mastercard

AN 5762 Revised Standards for Europe Region EMV 3DS 2.2 Roadmap for Remote Electronic Transactions

Type:
Bulletin Announcement

Category:
Operations
Rules/Standards

Audience:
Acquirer
Issuer
Processor
Merchant
Network Enablement Partner

Region:
Europe

Brand:
Mastercard®
Debit Mastercard®
Maestro®

Product or Service:
Identity Solutions

Action Indicator:
Brand Mandate
Program or service requirement
Critical action needed
Financial impact
Registration required
Testing required

Published:
1 February 2022

Effective:
14 October 2022

Executive Overview

Mastercard is updating various details regarding core information previously published about the EMV 3-D Secure (3DS) 2.2 roadmap for remote electronic transactions. For specifics, refer to the new section called Overview of updates.

Effective date details

Date	Details
14 October 2022	Revised Standards will become effective.

Customer benefit

As part of the roadmap, all Europe region Mastercard and Maestro issuers and acquirers must not only support EMV[1] 3DS 2.2, but must also adopt specific features.

EMV 3DS 2.2 brings a number of key benefits over the EMV 3DS 2.1 and older industry standards:

- Streamlines authentication through promotion of frictionless authentication by offering message enhancements for fewer step-up authentications
- Improves user experience for out-of-band (OOB) transactions by requiring issuers and acquirers (for their merchants) to support merchant app re-direction, eliminating the need for additional cardholder interaction to complete the challenge process
- Enables issuers to fully meet the requirements of the Payment Service Directive 2 (PSD2) Strong Customer Authentication (SCA) Regulatory Technical Standards (RTS) by offering fully compliant authentication methods
- Enables a fully functional trusted merchant listing (TML)[2] for merchants and issuers, thus creating a user-friendly and frictionless experience for cardholders
- Enables 3DS requestor challenge indicators for acquirer exemptions identification, thus helping merchants influence decisioning
- Enables 3DS requestor-initiated (3RI) payment authentication flow

[1] EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

[2] Whitelisting as documented in the EMV 3DS 2.2 specifications has been renamed to TML by Mastercard.

In addition to the EMV 3DS 2.2 standard and some EMV 3DS 2.2 announced features, issuers and acquirers must also adopt features that are intended to improve authentication performance:

- Authentication app re-direction, eliminating the need for additional cardholder interaction to complete the OOB app transactions
- Additional insights on the challenge flow performance to facilitate monitoring and problem resolution

For ease of reference, this bulletin announcement makes reference to the technical requirements of the EMV 3DS v2.2 roadmap items and brings clarity about how customers can use the features to enhance the overall digital experience and achieve performance improvements in areas that have not been delivering expected results.

Furthermore, monitoring customer behavior with program requirements and key performance indicators (KPIs) will help issuers and acquirers (for their merchants) to reduce the possibility of errors while achieving performance improvements in the authentication flow.

What Mastercard is doing

Mastercard is rolling out a Europe region-wide roadmap to achieve a network migration to EMV 3DS 2.2, requiring the support of EMV 3DS features that will strengthen the support of the PSD2 regulation, where applicable, and that will allow performance improvements in those areas that have not returned the expected results since introduction of EMV 3DS.

In this bulletin announcement, Mastercard is providing all parties with more details and background about the features technical definitions introduced as part of the roadmap.

Likewise, Mastercard is reporting on the eventual introduction of programs to monitor that issuers and acquirers in the Europe region are performing as designed and complying with the requirements documented in this bulletin announcement.

Version history

Date	Description of change
1 February 2022	• Added details regarding the requirements to support the EMV 3DS v.2.2 authentication standard Added details regarding the monitoring programs that will help drive adoption of the new authentication roadmap • Included technical requirements details in the TML, 3RI, and authentication to merchant app re-direction features • Included insights regarding the HTML access control server (ACS) interface type in app challenge flow • Provided more information about compulsory functional testing • Added Network Enablement Partner to the Audience field. • Attached a new Q&A Blog spreadsheet, as well as an Issuer Test Result Matrix spreadsheet

Date	Description of change
1 February 2022 (continued)	• Added the following new sections or renamed and revised previously published sections: – Overview of updates – Supporting and using the EMV 3DS v2.2 standard – Functional testing requirements – Compliance overview – Program criteria – Comply-by date and assessments
28 September 2021	Initial publication date

Overview of updates

Mastercard previously announced revised Standards to facilitate EMV 3DS version 2.2 implementation for all card-not-present (CNP) transactions on Mastercard and Maestro-branded account ranges. The Standards will require all issuers and acquirers operating in the Europe region to support cardholder authentication using the EMV 3DS v2.2 standard and to comply with the Mastercard Identity Check (IDC) Program rules, effective 14 October 2022.

