Arcot
by Broadcom

SOLUTION BRIEF

1H 2024

Arcot EMV 3DS Processing Recommendations

ISSUER RECOMMENDATIONS

- Correct Treatment of the 3DS Requestor Challenge and Authentication Indicators
- Proper Treatment of 3DS Requestor Initiated Transactions
- Decoupled Authentication

MERCHANT RECOMMENDATIONS

- 3DS Requestor Challenge and Authentication Indicators
- Use 3RI Requests for Recurring, Split, Delayed, and Multiparty Transactions
- Share Merchant Risk Level Indicator with Issuers

Welcome to the Spring/Summer 2024 edition of Arcot's issuer and merchant/acquirer processing recommendations for EMV 3DS. These recommendations are published to help the industry optimize EMV 3DS processing worldwide and in the context of the European revised Payment Services Directive (PSD2) regulations.

The ultimate objective is simple: **EMV 3DS is a tool to improve authorization success rates for merchants and issuers.**

EMV 3DS is the optimal way to share rich transaction metadata that can be used to improve authorization rates as well as orchestrate an authentication challenge where required, and to selectively apply those challenges to exactly the right transactions. However, maximum success for EMV 3DS has a number of dependencies, as the protocol is very powerful, with many features that can be actively exploited to share insights across the ecosystem to maximize success rates while minimizing fraud rates.

Accordingly, the Arcot division is delighted to present its first half of 2024 recommendations for EMV 3DS optimization for issuers and merchants. Additionally, the Arcot team will continue to publish recommendations in the future to help the entire ecosystem get the benefits of improved authorization rates using EMV 3DS.

Issuer Recommendations

Correct Treatment of the 3DS Requestor Challenge and Authentication Indicators

Scope: Worldwide

Merchants are advised to make proper use of the 3DS Requestor Challenge and Authentication Indicator fields. These are fields merchants can use to signal to the access control server (ACS) a preference with respect to cardholder challenges, and the type of authentication request being sent. In the real world, the use of these fields still shows a very high degree of inconsistency between merchants and geographies, suggesting that the fields use is still not well understood. For their use to be effective, proper corresponding treatment by issuers is equally important.

