SOLUTION BRIEF

Q2 2023

Arcot EMV 3DS Processing Recommendations for PSD2

Welcome to the second quarter 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 in the context of the PSD2 regulations.

EMV 3DS is the optimal way to process PSD2 SCA and associated SCA exemptions for card payments. In a survey of EU issuers and merchants conducted by Arcot in March 2023, two-thirds of participants cited sending transactions via the "Direct to Authorization" rail, i.e. trying to bypass EMV 3DS, gave the lowest success rate overall, while only one respondent asserted that Direct to Authorization performed best.

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 in order to share insights across the ecosystem with a view to maximizing success rates while minimizing fraud rates. Accordingly, Arcot is delighted to present its second-quarter recommendations for EMV 3DS optimization for issuers and merchants, and we will be continuing to publish recommendations in the future with the intention of helping the entire ecosystem get the benefits of improved transaction conversion and success rates via EMV 3DS.

Issuer Recommendations

Prioritize the Acceptance of Acquirer TRA

Issuers should give favorable treatment to 3DS transactions where Acquirer TRA SCA exemption is being claimed.

Benefits and Why

- Exemptions to PSD2 SCA should be applied to as many transactions as feasible to offer the best cardholder experience.
- When the Acquirer TRA exemption is claimed, the Acquirer is asserting that, based on their risk assessment, the transaction is sufficiently low risk and within their allowed ETV thresholds to qualify for an SCA exemption.
- If the issuer accepts the Acquirer TRA exemption for the transaction fraud chargeback liability, which would otherwise be shifted to the issuer for a 3DS transaction, is shifted back to the merchant.

How to Implement

- The Acquirer TRA exemption is indicated by the incoming 3DS AReq message containing the value "05" for the threeDSRequestorChallengeInd.
- Acquirer TRA should only be considered for in-scope PSD2 transactions, indicated by the Risk Analytics Elements RA_com_isPayeePSD2 = Y (for the merchant being in-scope) and RA_com_isPayerPSD2 = Y (for the issuer being in-scope).

- Specific risk-scoring policies can be configured in Risk Analytics to enable Acquirer TRA exemptions to be approved frictionlessly. In addition to the threeDSRequestorChallengeInd a risk rule may also consider other EMV 3DS data elements to enable merchant-specific risk policies to be implemented.

EMV 3DS Data Element	Risk Analytics Data Element	Notes
threeDSRequestorChallengeInd	3DS2_REQUESTOR_CHALLENGE_INDICATOR	Test for the value 05.
merchantName	MERCHANT_NAME	Merchant name. May be used to apply more or less flexible thresholds based on the identity of the merchant on whose behalf the Acquirer PSP is claiming the TRA exemption.
mcc	MERCH_CAT	Merchant Category Code. May be used to create more flexible thresholds based on the type of merchant involved in the transaction. For example, Acquirer TRA might have higher risk tolerance thresholds for a gaming/gambling merchant.
acquirerBIN	ACQ_BIN	Identification code for the merchant's acquirer. May be used to apply more or less flexible thresholds based on the identity of the Acquirer PSP claiming the TRA exemption.
acquirerMerchantID	MERCHANT_ID	Identification code for the merchant, as assigned by the Acquirer. A given merchant will have multiple IDs if they use multiple Acquirers. May be used to apply more or less flexible thresholds based on the identity of the merchant on whose behalf the Acquirer PSP is claiming the TRA exemption.

Maximize the Use of the Issuer TRA Exemptions

If the transaction doesn't qualify for an SCA exemption on the basis of the Acquirer TRA exemption, the issuer should apply for the Issuer TRA exemption as flexibly as possible to approve transactions frictionlessly.

Benefits and Why

- Exemptions to PSD2 SCA should be applied to as many transactions as feasible to offer the best cardholder experience.
- The concept of Issuer Transaction Risk Analysis is the most well-established method for approving transactions frictionlessly, with issuers applying "Risk-Based Authentication" principles for more than 15 years. Issuer TRA thus represents "Business As Usual", subject to the PSD2 ETV limitations for TRA.