This bulletin announcement contains additional information about the technical details of the new authentication protocol and some of the mandated features, namely TML, 3RI, and authentication to merchant app re-direction (also called 3DS requestor app URL). In addition, Mastercard is adding an additional requirement related to the use of HTML ACS interface in app challenge transactions.

This bulletin announcement does not include the technical specifications for implementing the v2.2 standard nor the required features. Technical documentation is readily available in the EMVCo 2.2 specifications and the *Mastercard Identity Check Program Guide*. Further, this bulletin announcement also does not cover two of the roadmap features (merchant to authentication app re-direction and insights on the challenge flow errors). Mastercard has decided to defer the specifications of these features to EMVCo, where a message extension will be specified and documented with an expected publication in early 2022.

Furthermore, Mastercard is also providing more details about issuer and merchant testing programs and the monitoring framework that Mastercard will set to help ensure EMV 3DS v2.2 transactions are properly handled by customers.

With regards to compliance, this bulletin announcement does not include details regarding KPIs, program fees, and enforcement dates for specific markets. Mastercard will communicate those details at a later time.

Customers should review the revisions published in this bulletin announcement and make appropriate plans to support the roadmap features.

Background

As EMV 3DS 2.2 is increasingly being adopted, and with many 3DS servers and ACS providers faced with their EMVCo Letter of Approval and Mastercard Letter of Compliance expiring, it is critical that Mastercard offer a roadmap to give customers a vision of when and how new features can and will be applied across the network.

Since EMV 3DS and PSD2 migration have reached significant volumes, Mastercard has witnessed an inadequate app challenge flow performance that is hindering further expansion of digital electronic commerce (e-commerce). The EMV 3DS 2.2 roadmap will offer features and solutions that should help overcome some of the challenges in this environment.

As core of this roadmap, Mastercard is mandating issuers and acquirers to support the EMV 3DS 2.2 standard, including adoption of relevant EMV 3DS features by 14 October 2022.

EMV 3DS 2.2 reinforces Mastercard's commitment to support customers to comply with the PSD2 requirement to apply SCA to electronic payments in the European Economic Area (EEA) countries, the United Kingdom, and Gibraltar.

Furthermore, the EMV 3DS 2.2 roadmap responds to the e-commerce ecosystem demand for a more structured, transparent, and aligned evolution of the EMV 3DS versions, creating the opportunity for Mastercard to establish a common ground in the Europe region.

Customer impact

In the Europe region, each customer must prepare its system and that of its service providers (such as its ACS providers and 3DS service providers) to support the EMV 3DS 2.2 standard as indicated in the Background section of this bulletin announcement.

While Mastercard will require customers to support EMV 3DS 2.2, it will not require that all transactions are sent using this version of the protocol.

Supporting and using the EMV 3DS v2.2 standard

To comply with the roadmap requirements, issuers and acquirers that operate in the Europe region must comply as noted in the following sections.

Requirements for issuers

To comply with the roadmap requirements, issuers that operate in the Europe region must:

- Verify that they have properly implemented EMV 3DS v2.2 specifications and that they are compliant with Mastercard IDC Program rules.
- Check that their ACS provider has passed EMV 3DS v2.2 certifications, thus obtaining a valid EMVCo Letter of Approval and a valid Mastercard Letter of Compliance.
- Ensure that their ACS provider has successfully completed ACS program testing and received certification from Mastercard.
- For issuers that use third-party providers (TPPs), contact their vendors for more information about product availability.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network registered as supporting EMV 3DS v2.2 through Identity Solutions Services Management (ISSM) by setting the ACS end protocol to 2.2.0 for each account range.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network activated to be processed through EMV 3DS v2.2 transactions by their ACS provider.

Requirements for acquirers

To comply with the roadmap requirements, acquirers that operate in the Europe region must:

- Ensure for themselves and for their service providers (such as 3DS service providers) the full implementation of EMV 3DS 2.2 specifications.
- Check that their online merchants and corresponding 3DS server or software development kit (SDK) vendor have passed all required EMV 3DS v2.2 certifications, from EMVCo (Letter of Approval) and Mastercard (Letter of Compliance).
- Work, as necessary and feasible, with their online merchants to ensure they use the mandate features which is essential for achieving better results in authentication.