Benefits and Rationale

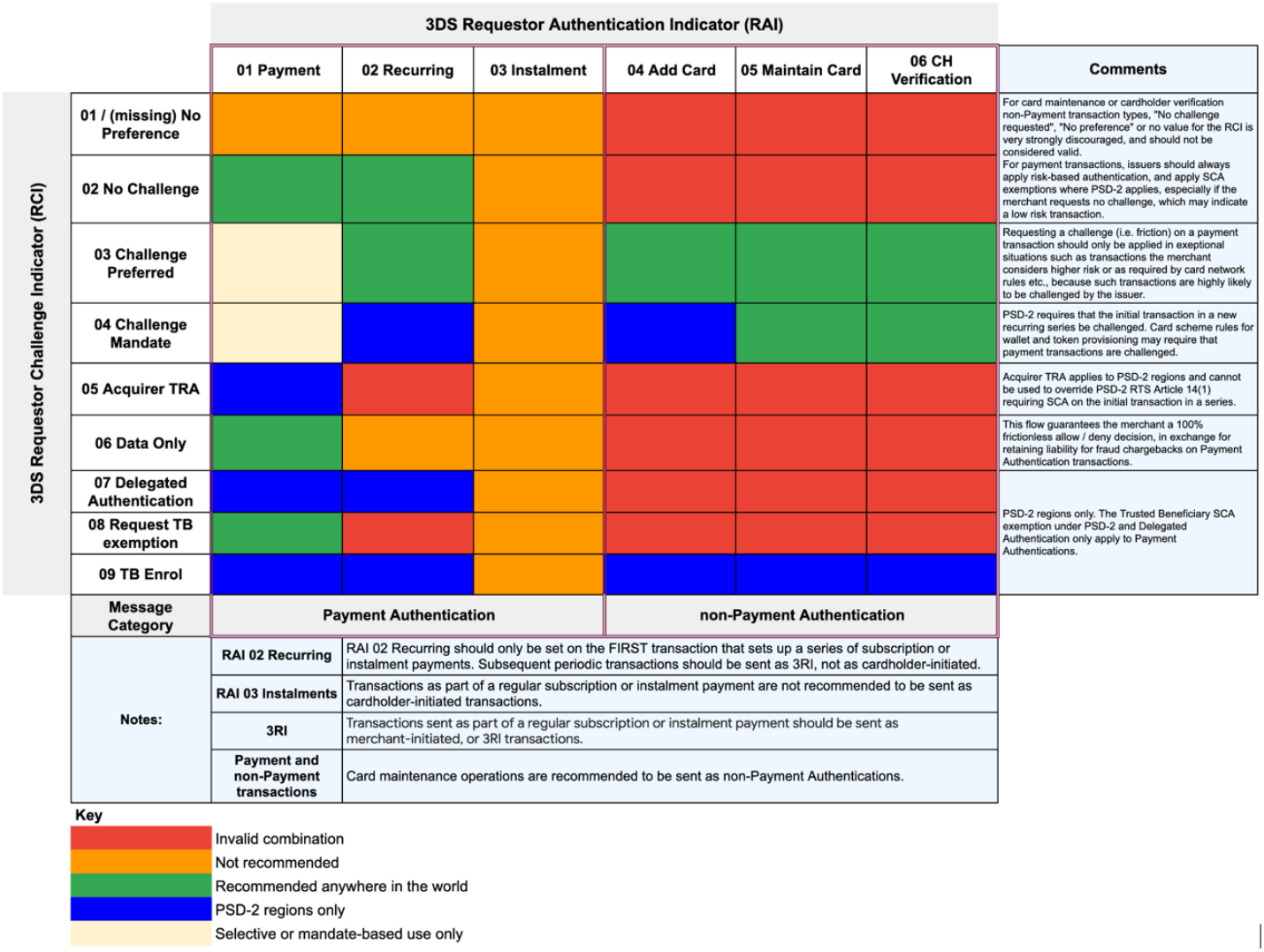
- There is a direct link between the percentage of frictionless flows and successful EMV 3DS transactions, with a higher percentage of frictionless flows leading directly to an increase in success rates.
- To help incentivize merchant consistency of these Indicators, it is important for issuers to have a consistent set of behaviors that merchants can rely on.

How to Implement

The key fields are threeDSRequestorChallengeInd (RCI) and threeDSRequestorAuthenticationInd (RAI) as defined by the EMV 3DS protocol. These fields in turn map to the risk analytics elements 3DS2_REQUESTOR_CHALLENGE_INDICATOR and CA_acc_threeDSRequestorAuthenticationInd in the Arcot platform.

Additional information about these fields can also be found later in this document in the Merchant Recommendations section. The following figure summarizes the recommended use of the 3DS RAI and RCI for cardholder-initiated (that is, *not* 3DS requestor initiated) payment and non-payment authentications.

Figure 1: 3DS RAI and RCI Payment and Non-Payment Authentication for Issuers



Proper Treatment of 3DS Requestor Initiated Transactions

Scope: Worldwide

3DS requestor initiated (3RI) 3DS transactions are 3DS authentication requests that are generated entirely by the merchant and not in response to cardholder activity. The name 3RI comes from the EMV 3DS Protocol Specification, which defines the 3DS requestor as being the entity that originates a 3DS authentication request. This request would equate to a merchant, their payment service provider, payment gateway, or acquirer, depending on who is providing an EMV 3DS service to the merchant. As such, it is roughly equivalent to the payment equivalent of merchant-initiated transaction (MIT).

3RI transactions can support cardholder challenge flows using the EMV 3DS 2.2.0 Decoupled Authentication flow. Decoupled Authentication is a challenge mechanism where a cardholder who is not present at the time an EMV 3DS authentication request is sent can be requested to authenticate at a later time. The maximum amount of time to wait for authentication to complete is defined by the merchant. Issuers should be reviewing decoupled flows and working with their 3DS ACS provider to implement Decoupled Authentication support.

