruits and vegetables are charged per weight or when an ordered item is replaced by a more expensive item.

In such use cases, the Merchant sends an authentication request for the pre-agreed purchase amount plus the typical margin in business.

Global recommendation: If the final transaction amount is higher, then it is recommended that an authentication request be made for the incremental amount.

European recommendation for dynamic linking: The amount in the authentication (pre-agreed purchase amount plus the typical margin in business) will need to be clearly communicated to the Cardholder. The Merchant should display, during checkout, the message

"The Authentication amount has been raised to … to include a margin

This amount has no financial impact on your card account"

> (or similar) to avoid Cardholder confusion and abandonments.

The safety margin should be minimal to prevent the abandonment of the authentication experience in case the incremental amount is prohibitive

4.4 Use Cases for Off-session Payments

Off-Session Payments are conducted when the Cardholder is NOT available behind his device to perform SCA.

This is including:

- Recurrent Payment with fixed amounts
- Recurrent Payment with variable amounts
- Recurring Payment combined with one-time purchase (mixed cart)

- Recurring payment with fixed limit/threshold (individual or corporate)
- Modifiable basket until cut-off
- Decoupled authentication

4.4.1 Recurring Payments

Global requirement: A Recurring Payment shall be indicated by the Merchant by the existing value 02 (=Recurring transaction) in the existing 3DS Requestor Authentication Indicator of the Authentication Request (AReq).

Global recommendation: A Strong Customer Authentication (SCA) for the first transaction of the recurring payments. If SCA is used based on the recommendation above, the 3DS Requestor Challenge Indicator = "04".

Global recommendation: Recurring payments with a variable frequency can set the Recurring Frequency to "1" to indicate that the frequency of payments is not set.

Mastercard's position for Europe:

Position

As of 1 November 2019 for intra-EEA recurring payment Transactions, 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 authorizations to allow the Issuer to validate that Strong Customer Authentication happened on the initial recurring payment authorization, as is required under PSD2 RTS.

If the initial authorization happened before 14 September 2019, then the Trace ID must have the following values:

- Positions 1–3 = "MCC"
- Positions 4–9 = "999999"
- Positions 10–13 = 1231
- Positions 14–15 = blank filled

Alternatively, if the initial authorization happened before 14 September 2019, then the Trace ID can refer to any other authorization belonging to that same recurring payment arrangement provided this authorization took place before 14 September 2019.

As of 1 November 2019, EEA Issuers must be able to process the Trace ID provided in authorizations in DE 48 sub-element 63 (Trace ID), for example to validate if an initial SCA took place to set-up the recurring payment arrangement as required under PSD2 RTS.

European requirement for dynamic linking: For existing Recurring Payments at the PSD2 RTS effective date of 14th September 2019, i.e. Recurring Payments setup before this date, the principle of "grandfathering" will be applied. This means that SCA is applicable to the setup of new Recurring Payments only, i.e. Recurring Payments initiated after the effective date of 14th September 2019.

Grandfathered Recurring Payments will be indicated as follows:

- 3DS Requestor Prior Transaction Reference = DS Transaction ID of the initial Recurring Payment Agreement authentication. This reference is a must to complete the authentication process successfully. All nines ("9") if the agreement was concluded before 14th September 2019.
- DE48 SE63 = Trace ID of the initial Recurring Payment Agreement. This reference is a must to complete the authentication process successfully. The Trace ID includes the Banknet Reference Number (BRN). The BRN will be set to "999999" if the agreement was concluded before 14th September 2019.[2]

The following table indicates the flags to be used for Recurring Payments in the authentication and authorization for the initial transaction in the series and for subsequent ones.

Recurring Payment and MIT for Recurring Payments - Initial Transaction
Bold text highlights items changing between the first transaction and subsequent ones.

Authentication	Authorization
• **Channel = PA (Payment Authentication)** • *3DS Requestor Authentication Indicator* = "02" (Recurring Payment) • ***3DS Requestor Challenge Indicator* ="03" (Challenge requested: 3DS Requestor Preference) or "04" (Challenge requested: Mandate). "04" for regulated markets.** • **3*DS Requestor Prior Transaction Reference* = {empty}** • ***Purchase Amount* = Maximum amount of the Recurring Payment Agreement or zero** • *Recurring Expiry* = Date at which Recurring Payment Agreement needs re-authentication • *Recurring Frequency* = Frequency of the Recurring Payment Agreement (1 when no frequency is set) DS Outcome: DS Transaction ID and AAV	• **DE4 (Transaction Amount) = Authenticated Purchase Amount** • DE22 (POS Entry Mode) = "10" (Card on File) • **DE48 SE22 SF1 not set.** • **DE48 SE42 = 212 or 217** • DE48 SE43 = AAV from authentication (SLI 212) • **DE48 SE63 = {empty}** • DE48 SE66 SF1 = "2" (EMV 3–D Secure (3DS 2.X)) • DE48 SE66 SF2 = DS Transaction ID from authentication • DE61 SE4 = "4" (Standing order/recurring transactions) Authorization Outcome : Trace ID

[2] In between 14th September and 1st November 2019, Issuer shall not decline recurring payment transactions just because the TraceID is absent: it is recommended to consider subsequent recurring payments as grandfathered.

Recurring Payment and MIT for Recurring Payments – Subsequent Transactions
Bold text highlights items changing between the first transaction and subsequent ones.

Authentication (optional)	Authorization
• **Channel = 3RI to indicate the cardholder is off-session as from EMV 3DS 2.2 only. Not available in EMV 3DS 2.1.** Issuers must skip AAV validation if the 3DS Requestor Prior Transaction Reference links to the initial Recurring Payment or MIT Agreement • *3DS Requestor Authentication Indicator* = “02” (Recurring Payment) • ***3DS Requestor Challenge Indicator* = “5” (Acquirer exemption)** • ***3DS Requestor Prior Transaction Reference* = DS Transaction ID for initial Recurring Payment Agreement authentication. All nines (“9”) if before 14th Sep 2019.** • ***Purchase Amount* = Amount not higher than the initial agreement Purchase Amount** • *Recurring Expiry* = Date at which Recurring Payment Agreement needs re-authentication • *Recurring Frequency* = Frequency of the Recurring Payment Agreement (1 when no frequency is set)	• **DE4 (Transaction Amount) = Purchase Amount (not higher than the initial agreement Purchase Amount)** • DE22 = “10” (Card on File) • **DE48 SE22 SF1 = “03” (Recurring Payment Exemption) or “01” (MIT)** • **DE48 SE42 = 212 or 217 (Fully authenticated if Issuer RBA has been used) or 210 (if no subsequent authentication or Acquirer Exemption/MIT). 216 if subsequent authentication and Recurring Payment was requested with Acquirer Exemption or MIT** • DE48 SE43 = AAV from authentication (SLI 212 or 216) • **DE48 SE63 = Trace ID of initial Recurring Payment Agreement. “999999” as Banknet Reference Number if before 14th Sep 2019.**[3] • DE48 SE66 SF1 = “2” (EMV 3–D Secure (3DS 2.X)) (SLI 212 or 216) • DE48 SE66 SF2 = DS Transaction ID from authentication (SLI 212 or 216) • DE61 SE4 = “4” (Standing order/recurring transactions)

4.4.2 Instalments

EMV 3DS specifications considers Instalments as a special case of Recurring Payment where the amount and frequency are fixed and limited in time (Recurring Frequency not set to “1”).

Such specification does not align with the Mastercard Rules where Instalments must have following characteristics:

- Authorization must be unique and for the full amount of the transaction. Issuers need to manage the open-to-buy of cardholders taking the instalments into account.
- Clearing occurs per instalment payment

Consequently, the amount of the authentication will be the total amount of the purchase or sum of all instalments, including fees and interest.