Requirement: Acquirers must have all online e-commerce enabled merchants in the Mastercard IDC authentication network ready to use EMV 3DS v2.2 transactions by their 3DS server or service as of 14 October 2022.

As a reminder, acquirers should take into consideration that, to promote interoperability, all IDC Program participants must continue to support EMV 3DS 2.1 transactions until Mastercard formally announces the decommissioning of EMV 3DS 2.1.

Furthermore, it should be noted that IDC service providers that have already completed EMV 3DS 2.2 certification (or will do so before 14 October 2022) must carry out additional functional testing to ensure the mandatory features defined in the roadmap are properly implemented. Mastercard will not require a new EMV 3DS 2.2 certification for this purpose.

Requirements for trusted merchant listing

PSD2 allows cardholders to list trusted merchants to bypass SCA whenever they make a purchase from that merchant. This is to enable frictionless experiences to the payers, where different merchants can be added to the cardholder's trusted merchant list.

Version 2.2 of the specifications allows merchants to influence decisioning by requesting trusted listing as part of the authentication transaction:

- Merchants can request the TML status for a card number.
- Merchants can request SCA in order to be listed.
- Merchants can request a frictionless authentication from the issuer applying the TML exemption.

Once the merchant is successfully added to the TML, then the merchant can leverage the issuer’s TML exemption for seamless authentication in subsequent transactions.

TML is a mandated issuer feature based on specific requirements, listed as follows.

Requirement: As of 14 October 2022, issuers must make a TML management portal or app available to the cardholder where the trusted merchant list can be managed, such as listings that can be updated or deleted.

Requirement: As of 14 October 2022, issuers and their ACS provider must support the TML Merchant Name mapping as identified in the Merchant List Report on ISSM.

Requirement: As of 14 October 2022, issuers must have the authentication pages updated to allow the merchant listing by the cardholder.

Requirement: As of 14 October 2022, issuers must allow cardholders to opt-out of the TML services altogether and must also allow cardholders to view, add, and remove merchants from their TML.

Requirement: As per PSD2 regulation, issuers must request SCA when the cardholder adds or modifies a merchant to his or her TML.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network registered as supporting TML through ISSM by setting the Whitelisting Supported by ACS to Yes for each account range.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network activated for TML to be processed through EMV 3DS v2.2 transactions by their ACS provider.

Requirement: As of 14 October 2022, when a merchant is requesting to be listed as trusted merchant, the issuer must not systematically refuse the requested listing.

Requirement: As of 14 October 2022, issuers must provide the TML status upon request of a merchant through EMV 3DS authentication.

Requirement: As of 14 October 2022, when a merchant is requesting to be exempted from SCA as a trusted merchant, the issuer must not systematically refuse the requested exemption.

Recommendation: Mastercard strongly recommends merchants to use TML to increase the share of frictionless authenticated transactions, improving the cardholder experience and reducing abandonment rates.

NOTE: For more information about TML technical details, refer to the Trusted Merchant Listing (TML) processing section in the *Mastercard Identity Check Program Guide*.

NOTE: For more information and recommended best course of action on cardholder user experience for adding merchants and for managing the merchant whitelist, risk considerations, and operational considerations, refer to the *Mastercard Standards for Trusted Merchant Listing*.

Requirements for 3RI payments

Version 2.2 of EMV 3DS specifications introduces the support for 3RI payments, which offers merchants the option to system-generate a payment transaction (Device Channel = 03-3RI, Message Category = 01-PA) when the cardholder is not in session.

3RI payment transactions are highly beneficial for use cases like partial or split shipments, agent model, and recurring payments. In these use cases, there is an initial purchase transaction while the cardholder is in session, called consumer-initiated transaction (CIT), followed by subsequent transactions that are 3RI MIT.

NOTE: For 3RI, payments where the cardholder is in session are referred to as initial/first/originally authenticated transactions, while payments where the cardholder is off session are referred to as subsequent transactions.

With 3RI payments, merchants can provide evidence that SCA has been performed where the customer was involved and maintain their fraud liability protection for the full amount that has been authenticated. 3RI payments might also result in performance improvements as merchants are able to connect subsequent payments with initial authenticated transactions.

ACS providers and 3DS servers that intend to process 3RI payments must retain reference data from the initial and originally authenticated transaction such as amount, currency, and transaction reference ID. ACS providers must ensure that the 3RI amount does not exceed the originally authenticated amount. Upon successful processing, the ACS will return an authentication value in the response message.