Benefits and Rationale

- 3RI is a flow that will see increasing use by merchants as it enables additional use cases for EMV 3DS that do not carry a risk of friction or abandonment.
- Issuers should be positioned to correctly process all EMV 3DS flows to ensure success as merchants adopt them.
- 3RI transactions allow issuers to build a more complete picture of the lifecycle of engagement between the bank's cardholder and the merchants they use, potentially covering token and wallet provisioning, assorted status and verification checks, processing of complex transaction sequences, and split/delayed shipment scenarios, all of which may better support increased approval rates and better dispute investigation and resolution.
- Decoupled Authentication flows are a powerful authentication method that can eliminate friction from the checkout process and has powerful applications for sophisticated fraud prevention scenarios such as social engineering.

How to Implement

3RI is becoming an increasingly important 3DS flow. The following table is a list of scenarios where 3RI transactions may be sent by merchants, together with processing guidance for issuers.

Table 1: 3RI Transactions with Processing Guidance for Issuers

Reference	Summary	Details
1	Authentication value (AV)	On the major payment networks, an Authentication Value cryptogram (for example, AAV, CAVV, AEVV) is valid for a maximum of 90 days. An AV from one authentication request can be used on multiple authorization requests, for example, in cases such as multiparty travel bookings, split shipments, and so on. If a shipment is delayed or authorization is required for other operational reasons more than 90 days after the original authentication request, the merchant can send a 3RI EMV 3DS authentication request to obtain a new AV for a subsequent MIT authorization message, retaining liability shift. Issuers should approve these EMV 3DS requests unless there are exceptional overriding circumstances. For example, the card is no longer valid, the card was reported lost/stolen, and so on.
1a	Split shipment	Merchants may send a 3RI EMV 3DS authentication request with a 3RI indicator value of 06 to indicate that this is a split shipment request.
1b	Delayed shipment	Merchants may send a 3RI EMV 3DS authentication request with a 3RI indicator value of 06 when authorization for an authenticated transaction will be sent more than 90 days after the original authentication. This request may also be for a partial amount, for example, if a deposit on the original shipment had been taken at the time of authentication.
1c	Multiparty transactions	Merchants may send 3RI EMV 3DS authentication requests corresponding to each party in a multiparty transaction. A common example would be a travel agent that sells a package including flights, car hire, and accommodation. 3RI transactions are used to obtain an AV for each party to the transaction for inclusion in the appropriate authorization request.

Table 1: 3RI Transactions with Processing Guidance for Issuers (cont.)

Reference	Summary	Details
2	Recurring transactions 3RI Indicator 02	The initial setup of a recurring series of installment transactions must be authenticated, either through a frictionless or challenge flow, depending on the market and regulatory requirements. Subsequent transactions in a recurring series can be sent as EMV 3DS 3RI transactions, globally on the Mastercard network and in LAC, CEMEA, and AP regions for Visa. Issuers should generally approve recurring and installment 3RI transactions unless there are overriding reasons not to do so, for example, the card is no longer valid, the card is lost/stolen, and so on.
3	Add/maintain card 3RI Indicator 03/04	Where a card is requested to be added to a digital wallet, or card details stored in the wallet may be changing, and the cardholder is not available to complete an authentication challenge, a merchant may send an EMV 3DS non-payment 3RI authentication request to notify the issuer and obtain approval through a Decoupled Authentication challenge. Issuers should enable Decoupled Authentication and generally approve, through a Decoupled Authentication flow, card maintenance 3RI transactions unless there are overriding reasons not to do so. For example, the card is no longer valid, the card is lost/stolen, and so on.
4	Account verification 3RI Indicator 05	A merchant may send an EMV 3DS non-payment 3RI authentication request to verify the validity and standing of an account when the cardholder is not available to authenticate. This may form part of the setup and management of card-on-file procedures. For example. EMV 3DS 3RI non-payment transactions for account verification are a modern replacement for outdated authorization-based methods such as the $0 authorization request. Issuers should generally approve, through Decoupled Authentication, card verification 3RI transactions unless there are overriding reasons not to do so. For example, the card is no longer valid, the card is lost/stolen, and so on.
5	PSD-2 trusted beneficiary status checks 3RI indicator 10	This check applies to the EU PSD-2 regions only. A merchant can use an EMV 3DS 3RI non-payment authentication transaction to verify if they are present in a cardholder's *Trusted Beneficiary* list.