[3] In between 14th September and 1st November 2019, Issuer shall not decline recurring payment transactions just because the TraceID is absent: it is recommended to consider subsequent recurring payments as grandfathered.

4.4.3 Decoupled Authentication

This section is provided for information only. The decoupled authentication feature is not yet available. Mastercard will communicate in future announcements as of when this feature can be used.

It may happen that, in a challenge situation, Issuers want to reach out to authenticate their Cardholder outside of the EMV 3DS message flows. Use cases are:

- Where SCA may be required when the Cardholder is off-session (recurring payments for variable amounts, authorization amount is above authentication amount and an authentication for the difference is needed).
- For Mail Order/Telephone Order (MOTO) transactions. Refer to section on "Mail Order / Telephone Order (MOTO)".

The EMV 3DS 2.2 specifications support decoupled authentications.

In a typical decoupled authentication, the following flow will apply:

- The Merchant initiates an Authentication Request (AReq) indicating they would like to perform a decoupled authentication with the maximum timeout allowed e.g. 1 week).
- The Issuer responds back indicating they support decoupled authentication for their Cardholders or not.
- If this Issuer does, it authenticates the Cardholder outside the normal Challenge Request/Challenge Response (CReq/Cres) flow.
- Upon authentication, the Issuer sends the results back via the Results Request (RReq) message
- The Merchant confirms with the Results Response (RRes).

Before the authentication window times out, the recommended user experience is for Issuers to attempt strong customer authentication via authentication app with push notification or email. Several attempts may be required in the allowed authentication window.

As the Cardholder will be off-session and the authentication will be decoupled, it is important that the Cardholder is given all necessary recognizable data elements (Merchant name, incremental transaction amount, reasons for additional authentication) that will allow him to go through the authentication process seamlessly.

Section 5 - Specific requirements under PSD2

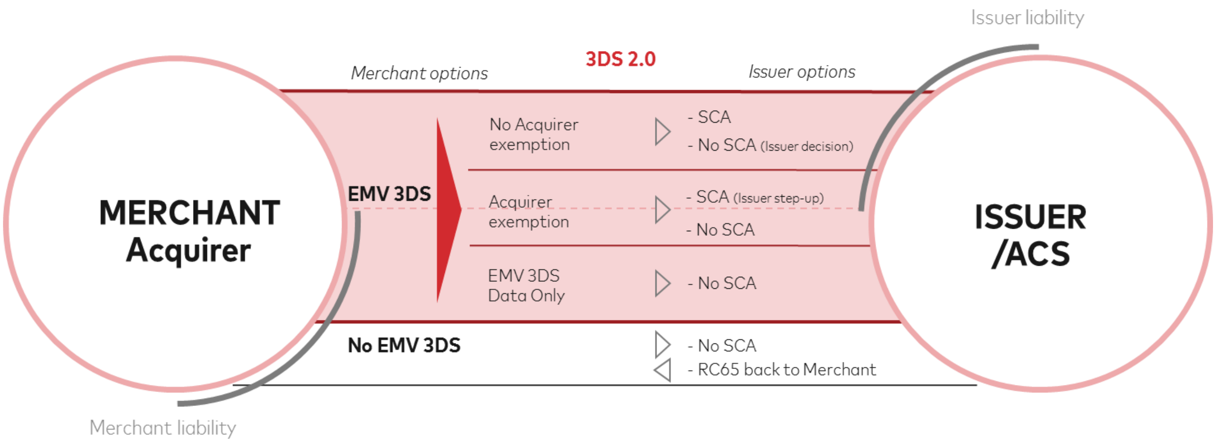
5.1 When to apply SCA?

SCA will need to be applied as per PSD2 RTS requirements. SCA will be required when:

- The transaction is not out of scope of the PSD2 RTS
- No PSD2 SCA exemption applies for a payment transaction
- Adding a card to a Merchant's file (card-on-file)
- Starting a recurring payment arrangement for fixed and variable amounts, including setting the initial mandate for Merchant-Initiated Transactions
- Changing a recurring payment agreement for a higher amount (premium offering for example)
- Setup of white-listing (or viewing/amending white-lists)
- Binding a device to a Cardholder

In all other scenarios the Issuer will always have the final word to apply SCA. Mastercard recommends that, risk permitting, Issuers offer a frictionless consumer experience when SCA is not required by regulation.

Mastercard will be offering all possible authentication combinations to satisfy Issuers and Acquirers needs. The following diagram depicts options available at the Merchant side as well as at the Issuer side, compatible options as well as where liability lies under PSD2 RTS requirements.



In the case of Whitelisting, the Merchant will not know in advance if it is Whitelisted (or if it has been removed from the Cardholder's Merchant whitelist). The Merchant should therefore, systematically initiate the EMV 3DS flow as if SCA would apply.

5.2 Dynamic Linking requirements and AAV validation

The Merchant name and authentication amount have to be shown to the Cardholder during the authentication experience, on the Merchant page (controlled by the 3DS Server) and on the authentication page (controlled by the ACS). The information is available in the EMV 3DS AReq message with MerchantName and purchaseAmount.

When the RTS comes into force in September 2019, Dynamic Linking will be required: the authentication code (AAV) has to be linked to Merchant (e.g Merchant name) and authentication amount.

> This requires the Merchant in authentication and authorization to correspond for a strict interpretation of the PSD2 SCA dynamic linking requirements (refer to section on "Merchant Names"). The Merchant and its name in clearing can be different and should not be changed to comply with current rules.

Mastercard is aware that current business and industry practices do not always allow for such linking of the merchant name and amount. A request has been raised with the European Banking Authority (EBA) to allow the use of the Directory Server Transaction ID to achieve the linking instead of merchant and amount. So far, no response has been received and in order to allow Customers and partners to prepare for the September 14 implementation date of PSD2, Mastercard is advising the following position in regards to Dynamic Linking and AAV validation.

Mastercard's own AAV Validation Service will perform AAV validation and matching based on the use of the Directory Server Transaction ID will not validate based on Merchant, in recognition of the risk that in today's environment the Merchant name and amount may vary between authentication and authorization. Such a difference in these elements could lead to the AAV validation failing and causing a decline in valid transactions.

Therefore, the Mastercard On-Behalf AAV Validation Service will perform AAV validation based on the DS Transaction ID and will also inform the issuer how the amount in the authorization compares to the amount in the authentication (lower or the same, higher by up to 20%, higher than 20%).

Mastercard recommends that for Issuers who perform AAV validation on their side, to recognize that if the AAV contains Merchant name and amount, that these elements may cause the AAV validation to fail due to differences in these items between authentication and authorization. Therefore, Issuers are recommended to use the SPA 2 AAV Validation method based on DS Transaction ID combined with a validation of the amount as the main reference and not based on Merchant.

The above requirements are temporary steps to ensure that valid transactions are not declined due to issues with Merchant names and amount. Going forward in order to ensure that Merchant names match in both authentication and authorization, Mastercard will introduce a rule with compliance required by 1 July 2020 that merchant names used in authentication must uniquely identify a merchant.

In some cases, the authorization amount will be below the authentication amount.