NOTE: ACS providers are not obliged to retain reference data from initial authenticated transactions that have taken place before 14 October 2022.

The 3RI payment request for the subsequent transactions must indicate the type of transaction and must reference the initial authenticated transaction.

Within a 3RI authentication response, the e-commerce service level indicator will be set to 02 with a corresponding AAV Leading Indicator (AAV LI) of kA to identify a non-recurring payment 3RI transaction. The e-commerce service level indicator will be set to 07 with a corresponding AAV LI of kO to identify a recurring payment 3RI transaction.

Upon completion of the 3RI authentication process, 3DS servers can then present the transaction for authorization with a SLI of 212 or 217 and the accountholder authentication value (AAV) LI.

The IDC Program is defining the following requirements and recommendation when processing 3RI payments:

Requirement 128: A 3RI payment transaction's 3DS Requestor Prior Transaction Authentication Data (Field Name: threeDSReqPriorAuthData) field must be used to reference the DS transaction ID of the initial authentication transaction (frictionless or challenge) that the 3RI payment is tied to.

NOTE: The use of all the elements in the 3DS Requestor Prior Transaction Authentication Information (Field Name: threeDSRequestorPriorAuthenticationInfo) increases the ACS's chances of approving the transaction without requiring extra authentication.

Requirement 142: All issuer account ranges must support application based, browser based, and 3DS 3RI transactions.

Requirement 173: 3RI transactions, payment or non-payment, must not be used for an add card transaction.

Recommendation: For 3RI payment transactions, use Authentication amount = Amount of the individual 3RI transaction.

NOTE: For the exact data field to reference the DS transaction ID of the initial authentication transaction, refer to the following chapters in the *Mastercard Identity Check Program Guide*: 3RI Transaction Processing (payment and non-payment) and Recurring payment processing.

In addition to the above-mentioned requirements, some other requirements are established when handing 3RI payments.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network activated for 3RI to be processed through EMV 3DS v2.2 by their ACS provider.

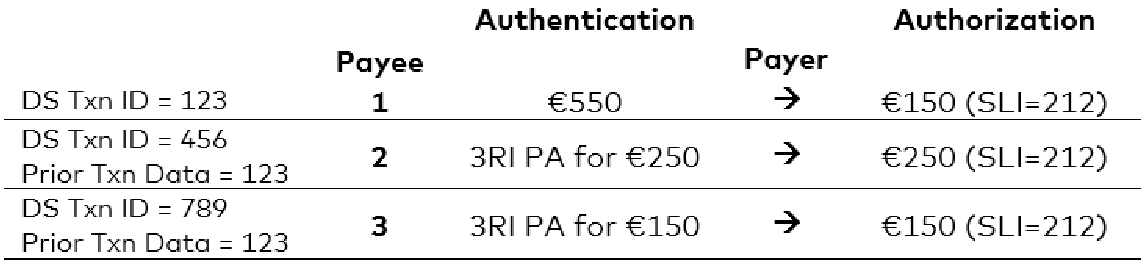
Requirement: As of 14 October 2022, issuers must not systematically refuse the frictionless authentication of a correctly formatted and configured 3RI authentication request.

Requirement: Acquirers and their online merchants must not request 3RI authentication for an amount that exceeds the amount of the initial and correctly referenced authentication that obtained SCA from the cardholder.

Requirement: Acquirers and their online merchants, when sending the authorization upon successful 3RI authentication, must reference the Trace ID of the authorization of the initial transaction where SCA was obtained from the cardholder.

The following payment use cases are part of the mandate:

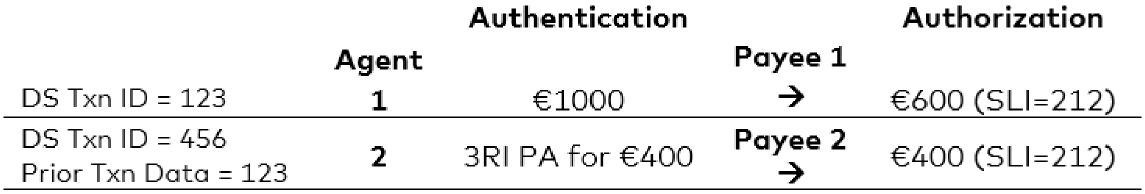
- **Partial/split shipment:** This is a use case when, for example, ordered products are not all available at the same time and the merchant decides to ship them separately.
  If the acquirer presents a separate authorization for each shipment, including specific shipment costs, the transaction can be handled using EMV 3DS v2.2 protocol as follows:



		Authentication		Authorization
	Payee		Payer	
DS Txn ID = 123	1	€550	→	€150 (SLI=212)
DS Txn ID = 456 Prior Txn Data = 123	2	3RI PA for €250	→	€250 (SLI=212)
DS Txn ID = 789 Prior Txn Data = 123	3	3RI PA for €150	→	€150 (SLI=212)

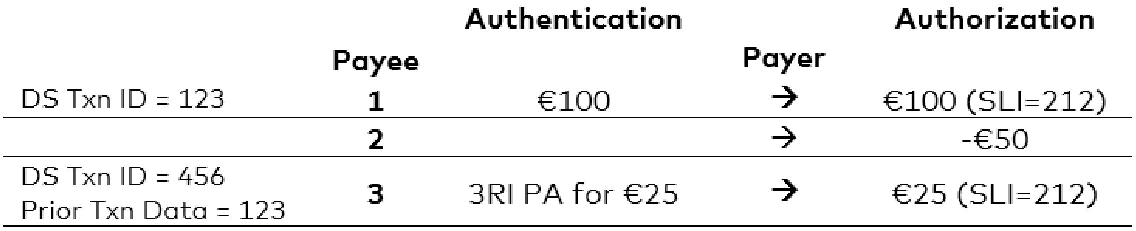
- **Agent payment with multiple merchants:** This is a use case where the travel agent website manages orders for both hotels and airlines for different merchants. In such use cases, there will be one authentication followed by multiple authorizations for each of the merchants. In addition to the currently defined model where different merchants re-use the AAV of the initial and single authentication, 3RI offers these different merchants an alternative model.

Following is an example of how it will work. The transaction is authenticated for the full amount. The first authorization is submitted as a SLI = 212 (fully Authenticated) for the number of goods and services offered by merchant 1 (payee 1). The transaction for the merchant 2 (payee2) is authenticated as a 3RI payment transaction for the number of goods or services offered by merchant 2, which generates a new AAV and DS Transaction ID. The 3RI payment request for the second merchant must reference the DS transaction ID of the initial or first fully authenticated payment transaction using the 3DS Requestor Prior Transaction Authentication data field. All transactions are then submitted into authorization as a SLI= 212 (fully authenticated) with their respective AAVs and DS Transaction ID.



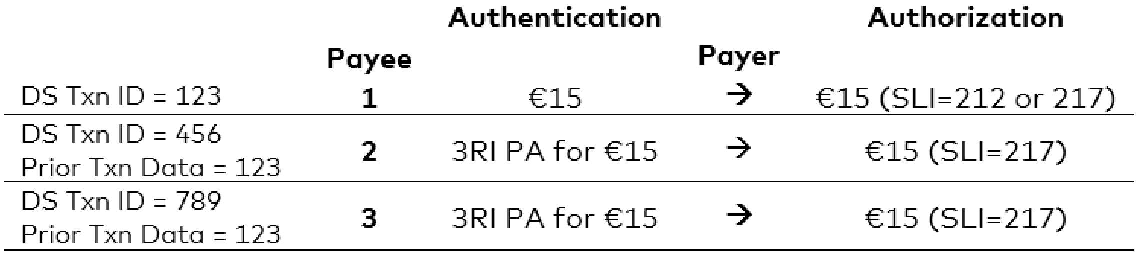
	Agent	Authentication	Payee 1	Authorization
DS Txn ID = 123	1	€1000	→	€600 (SLI=212)
DS Txn ID = 456 Prior Txn Data = 123	2	3RI PA for €400	Payee 2 →	€400 (SLI=212)

- **Replacement of a refunded purchase:** This is a use case where, for example, retailers allow cardholders to purchase items and offer free returns of products and goods cardholder does not want. The refunds are initiated even before merchant physically receives the returned goods and verifies. If the returned goods do not contain some of the actual merchandize that was supposed to be returned, then the merchant needs to be able to charge the consumer again for the missing goods.
  The merchant can use 3RI payments transaction to authenticate for the amount that needs to get re-charged to the cardholder. Following is an example where the returned goods value is EUR 50, and the missing goods are valued at EUR 25. For example,



	Payee	Authentication	Payer	Authorization
DS Txn ID = 123	1	€100	→	€100 (SLI=212)
	2		→	-€50
DS Txn ID = 456 Prior Txn Data = 123	3	3RI PA for €25	→	€25 (SLI=212)