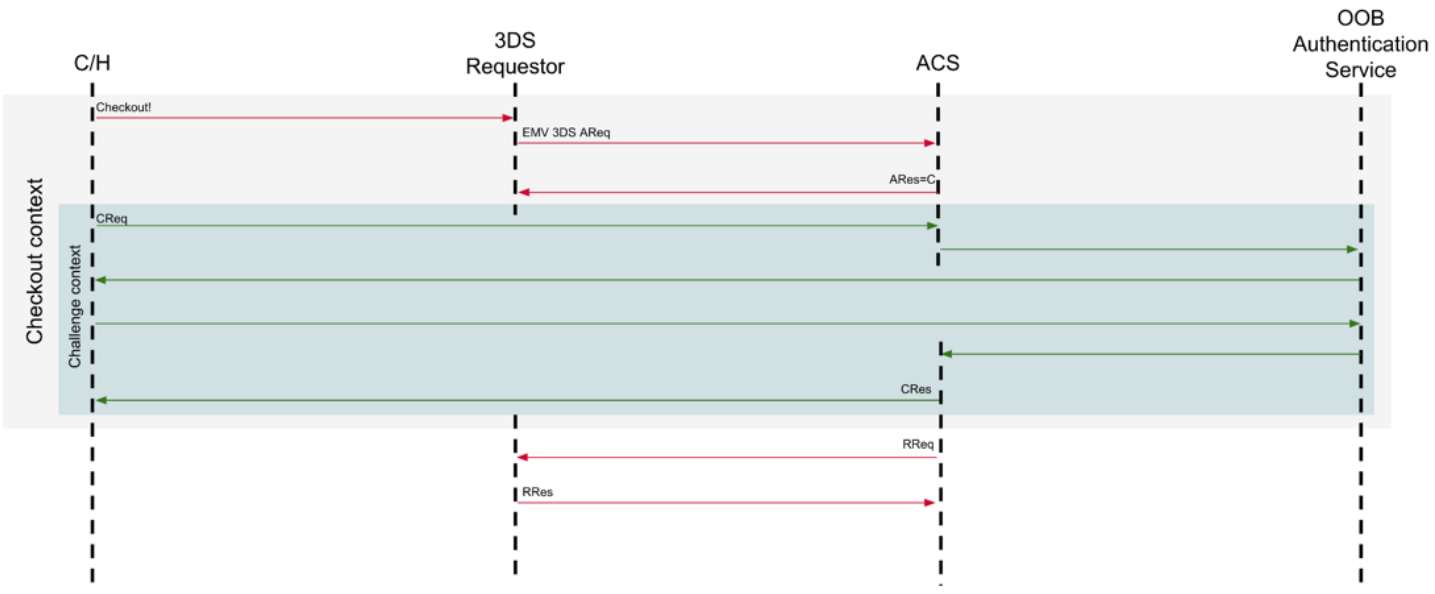
Decoupled Authentication

Scope: Worldwide

As recommended previously, issuers should enable Decoupled Authentication challenge flows.

In a conventional EMV 3DS transaction, the cardholder challenge flow happens as part of the merchant checkout process. This flow is represented in the following figure, where the green-shaded area representing the challenge flow is seen to be part of the gray-shaded area representing the checkout flow. The other details in the figure are not important for the purposes of these recommendations.