The process is the following:

1. During authentication, a unique DS Transaction ID is generated by Mastercard and provided to both Issuer's ACS and the Merchant.
   The Issuer's ACS generates an IAV, a cryptogram, to confirm that the authentication was approved.
2. The Merchant provides the DS Transaction ID with the AAV in the authorization message.
3. **Self-validation by the Issuer**: The Issuer can self-validate Dynamic Linking during authorization processing with potential following recommended approaches.
   The Issuer then calculates the part of the AAV called IAV using the same formula, method and encryption keys as originally calculated by the ACS:
   a) Either both ACS and Issuer calculate the IAV using the Merchant name and authorization amount provided respectively in the authentication and authorization message. The Issuer then compares the resulting IAV with the IAV provided in the authorization message as part of the AAV.
      If the IAV does not match, this could be due to the amounts and/or Merchant name being different from the authentication vs. authorization. In this case the Issuer will need to compare the amount and Merchant

name from authentication to authorization and determine the potential variance between both.

b) Or both ACS and Issuer calculate the IAV using blanks for Merchant name and zeroes for the authorization amount. The Issuer then compares the resulting IAV with the IAV provided in the authorization message as part of the AAV.
If the IAV then does not match this indicates that the IAV used in the authorization is likely not originating from the corresponding authentication message. If the IAV does match the Issuer will need to compare the amount and Merchant name from authentication to authorization and determine the potential variance between both.

c) Comparing the amount and Merchant name between authentication and authorization messages can be accomplished with the DS Transaction ID provided in the authorization message since it was also previously provided to the ACS during the authentication. It will require the Issuer's authorization system to have a direct real-time connection to the ACS to retrieve the authentication message that can then be compared to the authorization message.
An alternative to c) is for Issuers to use the on-behalf AAV validation service offered by Mastercard.
Mastercard cannot validate the IAV. It is up to the Issuer to comply with the PSD2 RTS on SCA for dynamic linking. For example, Issuers may calculate the IAV based on the Primary Account Number (PAN), DS Transaction ID and amount. This requires the DS Transaction ID to be populated by the Acquirer, which explains why the DS Transaction ID is conditional, i.e. mandated if the Acquirer is in the EEA.

d) When comparing the amount, the Issuer should also ensure that the authentication amount is not lower than the authorization amount, or the sum of the authorization amounts relating to the same DS Transaction ID.

4. **On-behalf AAV validation service** by Mastercard.

Self-validation by Issuers may be challenging for different reasons:

- Different existing industry business and technical models make it difficult to impossible to meet the requirement that the Merchant name and the amount in authentication and authorization must correspond.
- Issuers may experience delays in getting ready with EMV 3DS and PSD2 RTS due to complexity of the IAV validation and the requirement to exchange keys with their ACS.

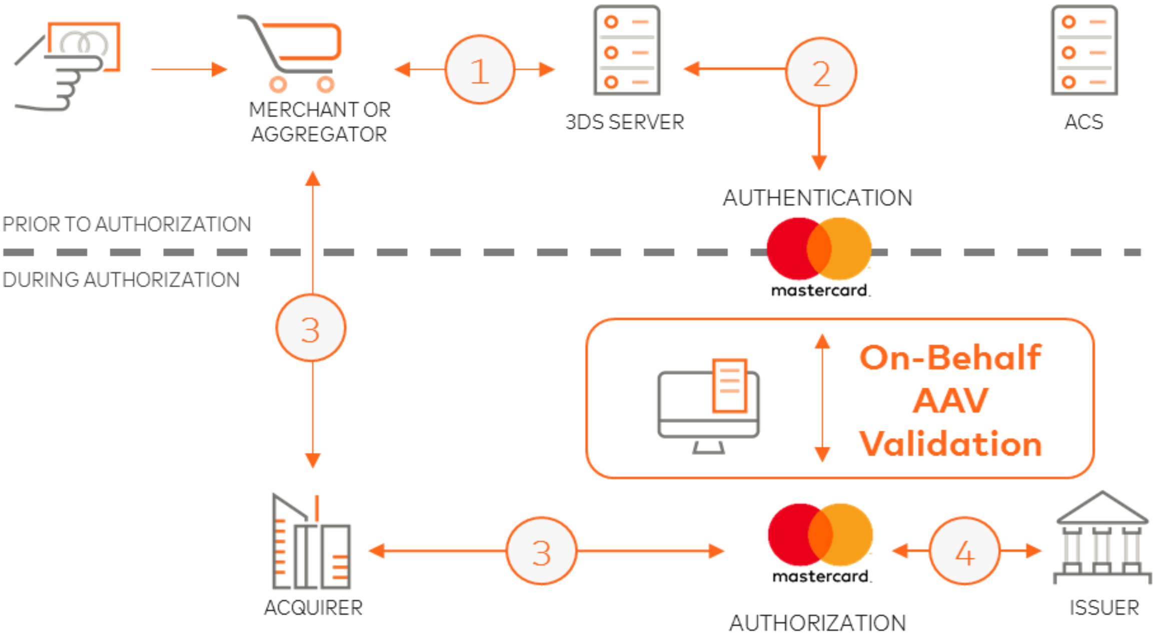
- Many Issuers do not have a real-time on-line connection to their ACS Service to access Authentication Data.

Mastercard is ideally placed to stand-in:

- Mastercard on-behalf AAV validation service is using its own keys and does not require any key exchange.
- The Mastercard authentication and authorization networks are residing on connected platforms allowing easy and fast data matching and comparison.

With the above argument in mind, Mastercard has suggested the following clarification to the PSD2 RTS on SCA:

> "For remote transactions, if the transaction amount and/or the Merchant's name differs between authentication and authorization, the dynamic link requirement is complied with if the Issuer matches and validates the authentication code generated during authentication with the code sent in authorization."



The Mastercard on-behalf AAV validation service has been adapted so that:

Via the DS Transaction ID, Mastercard:

- Retrieves the AAV generated by the ACS during authentication and matches it to the AAV in the authorization message.
- Compares the authentication and authorization amounts.

- Provides the outcome of the above matching and comparison processes to the Issuer in the authorization message:
    - Match with lower amount
    - Match with equal amount
    - Match with amount within an acceptable tolerance
    - No Match

If the DS Transaction ID (despite a mandate to provide it) is not provided, then the on-behalf AAV validation will attempt to match the authentication with the authorization based on the AAV and card number. The matching rate will be around 80% meaning that the validation will be flagged as of lower quality.

5.3 Fraud level calculation

For the Mastercard Identity Check™ Program KPIs, target fraud rates will be reviewed annually based on program performance and may be adjusted to actual market needs throughout the program. Every Issuer must report its Mastercard fraud data to the System to Avoid Fraud Effectively (SAFE).

For the PSD2 RTS, the methodology and any model used to calculate the fraud rates as well as the fraud rates themselves, shall be adequately documented and made fully available to the EBA and local competent authorities.

Refer to the RTS for the methodology and reporting requirements relating to RTS/SCA fraud rates as discussions are still ongoing. The following elements are considered:

- The fraud rate is based on electronic remote card-based payment transactions, i.e. CNP transactions, in the EEA region (two-leg transactions) but excludes as per the PSD2 RTS:
    - Mail Order/Telephone (MOTO) transactions
    - Anonymous prepaid card transactions
    - Merchant-Initiated Transactions (MITs)
    - Friendly frauds
- Acquirer fraud data will be provided by Mastercard through SAFE reports. SAFE reported data only includes fraud data for Mastercard branded cards. The breakdown of the information will allow Acquirers to filter CNP minus MOTO transactions and get gross fraud rates.
- As suggested in the EBA Opinion document, gross fraud rates should be provided (i.e. including fraud caused by an exemption applied by the other PSP). The fraud rate is the gross amount of fraudulent transactions meeting the above criteria divided by the gross amount of transactions meeting again the same above criteria.

- Refer to the Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2): "Guidelines on fraud reporting under Article 96(6) PSD2 (EBA-GL-2018-05)".

  Refer to the following document for more information on SAFE reports made available to Acquirers on a daily basis: ***"SAFE Product User Guide" (10 May 2016)***

  available in the Publications section of Mastercard Connect for information on SAFE reported data and specifications.

As PSD2 RTS will inevitably decrease fraud levels at the Issuer side, Issuer fraud prevention tools (neural, rule-based) should be retrained or be revisited (rules and thresholds) to accommodate the improved environment.