- **Recurring payments with fixed amounts:** This is a use case where, for example, there is a monthly newspaper or streaming service subscription. The cardholder subscribes for the service, pays for the upfront cost and gets charged on a monthly basis while not in session. With the usage of 3RI payment transaction, the transaction is authenticated for each subsequent fixed amount.
  With the usage of 3RI payment transaction, the transaction is authenticated for each subsequent fixed amount. All authorizations are submitted as a SLI = 217 for amount of goods and services offered by merchant with their respective AAVs and DS Transaction ID. For example,



	Payee	Authentication	Payer	Authorization
DS Txn ID = 123	1	€15	→	€15 (SLI=212 or 217)
DS Txn ID = 456 Prior Txn Data = 123	2	3RI PA for €15	→	€15 (SLI=217)
DS Txn ID = 789 Prior Txn Data = 123	3	3RI PA for €15	→	€15 (SLI=217)

- **TML status check:** A merchant can check the status of its trusted listing using 3RI payment or non-payment transaction in version 2.2 of EMV 3DS.

Recommendation: As per Mastercard revised Standards, while the feature 3RI for payment and non-payment transactions is mandated for issuers only, to reap the full benefit of EMV 3DS v2.2, online merchants have the option to use this feature to effectively manage complex use cases.

NOTE: For more information about 3RI technical details, refer to the following chapters in *Mastercard Identity Check Program Guide*: 3RI Transaction Processing (payment and non-payment) and Recurring payment processing.

Requirements for authentication to merchant app re-direction

Version 2.1 does not allow a user-friendly transfer between the issuer authentication app and the merchant app on a consumer device that can process a 3DS transaction. EMV 3DS v2.2 and subsequent versions resolve this issue as they support automatic redirection between apps.

Authentication to merchant app redirection (also called 3DS requestor app URL) improves user experience in OOB transactions as it allows moving from the authentication app to the merchant app without any cardholder action, thereby reducing touch points, friction and potential for failure.

In the challenge flow, the merchant app, through the 3DS software development kit (SDK), interacts with the ACS and declares its URL, thus enabling the authentication app to call the merchant app after the OOB authentication has occurred.

Requirement: As of 14 October 2022, Mastercard will require the support and use of authentication to merchant app re-direction in all app device channel transactions' challenge flow. The EMV 3DS v2.2 support requirements are changed from optional to required.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network enabled for authentication to merchant app re-direction to be processed through EMV 3DS v2.2 transactions by their ACS provider and on their authentication app in accordance with EMV 3DS v2.2 specifications.

Requirement: As of 14 October 2022, acquirers and their online merchants enabled in the Mastercard IDC authentication network and operating a merchant app for e-commerce purchases must activate their 3DS server or service to support the authentication to merchant app re-direction through the merchant app, the 3DS SDK, and EMV 3DS v2.2 transactions and in accordance with EMV 3DS v2.2 specifications.

Requirement: As of 14 October 2022, all acquirers and their online merchants must perform app-based authentications only using EMV 3DS v2.2 and with app-redirection through the merchant app if the cardholder authentication method is OOB.

NOTE: For more information about authentication to merchant app re-direction technical details, refer to the EMVCo v2.2 specifications.

Requirements for HTML ACS interface type in app challenged transactions

Throughout the PSD2 migration monitoring period and confirmed through the results of the issuer app testing program, it has been demonstrated that the HTML interface type in app device channel transactions is delivering a poor cardholder experience and performance.

Requirement: As of 14 October 2022, issuers must no longer propose the HTML ACS interface as part of the ACS rendering type for app device channel transactions.

Requirements for merchant to authentication app re-direction

Just as with the authentication to merchant app redirection, merchant to authentication app redirection (also called OOB app URL) improves user experience in OOB transactions as it allows moving from the merchant app to the authentication app without any cardholder action, thereby reducing touch points, friction, and potential for failure.

In the challenge flow, the authentication app interacts with the 3DS SDK and merchant app and declares its URL through the ACS, thus enabling the merchant app to call the authentication app to initiate the OOB authentication.

Requirement: As of 14 October 2022, Mastercard will require the support and use of merchant to authentication app re-direction in all app device channel transactions' challenge flow. Detailed EMVCo message extension specifications will be identified as required.

Requirement: As of 14 October 2022, issuers must have all e-commerce enabled account ranges in the Mastercard IDC authentication network enabled for merchant to authentication app re-direction to be processed through EMV 3DS v2.2 transactions by their ACS provider and on their authentication app in accordance with the EMVCo message extension specifications to be announced.