How to Implement

- Although Risk-Based Authentication can be applied worldwide, to apply Issuer TRA correctly under PSD2, in-scope PSD2 transactions are indicated by the Risk Analytics Elements RA_com_isPayeePSD2 = Y (for the merchant being in-scope) and RA_com_isPayerPSD2 = Y (for the issuer being in-scope).
- Issuer TRA can only be applied to transactions within certain value limits, depending on the issuer's fraud rate. Accordingly, the Risk Analytics "AMOUNT" data element must be tested against the Issuer's current value threshold (the so-called "ETV").
- The RA predictive model score is central to the application of Issuer TRA. The model score is available in the PREDICTIVE_SCORE Data Element.

Implement the Trusted Beneficiary Exemption

Finally, where no TRA exemption applies to the transaction, the Trusted Beneficiary exemption should be considered. Issuers should offer cardholders the ability to add merchants to their Trusted Beneficiary lists via the Arcot for Issuers platform features that support Trusted Beneficiary management and exemption application.

Benefits and Why

- Exemptions to PSD2 SCA should be applied to as many transactions as feasible to offer the best cardholder experience.
- Trusted Beneficiary can be applied as an SCA exemption to any transaction, of any value, regardless of fraud rate, where the cardholder has added the merchant to their personal list of Trusted Beneficiaries. It is a very flexible exemption, therefore, with no complex eligibility criteria.

How to Implement

- The Trusted Beneficiary SCA exemption should only be considered for in-scope PSD2 transactions, indicated by the Risk Analytics Elements RA_com_isPayeePSD2 = Y (for the merchant being in-scope) and RA_com_isPayerPSD2 = Y (for the issuer being in-scope).

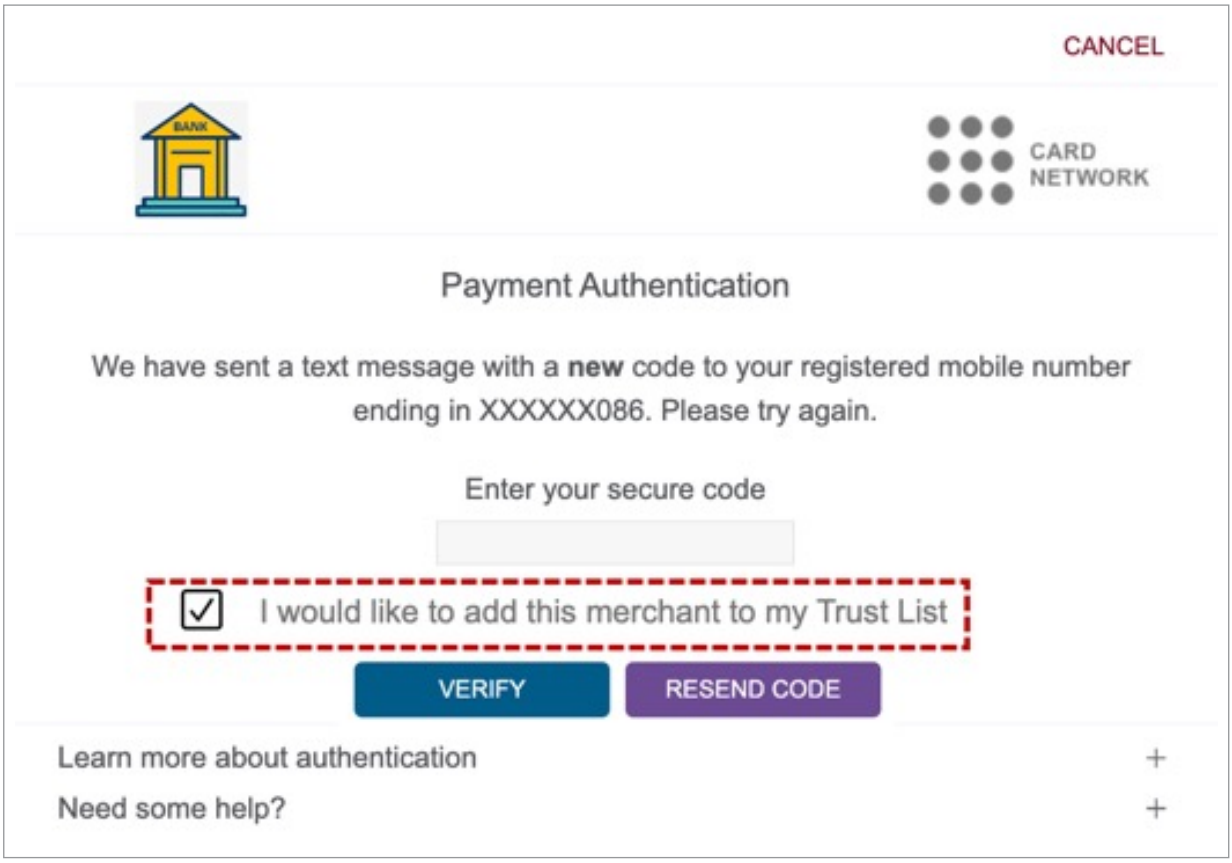
A "best practice" Trusted Beneficiary implementation should leverage features of the Arcot for Issuers platform as well as possible issuer back-end integrations to enable cardholder management of cardholder Trusted Beneficiary lists.