5.3.1 Fraud types

Two new fraud types will be added to the Fraud & Loss Database in September 2019 to comply PSD2 fraud types:

- Modification of payment details
- Manipulation of the Cardholder

5.4 Transaction monitoring

The PSD2 RTS' Article 2 specifies that Payment Service Providers (PSPs) shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions.

Risk-based factors that should be taken into account include:

- lists of compromised or stolen authentication elements;
- the amount of each payment transaction;
- known fraud scenarios in the provision of payment services;
- signs of malware infection in any sessions of the authentication procedure;
- in case the access device or the software is provided by the PSP, a log of the use of the access device or the software provided to the Cardholder and the abnormal use of the access device or the software.

EMV 3DS with Transaction Monitoring data and solutions (including device data linked to fraud) will facilitate the compliance with the PSD2 RTS. Alternative technical solutions may also be used.

Section 6 - Authentication Services

Mastercard will offer to its Customers a number of authentication services to help them comply with the PSD2 RTS requirements.

6.1 Digital Transaction Insights

EMV 3DS is allowing ecommerce Merchants to share a wealth of Cardholder data that they may be collecting during the purchasing process. Through Authentication, Issuers may be taking the appropriate decision to challenge or authenticate based on a risk-based decision.

Mastercard Digital Transaction Insights enables Issuers to receive an assurance level assessment of this Cardholder data from Mastercard during the authorization process. By facilitating the exchange and normalization of consumer account and device data provided by participating Merchants in EMV 3DS, Mastercard Digital Transaction Insights helps give Issuers a level of assurance that consumers are transacting using attributes—such as account, device, and IP address, for example—that are typically associated with them.

It is recommended that these Digital Transaction Insights are used by the Issuer's fraud prevention tool to reduce fraud and false declines.

The Digital Transaction Insights service will rely on the DS Transaction ID to match the authorization to the authentication. However, if the DS transaction ID is not provided, the service will still be able to perform the matching. In this latter case, the matching rate is around 80%.

The Digital Transaction Insights are delivered to an Issuer in two distinct fields:

- a risk assessment with a value from 0 to 9 (zero representing lowest risk)
- a reason code with a value from A to Z (A representing highest risk)

As Merchants coming on board of EMV 3DS are only expected to be fully migrated at the earliest by September 2019, Issuers should use this migration period to learn from the assessment and build fraud rules on the analysis results. Ad interim, Issuers may find the reason code most useful as it gives a concrete indication of the risk condition that is being identified.

Refer to the following document for more information on this topic: ***AN 2122 - Introduction of Mastercard Digital Transaction Insights Service***

6.2 Smart Authentication for Issuer/ACS

This service – previously known as ACS RBA - is available to Issuer's ACS services when receiving EMV 3DS authentication requests.

There may be instances where the Issuer's ACS services have limited to no risk scoring capabilities. For those Issuers, Mastercard will provide a risk score in the authentication request towards the ACS service by applying a risk scoring model.

The ACS service will then be able to apply the risk score in its authentication experience to determine whether or not an authentication challenge is required, i.e. to apply risk-based authentication.

This Risk Scoring for Authentication service is available for all European – regulated or non-regulated - Issuers.

The Smart Authentication for Issuers risk assessment is delivered to an Issuer in three distinct fields:

- a risk assessment decision categorizing an authentication as low vs. not low risk
- a risk assessment with a value from 000 to 950 (zero representing lowest risk)
- a reason code with a value from A to Z (A representing highest risk)

ACS services may either use the risk assessment decision as input to their risk-based authentication process or they can use the risk assessment to make their own decision of what value to use as delimitation of low vs. not low risk transactions.

Refer to the following document for more information on this topic*:* ***AN 2036—Revised Standards—Mastercard Introduces Access Control Service Risk Based Authentication and Stand-In Risk Based Authentication Service***

6.3 Smart Authentication Stand-In

This service – previously known as Stand-In RBA - is available to Issuers when being provided with EMV 3DS authentication requests. For 3DS 1.0.2 authentication requests Mastercard will continue offering the Attempts Server service.

There may be instances where the Issuer's ACS services cannot be reached such as during temporary outages or connectivity issues, or when a card range or individual card is not enrolled in the Mastercard Identity Check™ Program. In such situations, Mastercard will provide an authentication response on behalf of the ACS/Issuer by applying its authentication risk scoring model.

Issuers in the EEA will be automatically opted-in on 18 October 2019, with opt-out option, for a purchase amount up to 30 EUR. In 2020, Mastercard may enhance the authentication stand-in service to include Issuer TRA exemptions with a mechanism for Issuers to provide Mastercard with their maximum amount (100 EUR, 250 EUR or 500 EUR) up to which stand-in can be performed.

When the risk is low and the purchase amount does not exceed the service maximum amount (initially 30€), an approved authentication response will be returned to the Merchant or PSP with fully authenticated AAV. When the risk is high or the purchase amount exceeds the service maximum amount (initially 30€), or the card is not enrolled in EMV 3DS, an Attempt authentication response will be returned to the Merchant or PSP with Transaction Status = "A". In this case trying again with a 3DS1 authentication is likely to be approved, which leads to higher authorization approval rates.

Issuers in the EEA will be automatically opted-in on 18 October 2019 to the on-behalf AAV validation, as only in the on-behalf validation service the Smart Authentication Stand-In generated AAV can be validated.

The existing fraud chargeback protection for e-commerce merchants that use SecureCode will also apply for transactions using Mastercard Identity Check / EMV 3DS authentications in EEA as of 1 October 2019.

Issuers in non-regulated markets in HGEM and Switzerland will be automatically opted into the standard Stand-In Authentication service at the time of their migration to EMV 3DS and the Mastercard Identity Check™ Program.

Refer to announcements AN-1376 and AN-1396 for a complete overview of roadmap milestones and effective dates for these markets. As of 1 October 2019, for Issuers in High Growth Emerging Markets✪ and Switzerland, the Stand-In

Authentication service will be turned on for all remaining Issuers and will replace the Attempts Server service.

✪ Refer to the Appendix-A and Appendix-B for the list of concerned markets.

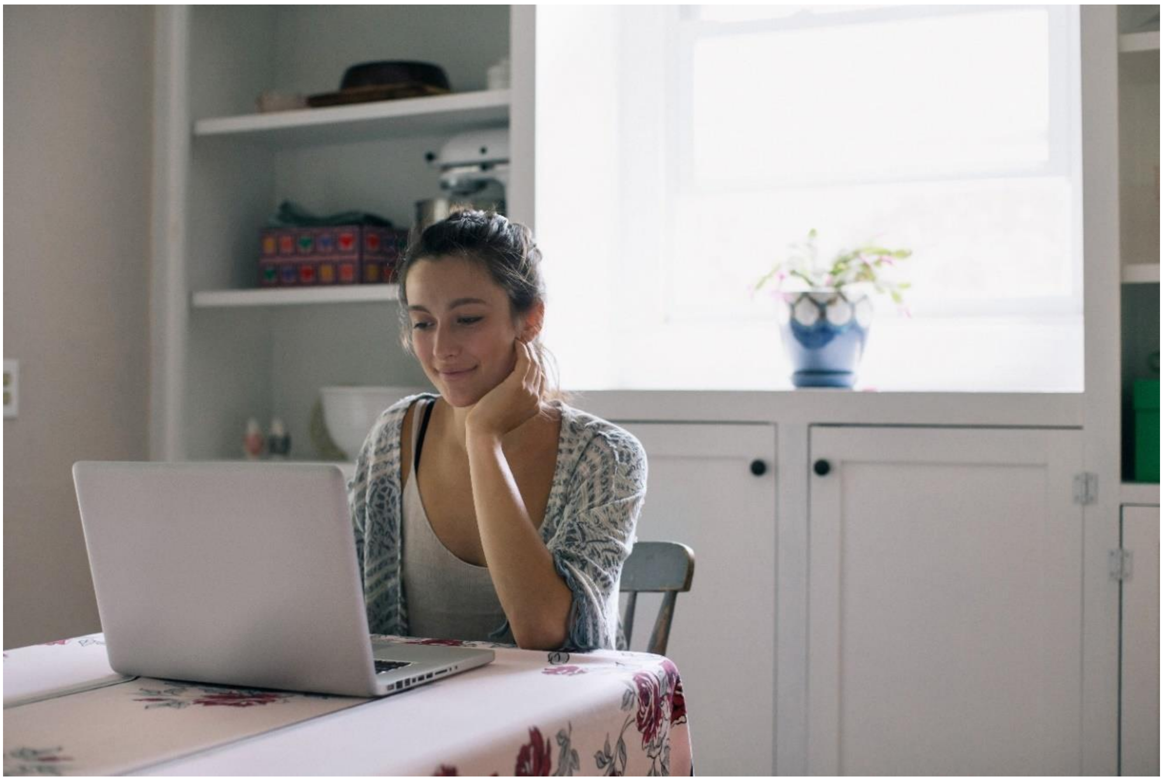
Refer to the following document for more information on this topic: ***AN 2036—Revised Standards—Mastercard Introduces Access Control Service Risk Based Authentication and Stand-In Risk Based Authentication Service***

