Arcot
by Broadcom

SOLUTION BRIEF

2H 2024

Arcot EMV 3DS Processing Recommendations

PROCESSING RECOMMENDATIONS

Welcome to the Autumn/Winter 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.

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 between merchants and issuers 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.

Previous versions of these processing recommendations have been structured with three recommendations for issuers and three for merchants and acquirers. For this version, the structure has been simplified, presenting two closely-related recommendations with implementation guidance for issuers and merchants/acquirers.

Recommendation 1: 3DS Requestor Challenge Indicator Values 02, 03, 04

Scope: Worldwide

The 3DS Requestor Challenge Indicator (RCI) is a field merchants should use to signal to the access control server (ACS) a merchant challenge preference. In the real world, its use still shows a very high degree of inconsistency between merchants and geographies. Therefore for this version of the processing recommendations, we have decided to focus on specific values for this field and simplify the guidance when compared with previous processing recommendations.

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.
- EMV 3DS is a tool that merchants and issuers can use to optimize cardholder journeys by removing friction for low-risk transactions that do not need to be challenged, and stopping fraud by challenging or denying risky transactions. EMV 3DS enables merchants and issuers to cooperate to achieve these twin objectives.

The table below summarizes the sections that follow:

Transaction Scenario	Merchant EMV 3DS Request	Issuer Response
Merchant low risk; issuer low risk	3DSRequestorChallengeInd 02 acctInfo: suspiciousAccActivity 01	Frictionless approval
Merchant low risk; issuer high risk		Challenge or Deny
Merchant high risk; issuer low risk	3DSRequestorChallengeInd 03 acctInfo: suspiciousAccActivity 02	Challenge
Merchant high risk; issuer high risk		Challenge or Deny
Challenge mandated	3DSRequestorChallengeInd 04	Challenge

1.1 Merchant Low-Risk Transactions

As per the EMV 3DS Core Specification, the 3DS RCI value of *02* corresponds to *No challenge requested*.

The merchant is requesting the issuer not to challenge the cardholder for this transaction on the basis that the transaction represents a low fraud risk.

The value of *02* is recommended to be used by merchants who have a fraud/risk assessment process in place. Those transactions that are considered, based on merchant insights, to represent a low risk of fraud should be sent with the value 02. Issuer ACS systems should be configured to give preferential treatment to approving such requests without friction (i.e. a challenge).

Merchants with sophisticated fraud/risk scoring systems in place should also consider an additional EMV 3DS field to designate that the transaction represents a low risk of fraud. A proposal for such risk insight sharing based on encoding the Suspicious Account Activity field of the EMV 3DS Merchant Risk Indicator has been detailed in previous versions of these processing recommendations. As a reminder, the recommendation is that transactions explicitly being assessed as low fraud risk by a merchant fraud screening system should be sent to the issuer's ACS with the value *01* in the Suspicious Account Activity field.

EMV 3DS RCI 02 together with Suspicious Account Activity Field 01 is a powerful signal from the merchant to the issuer that the merchant has assessed the transaction as a low fraud risk. Issuer ACS systems should treat such transactions sympathetically, only challenging or denying those where the issuer's risk assessment conclusion is significantly different and the transaction represents a high risk of fraud.

> **Note for PSD-2 Regions:** Unless a merchant is claiming the Acquirer Transaction Risk Analysis exemption, an issuer may still need to challenge a low-risk transaction because the transaction does not qualify for any other PSD-2 SCA exemption. However, a transaction assessed as low risk by a merchant can be approved on the basis of another qualifying exemption, such as Trusted Beneficiary. It is not a requirement that a merchant low-risk transaction be exempted from SCA via the Issuer TRA exemption.

How to Implement

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 follows:

3DSRequestorChallengeInd = 02
acctInfo.suspiciousAccActivity = 01

Issuers should configure their Risk Analytics rules to frictionlessly approve merchant low-risk transactions, unless there is an overriding reason to do so. The key fields are the threeDSRequestorChallengeInd and (RCI as defined by the EMV 3DS protocol) and the acctInfo.suspiciousAccActivity field, which in turn map to the Risk Analytics elements 3DS2_REQUESTOR_CHALLENGE_INDICATOR and CA_atn_buyerSuspiciousActivity in the Arcot platform.

1.2 Merchant High-Risk Transactions

As per the EMV 3DS Core Specification, the 3DS RCI value of *03* corresponds to *Challenge requested* (3DS Requestor preference).

The merchant/acquirer (3DS Requestor) is making a conscious decision to explicitly recommend this transaction to go to a challenge flow.