Requirement: As of 14 October 2022, acquirers and their online merchants enabled in the Mastercard IDC authentication network and operating a merchant app for e-commerce purchases must activate their 3DS server or service to support the merchant to authentication app re-direction through the merchant app, the 3DS SDK, and EMV 3DS v2.2 transactions and in accordance with the EMVCo message extension specifications to be announced.

Requirement: As of 14 October 2022, all acquirers and their online merchants must perform app-based authentications only using EMV 3DS v2.2 and with app-redirection through the merchant app if the cardholder authentication method is OOB.

NOTE: For more information about merchant to authentication app re-direction technical details, refer to a future EMVCo message extension specifications.

Requirements for insights on the challenge flow errors

Through the introduction of EMVCo message extension specifications, Mastercard will require issuers to use the Challenge Error Reporting feature to provide additional insights on the error messages received or sent during the challenge flow.

Requirement: As of 14 October 2022, issuers must make the errors that are encountered during the challenge flow available through EMV 3DS v2.2 transactions by their ACS provider and on their authentication app in accordance with the EMVCo message extension specifications to be announced.

NOTE: For more information about insights on the challenge flow errors technical details, refer to a future EMVCo message extension specifications.

Overview of revised Standards

This bulletin announcement describes the following revised Standards:

- In the Europe region, effective 14 October 2022, customers must ensure support for the EMV 3DS 2.2 specifications as follows:
  - An issuer must enroll all e-commerce-enabled Mastercard and Maestro BIN ranges in EMV 3DS 2.2 and ensure full implementation of EMV 3DS 2.2 and use of the following features: TML, 3RI, authentication to merchant app redirection (also called 3DS requestor app URL), merchant to authentication app redirection, and insights on the challenge flow errors. This will enable issuers to achieve full compliance with PSD2 SCA RTS while improving the cardholder's digital payment experience.
  - An acquirer must itself implement EMV 3DS 2.2 and must ensure that its merchants and service providers (such as its 3DS service providers) implement and use the EMV 3DS 2.2 authentication to merchant app redirection (also called 3DS requestor app URL) and merchant to authentication app redirection. This will improve consumer experience with in-app payments, reducing abandonment and increasing acceptance locations.
- New issuer BIN ranges and merchants and existing issuer BIN ranges and merchants that already support EMV 3DS version 2.1 must continue to support this version to ensure interoperability with merchants and issuers that do not yet support EMV 3DS 2.2 (such as those outside the Europe region). It should be noted that Mastercard has already set out in AN 3391 Mastercard Customer Roadmap to Transition from 3DS 1.0 to EMV 3DS (2.0) the decommissioning of 3DS 1.0 (SecureCode) by October 2022.

Functional testing requirements

To support customers in implementing the EMV 3DS v2.2 standard and the mandate features effectively, Mastercard will make the Europe region browser-based and app-based testing platforms, and the test scenarios, available as of January 2022.

All issuers and acquirers (for their app-based merchants) operating in the Europe region must conduct functional testing to help ensure browser and app-based flow transactions are properly handled in their systems and those from their service providers (such as ACS providers, 3DS servers, or SDK vendors).

Mastercard will compulsorily require issuers and acquirers (for their merchants) to fulfill functionality testing and will provide information about how to validate transactions in the production environment at a later date.

Issuer testing approach

Issuers can use the Mastercard Issuer Browser Testing Platform for browser-based flow transactions (by enrolling at https://validation.sibs.ro/login.php). Issuers can freely use any other platform to perform the test cases listed in the first tab (called Browser testing EMV 3DS 2.2) of the attached Excel file.

For app-based flow transactions, Mastercard will make platform and test scenarios available as of the second quarter of 2022. Mastercard will communicate more details in this regard at a later time.

Requirement: As of 14 October 2022, issuers must have successfully completed all EMV 3DS v2.2 test cases set in the Mastercard Issuer Browser Testing Platform, which includes test scenarios for TML and 3RI. Additional test cases relating to SCA exemptions (such as low value payments and transaction risk analysis) and iFrame challenge window sizes also must be completed by issuers to ensure their set up is correct.

Requirement: As of 14 October 2022, issuers must have successfully completed all test cases that will be defined in the Mastercard App-based Issuer Testing Platform, which refers to the app re-direction features (such as authentication to merchant app re-direction and merchant to authentication app re-direction).

Acquirer and merchant testing approach

To support acquirers and merchants in verifying that they have properly implemented the roadmap features, Mastercard will make its Mastercard App-based Merchant Testing Platform available alongside specific test scenarios as of the second quarter of 2022. Mastercard will communicate more details in this regard at a later time.