6.4 AAV Validation Service

Evolving fraud patterns have highlighted the vulnerability of Issuers when transactions are processed in Stand-In without applicable validation services. Issuers continue to experience fraud losses resulting from the lack of on-behalf AAV validation services. MasterCard offers an on-behalf AAV validation service both as pre-validation (i.e. the AAV is pre-validated for all authorizations sent to the Issuer authorization system) and stand-in service (i.e. the AAV is validated only during stand-in authorization processing)

Since 1 April 2017 MasterCard mandates AAV validation either by the Issuer (self-validation) or by Mastercard.

Refer to the following document for more information on this topic: ***AN 1085 — AAV Validation for EMV 3-D Secure***



Section 7 - User Experience (UX)

The Strong Customer Authentication EMV 3DS 2.1.0 User Experience Recommendations have been captured in a document that can be accessed through the Publications section of Mastercard Connect:

https://w201.mastercardconnect.com/hsm3ca267/homememb/library/shared/ENG/CATDS/CATDS_Manual.pdf

Section 8 - Implementation considerations

This document is not intended to provide information on the implementation or onboarding processes and tools.

Refer to the following documents for more information on this topic.

- Mastercard Identity Check™ Onboarding Guide for 3-D Secure Service Providers, Operators, Issuers, and Processors (20 September 2018)
- Mastercard Identity Check™ Onboarding Guide for Acquirers, Merchants, and 3DS Service Providers (20 September 2018)

Merchants on the acquiring side as well as BINs or card ranges on the issuing side will be setup in Mastercard's DS by associating them respectively to their 3DS Server and ACS. 3DS Servers and ACS's will receive their DS Originator ID at the end of the Mastercard Identity Check™ Compliance Testing.

Besides, as the Merchant name will be critical between the authentication and the authorization, it is important that Merchants and Acquirers make sure that Merchant names are unique, consistent and as descriptive/representative as possible.

8.1 Identity Solutions Service Manager (ISSM)

The ISSM tool is available since Q4-2018. It allows Issuers or ACS's to enable and setup their card ranges and Acquirers to enable and setup their Merchants for the Mastercard Identity Check™ Program.

On the Acquirer side, the Merchant name with Merchant Category Code (MCC) and country code are captured. This ensures consistency in Merchant names and allows some edits and alerts during the data entry. For example:

- Mastercard will alert the entry by different Acquirers of an existing Merchant name in a specific country.
- Mastercard will alert when an existing Merchant name is used in a specific country but by another Acquirer. The existing Merchant and the Merchant being entered should be contacted to confirm the entry.
- Mastercard will alert when an existing Merchant name is used in a different country. The existing Merchant should be contacted to confirm the entry.

Acquirers should be aware that the setup of their Merchants needs to be carefully managed to avoid potential identification issues. Acquirers will be able to perform extracts of existing ISSM combinations for their Merchants. The tool aims at reaching better quality in the identification of players in the authentication value chain. It also facilitates meeting some of the PSD2 RTS requirements on SCA, such as Dynamic Linking requirements.

Section 9 Authentication Quality and Key Performance Indicators

Mastercard is updating the Data Integrity Monitoring Program with new edits to monitor cardholder authentication through EMV® 3-D Secure (3DS), and fully authenticated transactions. Mastercard will also leverage a new feature of the Data Integrity Online application on Mastercard Connect™ to send Data Integrity related alerts and notifications to customers.

Data Integrity Monitoring is a Global program, however in many countries in Europe several KPIs (mainly the “quality” related ones like approval/abandonment etc) are already being monitored via Ecommerce Quality Funds. If that is the case, it will be clearly indicated in the Data Integrity announcements which countries are excluded for a specific KPI. As a result, the Data Integrity Monitoring program will then rather contain “technical” KPIs like authentication error rates, system availability etc.

The Data Integrity Monitoring Program will begin monitoring cardholder authentication messages using the EMV 3-D Secure protocol as well as fully authenticated 3DS transactions via new edits. These will get announced in phases, with first phase via AN 2401 (compliance data available April 2019, comply by date of 1 September 2019, and assessments for noncompliant customers will begin 1 October 2019 for the previous month's data). All next phases will have a later noncompliance assessment date in 2020.

Adding these additional validations will help ensure that the 3DS product is performing as designed and that consumers can enjoy both increased confidence in the security of their transactions and an efficient payment process. As a result, customers should see an improved cardholder experience with higher approval rates on card-not-present transactions and fewer chargebacks. The new edits will monitor Issuers and Acquirers.

In all cases, customers must be actively participating in a 3DS program and have at least 1,000 3DS transactions in a given month to be monitored.

Additionally, Mastercard is considering to send notification letters to:

- Issuers that don't support 3DS (1 nor 2)
- Customers whose ACS/3DS servers are not yet certified for EMV 3DS
- Key Acquirers for their top Ecom Merchants that never send 3DS

Section 10 - Marketing, Education and Communication

Mastercard has developed a holistic Education Plan regarding PSD2/SCA requirements and Mastercard Identity Check™.

Next to numerous B2B initiatives like webinars, workshops, white papers etc., Mastercard is also playing a role in enabling stakeholders (Issuers and Merchants) to communicate to cardholders and ensure consistent messaging.

The Europe region developed materials like a video, a Merchant FAQ, an infographic, a communication toolkit etc. which are being customized for the respective markets.

Please contact your local representative for more information on this and to get access to these materials.

Section 11 - References: what should Customers have already read on the subject?