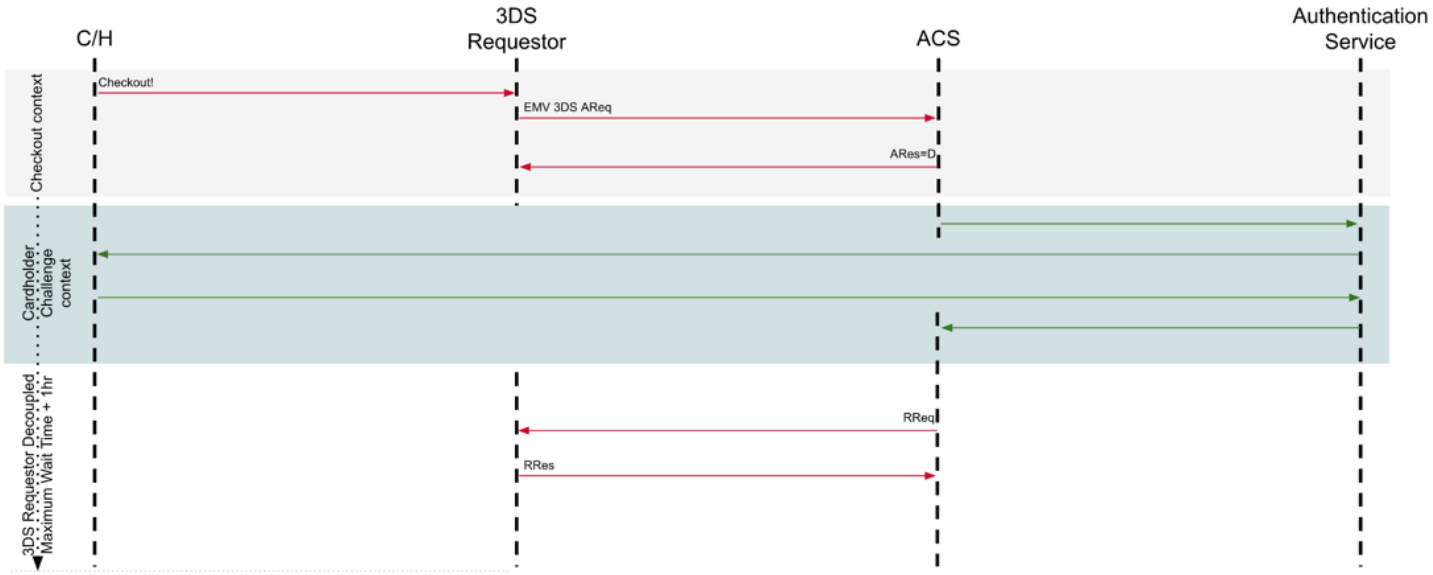
Figure 2: Conventional EMV 3DS Transaction



In a Decoupled Authentication flow the authentication happens *after* the EMV 3DS authentication has returned control to the merchant. The merchant thanks the cardholder for their order, perhaps informing them that they will receive further shipping updates in due course.

Meanwhile, at some later time, and with no involvement from the merchant, the issuer authenticates the cardholder, and, after the authentication outcome is known, updates the merchant with the result. This is shown in the following figure, where the green shaded area representing the challenge session is seen to be outside of, separate from, and subsequent to, the checkout flow:

Figure 3: Decoupled Authentication EMV 3DS Transaction



Issuers are recommended to implement out-of-band (OOB) authentication methods, and then work with their 3DS ACS service providers to enable Decoupled Authentication flows for their cardholders that use OOB authentication.

Benefits and Rationale

Because the authentication challenge flow is completely separate from the checkout flow, there is no risk of disruption to the checkout flow (that is, no risk of abandonment), and the disconnection between the checkout journey and the authentication journey enables some powerful use cases:

- Disruption of social engineering crimes, by injecting *time to think* into the authentication journey. A cardholder may be protected against social engineering by breaking the link between the criminal and the cardholder which exists during the checkout journey.
- Support for devices with no challenge flow user interface such as smart appliances, voice assistants, and so on.
- Corporate card use cases where the transaction approver may not be the same as the transaction initiator. For example, a corporate travel agent who initiates the purchase of a travel itinerary for a business traveler who approves the use of their corporate card to complete the purchase.

How to Implement

Decoupled Authentication requires OOB authentication. To support Decoupled Authentication flows, an issuer needs to have deployed an OOB authentication method.