There are two main phases to consider:

- Trusted Beneficiary list management
- Trusted Beneficiary Exemption application to transactions

Trusted Beneficiary List Management

- Trusted Beneficiary lists must be maintained by the cardholder. The Arcot for Issuers platform integrates per-cardholder TB lists.
- Arcot for Issuers can be configured for an issuer to offer a user journey that prompts the cardholder whether they would like to trust the current merchant during a challenge flow. Refer to an example screenshot below.
- A merchant can set the threeDSRequestorChallengeInd field to the value "09" to request the issuer to challenge a cardholder for the explicit purpose of adding the merchant to a cardholder's TB list. Issuers should test for this value in their Risk Analytics policy and return risk advice of "STEP-UP".
- APIs are exposed by the Arcot for Issuers platform to enable Trusted Beneficiaries to be added and deleted for a cardholder. This enables an issuer to offer TB management interfaces, for example via existing customer portals or customer support tools.



Applying the Trusted Beneficiary Exemption

- The RA Element "FM_atn_is_TrustedBeneficiary" is set to "Y" if the current merchant name, or merchant ID, is found in the cardholder's list of Trusted Beneficiaries. A Risk Analytics rule should be created to "ALLOW" transactions for a Trusted Beneficiary, or to DENY high-risk transactions. Arcot does not recommend putting high-risk transactions to a challenge flow; doing so may confuse the cardholder.

Metrics

Combining these recommendations, Arcot would encourage issuers to consider the following Key Performance Indicators as representative of successful implementation.

Metric	KPI	Comments
Authentication Success Rate	>94%	ASR > 90% is achieved in many regions today and is generally dependent on reducing the challenge rate.
Challenge Rate	<15%	Certain schemes/issuer/merchant combinations demonstrate that very low Challenge Rates are achievable.

Recommendation Roadmap

Arcot intends to publish these recommendations on a periodic basis. Future "Recommendations" guidance will include:

- Use of frictionless flows to reduce challenges and associated social engineering fraud.
- Migration of SCA challenge journeys from SMS OTP to mobile app multi-factor authentication.

Social engineering of authentication challenges is a significant problem affecting many online channels since the introduction of PSD2. A combination of approaches to mitigate this issue are being applied, such as additional risk intelligence during the challenge process to try to detect and prevent subversion of the challenge flow.

The objective of reducing SCA challenges should also be considered as a line of defense against the social engineering of SCA challenges. Reducing the challenge rate reduces the "attack surface". Issuers may wish to increase their DENY rate for high-risk transactions or certain transaction types and merchant category codes to reduce the likelihood of an SCA challenge being subverted. In the Autumn of 2023, the Arcot platform will be enhanced to support the flagging of RA Cases marked as fraudulent with a reason code to indicate Social Engineering as the cause.