11.1 Publications other than Bulletins and Announcements:

- EMV 3DS - Frequently Asked Questions
- EMV 3DS Protocol and Core Functions Specification – Version 2.2.0. (December 2018)
- Mastercard Identity Check™ Program Guide (30 October 2018)
- Mastercard Identity Check™ Onboarding Guide for 3-D Secure Service Providers, Operators, Issuers, and Processors (20 September May 2018)
- Mastercard Identity Check™ Onboarding Guide for Acquirers, Merchants, and 3DS Service Providers (20 September 2018)
- Mastercard SecureCode and Mastercard Identity Check™ - Compliance and Functional Test Facility Policies Procedures
- SPA2 AAV for the Mastercard Identity Check™ Program
- Mastercard Biometric Authentication—Europe Region (11 January 2018)
- Consumer Device Cardholder Verification Authentication Method Requirements (March 2018)
- Consumer Device Cardholder Verification Authentication Method Requirements and Evaluation Program (July 2017)
- Mastercard Standards for Merchant Whitelisting v0.1 (May 2018)

11.2 Operations Bulletins:

- (Global) Jan-16 - Best Practices for E-Commerce – Update
- (Global) Jan-16 - Best Practices for Lodging, Vehicle Rental, and Cruise Lines – Update
- (Global) Nov-16 - Global Safety and Security Standards Roadmap
- (Global) Nov-16 - Announcing Mastercard Identity Check™ Authentication Program
- (Global) Nov-16 - EMV 3DS—Upgrading the Technology behind Mastercard SecureCode and Mastercard Identity Check™
- (Global) Nov-16 - Guidance on Testing Procedures for EMV 3D Secure Software
- (Global) Nov-16 - AAV Validation Requirement for All SecureCode and Mastercard Identity Check™ Transactions

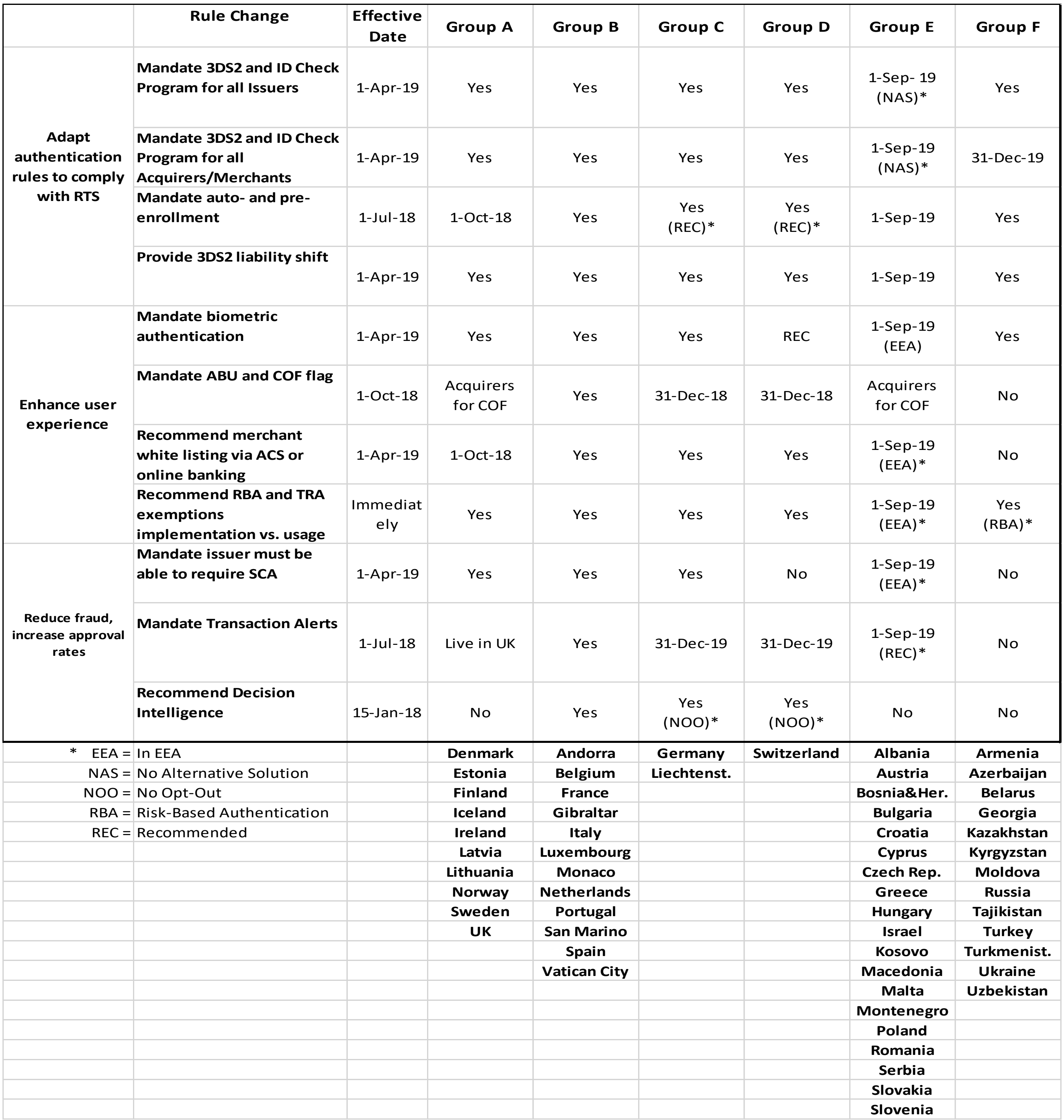
- (Global) Jan-17 - Self-Validation AAV Process for SecureCode or Identity Check™ Issuers
- (Global) Mar-17 - Global Safety and Security Standards Roadmap—Reminder
- (Global) Apr-17 - AAV Validation Requirement for All SecureCode and Mastercard Identity Check™ Transactions – Clarification
- (Global) Aug-17 - 3-D Secure 2.0 and Identity Check™ Program Update

11.3 Announcements:

- AN 1085 - AAV Validation for EMV 3-D Secure
- AN 1121 - Revised Standards—Credential-on-File and Recurring Payments Transactions
- AN 1163 - Digital Safety and Security Standards Roadmap
- AN 1165 - Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update
- AN 1218 - Mastercard Identity Check™ Program with EMV 3-D Secure (EMV 3DS) Rollout
- AN 1365 - Revised Safety and Security Standards Roadmap for Germany and Liechtenstein
- AN 1366 - Revised Safety and Security Standards Roadmap for Switzerland
- AN 1371—Mastercard Identity Check Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Germany and Liechtenstein
- AN 1376 - Mastercard Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Switzerland
- AN 1396 - Mastercard Identity Check™ Program and EMV 3-D Secure Update in High Growth European Market Countries
- AN 1533 - Revised Safety and Security Standards Roadmap for Select Countries in Central and Eastern Europe
- AN 1534 - Digital Safety and Security Standards Roadmap for the United Kingdom, Ireland, Nordics, and Baltics
- AN 1544 – Mastercard Identity Check™ Program and EMV 3-D Secure Version 2 (EMV 3DS) Update for Select Countries in the Europe Region
- AN 1630 - AAV Verification Service Enhancement
- AN 1803 - Acquirer Exemptions for Strong Customer Authentication under PSD2 and the RTS
- AN 1854 - Guidance on Implementing Mastercard Authentication Secure Hash Algorithm - 2 Certificates
- AN 2005 - Mastercard Identity Check™ Program Update

- AN 2051 - Contactless One-Tap PIN Request for Exemption Under PSD2 RTS Article 11
- AN 2113 - Enhancements to AAV Validation for EMV 3-D Secure
- AN 2122 - Introduction of Mastercard Digital Transaction Insights Service
- AN 2261 - EMV 3DS Compliance Plan and User Experience Review Process for the CEE Countries
- AN 2288 - Data Integrity Monitoring Program - New Edits to Monitor Use and Acceptance of Credential-On-File Indicator
- AN 2401- Data Integrity Monitoring Program - New Edits for EMV 3-D Secure and New Alerts and Notifications Feature
- AN 2509 - Announcing the Prepaid Anonymous Indicator ("Anonymous Indicator")
- AN 2606 - Enhancements to Support Contactless Tracking with Single Tap and PIN Request
- AN 2609 - Enhancements to Support the Low-Risk Transaction Indicator for EEA Customers