An OOB authentication method is one where the authentication session is outside the scope of an EMV 3DS transaction. An example of an authentication flow that is *not* an OOB flow is SMS OTP. The OTP is entered into a challenge window that is presented by the ACS, and the authentication challenge is part of the 3DS session. Biometric authentication using a mobile app, perhaps where a push notification is sent by the issuer to the device to request authentication *is* an example of an OOB flow. The authentication challenge session is between the mobile app and the bank's servers, and is outside the scope of the EMV 3DS transaction itself.

For a Decoupled Authentication flow to work, an OOB authentication method is required. This method has the added benefit of ensuring that more robust forms of authentication are available to cardholders, and it is less susceptible to attacks such as social engineering, SIM swaps, and so on. With the emergence of *app less* mobile strong authentication options such as freely available OTP generator apps (for example, Google Authenticator and Microsoft Authenticator) and passkey authentication, there are plenty of options for stronger authentication methods even for organizations without a mobile app development and support capability.

Merchant Recommendations

3DS Requestor Challenge and Authentication Indicators

Scope: Worldwide

This section provides an update to the guidance in prior editions of these processing recommendations.

The 3DS RCI is a field merchants can use to signal to the ACS a cardholder challenge preference. In the real world, its use still shows a very high degree of inconsistency between merchants and geographies. Additionally, Arcot data suggests that there is still considerable confusion among 3DS implementers as to the proper usage of this field, especially when considered alongside another data field, the 3DS RAI.

Benefits and Rationale

- There is a direct link between the percentage of frictionless flows and successful EMV 3DS transactions, with a higher percentage of frictionless flows leading directly to an increase in success rates.
- Merchants almost always have a preference for a lower challenge rate, together with a view of the likelihood that the current transaction is fraudulent. Merchants should pass these insights and preferences, as well as accurate transaction type information through the 3DS RAI to issuers for them to challenge at an appropriate rate for the type of transaction.

How to Implement

The key fields are the threeDSRequestorChallengeInd (RCI) and threeDSRequestorAuthenticationInd (RAI) as defined by the EMV 3DS protocol. A summary of these two fields appears below:

Table 2: 3DS RCI and RAI Payment and Non-Payment Authentication for Merchants

Field	Values	Commentary
3DS Requestor Authentication Indicator	01 Payment transaction 02 Recurring transaction 03 Installment transaction 04 Add card 05 Maintain card 06 Token ID&V	Allows the merchant to indicate to the ACS the type of authentication request for a cardholder-initiated transaction. This is a *required* field for a cardholder-initiated transaction in EMV 3DS.
3DS Requestor Challenge Indicator	01 No preference 02 No challenge requested 03 Challenge requested 04 Challenge mandated 05 No challenge requested: risk analysis performed 06 Data share only 07 Authentication performed by merchant 08 Request to use Trusted Beneficiary Exemption 09 Challenge requested to add Trusted Beneficiary	Allows the merchant to indicate whether a cardholder challenge is requested or not for this transaction, and why that request is being made. This is an *optional* field in EMV 3DS.

Refer to the previous table in this document summarizing the recommended use of these indicators for cardholder-initiated payment and non-payment authentication transactions.

Merchants outside of PSD-2 regions, such as North America, should pay particular attention to the 3DS RCI value *06 Data share Only*, which is a 3DS flow that guarantees no issuer challenge in exchange for the merchant retaining fraud chargeback liability.

Use 3RI Requests for Recurring, Split, Delayed, and Multiparty Transactions

Scope: Worldwide

3RI transactions are 3DS authentication requests that are generated entirely by the merchant and not in response to cardholder activity. The name 3RI stems from the EMV 3DS Protocol Specification, which defines the 3DS requestor as being the entity that originates a 3DS authentication request. This request would equate to a merchant, their payment service provider, payment gateway, or acquirer, depending on who is providing an EMV 3DS service to the merchant. As such, it is roughly equivalent to the payment equivalent of MIT.