It is recommended that the reason merchants should express a deliberate preference for a transaction to be challenged is because the merchant has a fraud/risk assessment process in place, and the merchant considers that this transaction represents a higher level of fraud risk. Issuer ACS systems should be configured to challenge such transactions unless there are specific characteristics of the individual cardholder that would make a challenge nonviable. Issuers should consider that a merchant who assesses a transaction as carrying a higher fraud risk may have other business processes, such as manual review and conditional payment authorization decisioning, based on the issuer honoring the challenge preference. If an issuer frictionlessly approves an RCI 03 transaction, a merchant may decide not to proceed to authorization or may incur considerable additional processing costs associated with manual review. A properly challenged transaction will avoid these merchant business processes and be presented for authorization approval, maximizing overall payment success rates for all parties' benefit.

Merchants with sophisticated fraud/risk scoring systems in place should also consider an additional EMV 3DS field to designate the transaction as representing a higher risk of fraud. In a similar manner to the recommendation above relating to using the Suspicious Account Activity field to indicate a low fraud risk, it is recommended that transactions explicitly being assessed as higher fraud risk by a merchant fraud-screening system should be sent to the issuer's ACS with the value *02* in the Suspicious Account Activity field.

EMV 3DS RCI 03 together with Suspicious Account Activity Field 02 is a powerful signal from the merchant to the issuer that the merchant has assessed the transaction as a higher fraud risk. Issuer ACS systems should challenge such transactions, only denying those where the issuer's risk assessment conclusion indicates a very high risk of fraud.

How to Implement

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 follows:

3DSRequestorChallengeInd = 03
acctInfo: suspiciousAccActivity = 02

For issuers on the Arcot platform, issuers should subscribe to the RCI - Challenge Request policy in Risk Analytics. If the Risk Analytics Policy NOT used, and an issuer is managing the RCI 03 logic with their own rules, the key fields to consider are the threeDSRequestorChallengeInd (RCI as defined by the EMV 3DS protocol) and the acctInfo.suspiciousAccActivity field, which in turn map to the Risk Analytics elements 3DS2_REQUESTOR_CHALLENGE_INDICATOR and CA_atn_buyerSuspiciousActivity in the Arcot platform.

1.3 Transactions Subject to a Mandatory Challenge

As per the EMV 3DS Core Specification, the 3DS RCI value of *04* corresponds to *Challenge requested (Mandate)*. The merchant/acquirer (3DS Requestor) is asserting that this transaction requires a challenge flow for regulatory compliance reasons. This could happen for various reasons:

- Under PSD-2 and card scheme rules, the first transaction when setting up a recurring series of transactions must be authenticated.
- When tokenizing a card on file, a cardholder challenge is mandatory under PSD-2 rules.
- Most non-payment authentication scenarios require a cardholder challenge because the usual purpose of non-payment authentication is to verify the cardholder account.

How to Implement

Merchants, acquirers, and payment service providers should set the 3DS Requestor Challenge Indicator as follows when sending EMV 3DS Authentication Requests (AReqs):

3DSRequestorChallengeInd = 04

Issuers should subject such transactions to a challenge flow, unless there is an overriding inclusion, accessibility, or other countermanding regulatory requirement that allows a cardholder challenge not to be applied by exception. In the Arcot platform, the easiest way to follow the correct behavior is subscribe to the RCI - Challenge Mandate policy in Risk Analytics.

Recommendation 2: Leverage the EMV 3DS Data Share Only Flow

Scope: Worldwide

As per the EMV 3DS Core Specification, the value of *06* corresponds to *No challenge requested (Data share only)*, meaning the merchant is sending this EMV 3DS Authentication Request simply to share insights about a payment transaction. Per the EMV 3DS protocol, an RCI 06 transaction cannot be challenged. Card scheme authentication programs therefore do not offer liability shift on RCI 06 transactions.

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.
- Non-PSD-2 markets, which do not have prescribed rules for cardholder challenges, can leverage Data Share Only flows to optimize authorization approvals for e-commerce transactions with zero risk of friction.
- EMV 3DS is a tool that merchants and issuers can use to optimize cardholder journeys by removing friction for low-risk transactions that do not need to be challenged, and stopping fraud by challenging or denying risky transactions. EMV 3DS enables merchants and issuers to share rich transaction data in order to cooperate to achieve these twin objectives.

How to Implement

Merchants, acquirers, and payment service providers should set the 3DS Requestor Challenge Indicator as follows:

3DSRequestorChallengeInd = 06

For issuers on the Arcot platform, issuers should subscribe to the RCI - Data Share Only policy in Risk Analytics. If the Risk Analytics Policy is NOT used, and an issuer is managing the RCI 06 logic with their own rules, the key field to consider is the threeDSRequestorChallengeInd and (RCI as defined by the EMV 3DS protocol), which in turn maps to the Risk Analytics elements 3DS2_REQUESTOR_CHALLENGE_INDICATOR in the Arcot platform.

Learn More

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