Section 12 - Appendix-A: Mastercard's Digital Security Roadmap



	Rule Change	Effective Date	Group A	Group B	Group C	Group D	Group E	Group F
Adapt authentication rules to comply with RTS	Mandate 3DS2 and ID Check Program for all Issuers	1-Apr-19	Yes	Yes	Yes	Yes	1-Sep- 19 (NAS)*	Yes
	Mandate 3DS2 and ID Check Program for all Acquirers/Merchants	1-Apr-19	Yes	Yes	Yes	Yes	1-Sep-19 (NAS)*	31-Dec-19
	Mandate auto- and pre-enrollment	1-Jul-18	1-Oct-18	Yes	Yes (REC)*	Yes (REC)*	1-Sep-19	Yes
	Provide 3DS2 liability shift	1-Apr-19	Yes	Yes	Yes	Yes	1-Sep-19	Yes
Enhance user experience	Mandate biometric authentication	1-Apr-19	Yes	Yes	Yes	REC	1-Sep-19 (EEA)	Yes
	Mandate ABU and COF flag	1-Oct-18	Acquirers for COF	Yes	31-Dec-18	31-Dec-18	Acquirers for COF	No
	Recommend merchant white listing via ACS or online banking	1-Apr-19	1-Oct-18	Yes	Yes	Yes	1-Sep-19 (EEA)*	No
	Recommend RBA and TRA exemptions implementation vs. usage	Immediately	Yes	Yes	Yes	Yes	1-Sep-19 (EEA)*	Yes (RBA)*
Reduce fraud, increase approval rates	Mandate issuer must be able to require SCA	1-Apr-19	Yes	Yes	Yes	No	1-Sep-19 (EEA)*	No
	Mandate Transaction Alerts	1-Jul-18	Live in UK	Yes	31-Dec-19	31-Dec-19	1-Sep-19 (REC)*	No
	Recommend Decision Intelligence	15-Jan-18	No	Yes	Yes (NOO)*	Yes (NOO)*	No	No
* EEA =	In EEA		Denmark	Andorra	Germany	Switzerland	Albania	Armenia
NAS =	No Alternative Solution		Estonia	Belgium	Liechtenst.		Austria	Azerbaijan
NOO =	No Opt-Out		Finland	France			Bosnia&Her.	Belarus
RBA =	Risk-Based Authentication		Iceland	Gibraltar			Bulgaria	Georgia
REC =	Recommended		Ireland	Italy			Croatia	Kazakhstan
			Latvia	Luxembourg			Cyprus	Kyrgyzstan
			Lithuania	Monaco			Czech Rep.	Moldova
			Norway	Netherlands			Greece	Russia
			Sweden	Portugal			Hungary	Tajikistan
			UK	San Marino			Israel	Turkey
				Spain			Kosovo	Turkmenist.
				Vatican City			Macedonia	Ukraine
							Malta	Uzbekistan
							Montenegro	
							Poland	
							Romania	
							Serbia	
							Slovakia	
							Slovenia	

Section 13 - Appendix-B: Reference announcements for all countries in Europe

Country Name EEA Overseas in red	If EEA, Country	Division (Long)	Division (short)	If EEA, Currency non EUR in red	AN...
Aland Islands	ALA-248	UK&Ireland, Nordics&Baltics	UKINB	EUR-978	
Albania		Central Eastern Europe	CEE		1533
Andorra		Western Europe	WE		1163
Armenia		High Growth Emerging Markets	HGEM		1396
Austria	AUT-040	Central Eastern Europe	CEE	EUR-978	1533
Azerbaijan		High Growth Emerging Markets	HGEM		1396
Belarus		High Growth Emerging Markets	HGEM		1396
Belgium	BEL-056	Western Europe	WE	EUR-978	1163
Bosnia& Herzegovina		Central Eastern Europe	CEE		1533
Bulgaria	BGR-100	Central Eastern Europe	CEE	BGN-975	1533
Croatia	HRV-191	Central Eastern Europe	CEE	HRK-191	1533
Cyprus	CYP-196	Central Eastern Europe	CEE	EUR-978	1533
Czech Republic	CZE-203	Central Eastern Europe	CEE	CZK-203	1533
Denmark	DNK-208	UK&Ireland, Nordics&Baltics	UKINB	DKK-208	1534
Estonia	EST-233	UK&Ireland, Nordics&Baltics	UKINB	EUR-978	1534
Finland	FIN-246	UK&Ireland, Nordics&Baltics	UKINB	EUR-978	1534
France	FRA-250	Western Europe	WE	EUR-978	1163
French Guiana	GUF-254	Western Europe	WE	EUR-978	
Georgia		High Growth Emerging Markets	HGEM		1396
Germany	DEU-276	Germany&Switzerland	G&S	EUR-978	1365
Gibraltar	GIB-292	Western Europe	WE	GIP-292	1163
Greece	GRC-300	Central Eastern Europe	CEE	EUR-978	1533

Country Name EEA Overseas in red	Country	Division (Long)	Division (short)	If EEA, Currency non EUR in red	AN...
Guadeloupe	GLP-312	Western Europe	WE	EUR-978	
Hungary	HUN-348	Central Eastern Europe	CEE	HUF-348	1533
Iceland	ISL-352	UK&Ireland, Nordics&Baltics	UKINB	ISK-352	1534
Ireland	IRL-372	UK&Ireland, Nordics&Baltics	UKINB	EUR-978	1534
Israel		Central Eastern Europe	CEE		1533
Italy	ITA-380	Western Europe	WE	EUR-978	1163
Kazakhstan		High Growth Emerging Markets	HGEM		1396
Kosovo		Central Eastern Europe	CEE		1533
Kyrgyzstan		High Growth Emerging Markets	HGEM		1396
Latvia	LVA-428	UK&Ireland, Nordics&Baltics	UKINB	EUR-428	1534
Liechtenstein	LIE-438	Germany&Switzerland	G&S	CHF-756	1365
Lithuania	LTU440	UK&Ireland, Nordics&Baltics	UKINB	EUR-978	1534
Luxembourg	LUX-442	Western Europe	WE	EUR-978	1163
Macedonia		Central Eastern Europe	CEE		1533
Malta	MLT-470	Central Eastern Europe	CEE	EUR-978	1533
Martinique	MTQ-474	Western Europe	WE	EUR-978	
Mayotte	MYT-175	Western Europe	WE	EUR-978	
Moldova		High Growth Emerging Markets	HGEM		1396
Monaco		Western Europe	WE		1163
Montenegro		Central Eastern Europe	CEE		1533
Netherlands	NLD-528	Western Europe	WE	EUR-978	1163
Norway	NOR-578	UK&Ireland, Nordics&Baltics	UKINB	NOK-578	1534
Poland	POL-616	Central Eastern Europe	CEE	PLN-985	1533
Portugal	PRT-620	Western Europe	WE	EUR-978	1163
Reunion	REU-638	Western Europe	WE	EUR-978	
Romania	ROU-642	Central Eastern Europe	CEE	RON-946	1533
Russia		High Growth Emerging Markets	HGEM		1396
San Marino		Western Europe	WE		1163
Serbia		Central Eastern Europe	CEE		1533
Slovakia	SVK-703	Central Eastern Europe	CEE	EUR-978	1533
Slovenia	SVN-705	Central Eastern Europe	CEE	EUR-978	1533
Spain	ESP-724	Western Europe	WE	EUR-978	1163
Svalbard and Jan Mayen	SJM-744	UK&Ireland, Nordics&Baltics	UKINB	NOK-578	

Country Name EEA Overseas in red	Country	Division (Long)	Division (short)	If EEA, Currency non EUR in red	AN...
Sweden	SWE-752	UK&Ireland, Nordics&Baltics	UKINB	SEK-752	1534
Switzerland		Germany&Switzerland	G&S		1365
Tajikistan		High Growth Emerging Markets	HGEM		1396
Turkey		High Growth Emerging Markets	HGEM		1396
Turkmenistan		High Growth Emerging Markets	HGEM		1396
Ukraine		High Growth Emerging Markets	HGEM		1396
United Kingdom	GBR-826	UK&Ireland, Nordics&Baltics	UKINB	GBP-826	1534
Uzbekistan		High Growth Emerging Markets	HGEM		1396
Vatican City		Western Europe	WE		1163