3RI transactions can support cardholder challenge flows using the EMV 3DS 2.2.0 Decoupled Authentication flow. Decoupled Authentication is a challenge mechanism where a cardholder who is not present at the time an EMV 3DS authentication request is sent can complete authentication at a later time. The maximum amount of time to wait for authentication to complete is defined by the merchant. Merchants should work with their 3DS Server provider to assess their readiness to support decoupled flows, as issuer adoption will increase in the months ahead.

Benefits and Rationale

- 3RI should be used for recurring payment transactions such as subscription and installment payments. Mastercard has worldwide support for these flows through 3DS, while Visa has worldwide support for split/delayed/multiparty shipment flows and regional support for recurring payments.
- 3RI enables additional use cases for EMV 3DS that do not carry a risk of friction or abandonment.
- 3RI can ensure merchant liability shifts on recurring and installment transactions, split and delayed shipments, multiparty transactions (for example, travel agency), and so on. By using 3RI for these transaction types that would previously have gone straight to authorization as MITs, merchants can retain liability shifts for the entire series of transactions in a recurring series or multi-authorization scenario.
- 3RI transactions allow a more complete picture of the lifecycle of engagement between the bank's cardholder and the merchants they use, potentially covering token and wallet provisioning, assorted status and verification checks, processing of complex transaction sequences, and split/delayed shipment scenarios; all of which may better support increased approval rates and better dispute investigation and resolution.
- Decoupled Authentication flows are a powerful authentication method that can eliminate friction from the checkout process and have powerful applications for sophisticated fraud prevention scenarios such as social engineering.

How to Implement

Support for 3RI is largely a matter of the 3DS requestor, or merchant site, adapting its business logic to call the merchant's 3DS Server for transaction types that would previously have been Merchant-Initiated Transactions and not sent via 3DS. All EMV 3DS platform components must be certified by EMVCo to correctly process 3RI transactions, hence there should be minimal dependency on the 3DS Server provider to enable 3RI support.

Refer to the previous section in Issuer Recommendations for further guidance on 3RI flows and use cases.

Share Merchant Risk Level Indicator with Issuers

Scope: Worldwide

This recommendation was also given in the previous version of these recommendations. It is being represented here because of the amount of industry feedback we have received asking, "What one data field should a merchant send that would make a difference?" While all these recommendations address this question in some shape or form, sharing a risk indication with issuers is a very powerful complement to other recommendations in this document.

Where merchants perform a real-time risk analysis of their transactions they should share a Low/Medium/High fraud risk indicator with the issuer through the EMV 3DS AReq message.

Benefits and Rationale

- For transactions the merchant considers to be a low risk the issuer can consider this insight as part of their own risk evaluation, minimizing SCA challenges and declines.
- For transactions the merchant considers to be a high risk the issuer can consider this insight as part of their own risk evaluation, maximizing fraud prevention.
- Merchant risk insights are complementary to issuer risk insights. The merchant sees the cardholder's shopping behavior across payment instruments the merchant supports, while the issuer sees the cardholder's shopping behavior across merchants the cardholder uses.

How to Implement

- Merchants should determine a set of buckets to separate transactions into low, medium, and high risk buckets according to their scoring process. For example:

Low risk	25% of transaction volume by lowest risk score
Medium risk	60% of transaction volume is not bucketed as low or high risk
High risk	15% of transaction volume by highest risk score

- Merchants, acquirers, and payment service providers should include the cardholder account information AReq element *acctInfo* with the suspiciousAccActivity subfield included, as well as setting a value for the 3DS requestor challenge Indicator, as discussed earlier. For example:

Low risk	acctInfo: suspiciousAccActivity = 01 3DSRequestorChallengeInd = 02
Medium risk	No acctInfo field included 3DSRequestorChallengeInd = 02
High risk	acctInfo: suspiciousAccActivity = 02 3DSRequestorChallengeInd = 03

Learn More

Contact your Customer Success Manager to learn more about EMV 3DS processing recommendations for PSD2.

BROADCOM®
connecting everything®

For more information, visit our website at: www.arcot.com

Arcot-EMV-3DS-Recommendations-1H2024-SB100 May 31, 2024