Requirement: As of 14 October 2022, acquirers must ensure that all their app-based merchants have successfully completed all test cases that will be outlined in the Mastercard Merchant Testing Platform, which refers to the app re-direction features (such as authentication to merchant app re-direction and merchant to authentication app re-direction).

Testing platform availability

The testing platforms will be available for issuers and merchants in self-service mode. However, issuers and merchants will need to validate their test transactions and open a Mastercard Customer Implementation Services (CIS) project, which will consist of the following activities:

- Mastercard will assign an implementation specialist.
- Customers will perform tests in production.
- Mastercard will provide test cases.
- Customers will generate transactions using the test platform provided by Mastercard or a platform selected by the customer.
- Customers will provide the following transaction details for the implementation specialist to trace the transactions:
  - For authentication transactions:
    DS Transaction ID (DE 48 [Additional Data—Private Use], subelement 66 [Authentication Data], subfield 2 [Directory Server Transaction ID])
  - For authorization transactions:
    Network Data (DE 63 [Network Data] and transaction date)
- Upon successful completion[3] of the testing, Mastercard will provide a Production Test Acknowledgment Notification.

CIS test slots are limited and priority will be given to projects mandated by Mastercard. Thereafter, Mastercard will grant test slots on a first come, first served basis. At the time of opening the CIS project, the customer must be able to support all test cases in the attached Excel file.

NOTE: While Mastercard may contact customers that have not yet scheduled a project within a reasonable time frame, it is the customer's responsibility to initiate and complete the project in the specified time frame.

Compliance overview

Mastercard will continuously monitor transactions and perform systematic validations to promote data quality and help ensure that customers:

- Identify and amend unfavourable transactions behaviour trends
- Process transactions according to Mastercard processing rules, requirements, and Standards
- Adhere to product and service requirements as applicable

[3] The successful completion of the testing means that, in test cases in the first tab (called Browser testing EMV 3DS 2.2) of the attached Excel file that are related to TML, 3RI, low value payment and transaction risk analysis exemptions, and iFrame window size used for challenged transactions, transactions are performed without message errors and with approvals unless business rules require a decline. The deadline for opening a mandated CIS project is 1 September 2022.

Program criteria

To help ensure compliance with the EMV 3DS v2.2 roadmap, Mastercard will monitor that issuers enroll all account ranges in the EMV 3DS v2.2 standard and allow the use of the required features (namely, TML, 3RI, 3DS requestor app URL, OOB app URL, and challenge error reporting).

Similarly, Mastercard will validate that acquirers enable their online merchants to use EMV 3DS v2.2 transactions, and their app-based merchants transact using the authentication to merchant app re-direction and the merchant to authentication app re-direction features.

To monitor 3RI transactions, Mastercard will leverage the existing edit in the Data Integrity Monitoring Program that monitors 3DS activity (Edit7 - 3DS Requestor Initiated [ARes]).

NOTE: Complete information about the Data Integrity edit is reflected in the *Data Integrity Monitoring Program* manual.

Mastercard will communicate additional details about the monitoring criterion and applicable programs over the course of 2022 as part of the respective monitoring programs.

Comply-by date and assessments

Monitoring programs will officially begin to apply as of 14 October 2022 for the following Europe region countries:

Albania, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, New Macedonia, Norway, Netherlands, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

NOTE: In Germany, Maestro-branded account ranges without e-commerce traffic are not required to support the EMV 3DS v2.2 roadmap.

NOTE: This bulletin announcement will not apply to the Russian Federation (domestic) 3DS 1.0 Directory Server.

Mastercard will communicate the monitoring enforcement dates for the remaining Europe region countries at a later date.

Likewise, Mastercard will provide information about notifications and assessment start dates at a later time.

Revised Standards

To view marked revisions, refer to the attachment associated with this article. Additions are underlined; deletions are indicated with a strikethrough.

Additional information

Mastercard will update the Mastercard Identity Check Program Guide to reflect the technical implementation details and implementation requirements of the roadmap features. Or refer to:

- *Issuer Test Result Matrix* (Excel file attached to this bulletin announcement)
- *Mastercard Identity Check Onboarding Guide for ACS Service Providers, Operators, Issuers, and Processors* (available in the References library in the Technical Resource Center on Mastercard Connect)
- Q&A Blog (Excel file attached to this bulletin announcement)

Questions

Customers with questions about the information in this bulletin announcement should contact:

Identity Check Customer Support

idc_customer_support@mastercard.com