Section 14 - Appendix-C: List of acronyms

Acronym	Name
3DS	Three Domain Secure
3RI	3DS Requestor Initiated (Non-payment and Payment)
AAV	Accountholder Authentication Code
ABU	Automatic Billing Updater
ACS	Access Control Server
AReq	Authentication Request
ARes	Authentication Response
AuthE	Authentication
AuthO	Authorization
B2B	Business-to-Business
BAU	Business As Usual
BIN	Bank Identification Number

Acronym	Name
BPS	Basis Points
BRN	Banknet Reference Number
CAB	Card Acceptor Business
CDCVM	Consumer Device Cardholder Verification Method
CIS	Customer Interface Specifications
CIT	Cardholder or consumer Initiated Transaction
CNP	Card Not Present
COF	Card-On-File
CP	Card Present
CReq	Challenge Request
CRes	Challenge Response
CVM	Cardholder Verification Method
DS	Directory Server
DTI	Digital Transaction Insights
EBA	European Banking Authority
ECI	Electronic Commerce Indicator
EEA	European Economic Area
EMV	Europay Mastercard VISA
GDPR	General Data Privacy Regulation
GDS	Global Distribution System
HTML	Hypertext Markup Language
IAV	Issuer Authentication Value
ICA	Interbank Card Association
ICCP	
IPM	Integrated Product Messages
KBA	Knowledge-Based Authentication
KPI	Key Performance Indicator
LVP	Low-Value Payments
MCC	Merchant Category Code
MIT	Merchant-Initiated Transactions

Acronym	Name
MLRMP	Maestro Low Merchant Risk Program
MOTO	Mail Order Telephone Order
MPE	Member Parameter Extract
MRPP	Maestro Recurring Payment Program
MUPP	Maestro Utility Payment Program
OBS	On-Behalf Service
OOB	Out Of Band
OTP	One Time Password
PReq	Preparation Request
PRes	Preparation Response
PSD	Payment Services Directive
PSP	Payment Service Provider
RBA	Risk-Based Authentication
RReq	Results Request
RRes	Results Response
RTS	Regulatory Technical Standards
SAFE	System to Avoid Fraud Effectively
SCA	Strong Customer Authentication
SLI	Security Level Indicator
SPA	Secure Payment Application
TCC	Transaction Category Code
TRA	Transaction Risk Analysis
UCAF	Universal Cardholder Authentication Field
UI	User Interface
UX	User Experience
VCN	Virtual Card Number

Section 15 - Appendix-D: EMV 3DS Fields

In the following table:

x – optional
EC – Conditional by EMV
ER – Required by EMV / rejection by the Directory Server if not present
MC – Conditional by Mastercard
MR – Required by Mastercard / rejection by the Directory Server if not present

Fields that are filled with static or dummy values will be monitored by Mastercard.

Data Element	AReq	ARes	CReq	CRes	PReq	PRes	RReq	RRes
3DS Method Completion Indicator	ER							
3DS Requestor Authentication Indicator	ER							
3DS Requestor Authentication Information	MC							
3DS Requestor Challenge Indicator	MR							
3DS Requestor ID	MR							
3DS Requestor Name	MR							
3DS Requestor Prior Transaction Authentication Information	MC							
3DS Requestor URL	ER							
3DS Server Reference Number	ER				x			
3DS Server Operator ID	MR				x			
3DS Server Transaction ID	ER	x	x	x	x	x	x	x
3DS Server URL	ER							
3RI Indicator	ER							
Account Type	EC							
Acquirer BIN	MR							
Acquirer Merchant ID	MR							
ACS Challenge Mandated Indicator		x						
ACS Counter ACS to SDK				x				
ACS HTML				x				

Data Element	AReq	ARes	CReq	CRes	PReq	PRes	RReq	RRes
ACS Operator ID		x						
ACS Reference Number		x						
ACS Rendering Type		x					x	
ACS Signed Content		x						
ACS Transaction ID		x	x	x			x	x
ACS UI Type				x				
ACS URL		x						
Address Match Indicator	x							
Authentication Method							x	
Authentication Type		x					x	
Authentication Value		x					x	
Broadcast Information	EC	x						
Browser Accept Headers	ER							
Browser IP Address	EC							
Browser Java Enabled	ER							
Browser Language	ER							
Browser Screen Color Depth	ER							
Browser Screen Height	ER							
Browser Screen Width	ER							
Browser Time Zone	ER							
Browser User-Agent	ER							
Card/Token Expiry Date	MR							
Card Range Data						x		
Cardholder Account Information	x	x						
Cardholder Account Number	ER							
Cardholder Account Identifier	x							
Cardholder Billing Address City	EC							
Cardholder Billing Address Country	EC							
Cardholder Billing Address Line 1	EC							
Cardholder Billing Address Line 2	EC							
Cardholder Billing Address Line 3	EC							
Cardholder Billing Address Postal Code	EC							

Data Element	AReq	ARes	CReq	CRes	PReq	PRes	RReq	RRes
Cardholder Billing Address State	EC							
Cardholder Email Address	EC							
Cardholder Home Phone Number	EC							
Cardholder Mobile Phone Number	EC							
Cardholder Name	EC							
Cardholder Shipping Address City	EC							
Cardholder Shipping Address Country	EC							
Cardholder Shipping Address Line 1	EC							
Cardholder Shipping Address Line 2	EC							
Cardholder Shipping Address Line 3	EC							
Cardholder Shipping Address Postal Code	EC							
Cardholder Shipping Address State	EC							
Cardholder Work Phone Number	EC							
Challenge Additional Information Text				x				
Challenge Cancelation Indicator			x				x	
Challenge Completion Indicator				x				
Challenge Data Entry			x					
Challenge Information Header				x				
Challenge Information Label				x				
Challenge Information Text				x				
Challenge Information Text Indicator				x				
Challenge HTML Data Entry			x					
Challenge Selection Information				x				
Challenge Window Size			x					
Device Channel	ER							
Device Information	EC							
Device Rendering Options Supported	ER							
DS End Protocol Version						x		
DS Reference Number	EC	x						
DS Start Protocol Version						x		
DS Transaction ID	EC	x				x	x	x
DS URL	EC							
Electronic Commerce Indicator		x					x	

Data Element	AReq	ARes	CReq	CRes	PReq	PRes	RReq	RRes
EMV Payment Token Indicator	EC							
Expandable Information Label				x				
Expandable Information Text				x				
Instalment Payment Data	EC							
Interaction Counter							x	
Issuer Image				x				
Merchant Category Code	ER							
Merchant Country Code	ER							
Merchant Name	ER							
Merchant Risk Indicator	x							
Message Category	MR						x	
Message Extension	MC	x	x	x	x	x	x	x
Message Type	ER	x	x	x	x	x	x	x
Message Version Number	ER	x	x	x	x	x	x	x
Notification URL	ER							
OOB App URL				x				
OOB App Label				x				
OOB Continuation Indicator			x					
OOB Continuation Label				x				
Payment System Image				x				
Purchase Amount	ER							
Purchase Currency	ER							
Purchase Currency Exponent	ER							
Purchase Date & Time	ER							
Recurring Expiry	EC							
Recurring Frequency	EC							
Resend Challenge Information Code			x					
Resend Information Label				x				
Results Message Status								x
SDK App ID	ER							
SDK Counter SDK to ACS			x					
SDK Encrypted Data	EC							
SDK Ephemeral Public Key (Qc)	ER							
SDK Maximum Timeout	ER							

Data Element	AReq	ARes	CReq	CRes	PReq	PRes	RReq	RRes
SDK Reference Number	ER							
SDK Transaction ID	ER	x	x	x				
Serial Number					x	x		
Submit Authentication Label				x				
Transaction Status		x		x			x	
Transaction Status Reason		x					x	
Transaction Type	EC							
Why Information Label				x				
Why Information Text				x				