Arcot strongly recommends issuers have an active strategy to migrate to mobile app-based multi-factor authentication for qualified cardholders (e.g. based on vulnerability/accessibility requirements, smartphone-enabled, etc.). This will be covered in more detail in a future version of these recommendations, however migrating from SMS OTP will drive down costs, reduce fraud, and enable cardholders to interact consistently across digital channels and services with the bank.

Merchant Recommendations

Leverage Acquirer TRA Exemption to the Maximum Extent

Merchants, Acquirers, and Payment Service Providers should request the Acquirer TRA exemption via EMV 3DS for as many eligible transactions as possible, subject to the applicable ETV thresholds.

Benefits and Why

- Exemptions to PSD2 SCA should be applied to as many transactions as feasible to offer the best cardholder experience.
- When the Acquirer TRA exemption is claimed, the Acquirer is asserting that, based on their risk assessment, the transaction is sufficiently low risk and within their allowed ETV thresholds to qualify for an SCA exemption.
- To complement this guidance to merchants, Arcot is encouraging issuers to process transactions where Acquirer TRA is requested frictionlessly, not challenging those transactions and only denying those where the risk of fraud is high.

How to Implement

- The Acquirer TRA exemption is indicated by sending the 3DS AReq message containing the value “05” for the threeDSRequestorChallengeInd.
- Merchants should remain aware that they remain liable for fraud chargebacks when Acquirer TRA is claimed (as is the default case in e-commerce transaction) and should consider this when receiving chargeback claims on authenticated transactions.

Data Consistency

Merchants, Acquirers, and Payment Service Providers should be diligent in properly encoding data via the various EMV 3DS fields.

Benefits and Why

- Accurate, consistent, high-quality data enables merchants and issuers alike to properly evaluate the EMV 3DS data fields for fraud risk, maximizing both the likelihood of a frictionless flow and stopping the greatest amount of fraud.
- The chance of EMV 3DS requests being rejected owing to processing errors at the Directory Server or issuer ACS is reduced.
- Over time merchant 3DS Server providers and issuer ACS providers will be able to optimize their analytics, based on complete and good quality data, to reduce friction and stop fraud.

How to Implement

- **Use correct ISO codes:** where country or currency codes are specified by the EMV 3DS protocol, use valid currency codes (ISO 4217) and country codes (ISO 3166). (note that the EMV 3DS Protocol Specification defines certain currency code exceptions for irregular currencies such as precious metals).
- **Avoid hard-coding values:** Use real data, e.g.actual supplied transaction data; data gathered through device fingerprinting or an EMV 3DS SDK; contextual data such as timestamps, merchant IDs and names, etc. Where hard-coded placeholders are coded to avoid implementing real data collection but to comply with field inclusion requirements, these tend to trigger fraud and velocity rules at the issuer ACS, resulting in unnecessary transaction declines.
- **Send real, publicly routable, IP addresses:** ACSes use IP addresses to geolocate the cardholder involved in the transaction and to incorporate reputational risk insights associated with IP addresses as part of overall risk assessment. Sending RFC1918 non-routable IP addresses (e.g. those from a device’s local network interface, perhaps from a WiFi hotspot, home network, or similar) or hard-coded values such as “127.0.0.1” or “0.0.0.0” reduce the effectiveness of the ACS risk assessment, driving more challenge flows or transaction declines. E-commerce websites should always give some concept of the remote IP of the cardholder device that is in session with the merchant and it is ideal if such IP addresses are included in the browserIP field of the AReq message (for browser-based transactions), or, if possible, in field C010 of the SDK Device Data for SDK-based transactions (nb: in EMV 3DS 2.3.1 a new appIP field is being introduced to make the inclusion of a public IP for SDK transactions).

- **Use the 3DS Requestor Challenge Indicator consistently:** Take note of the values for the threeDSRequestorChallengeInd and, at minimum, avoid setting no value or the value "01 No Preference" for this field. Brief guidance regarding the most common values for this field is listed below.

Value	Meaning	Effect
02	Merchant requesting the transac-tion not to be challenged by the issuer.	Issuer ACS should allow or deny the transaction but not step it up with an au-thentication challenge (unless legally re-quired by PSD2).
03	Challenge requested by the 3DS Server (i.e. merchant).	Issuer should challenge the cardholder as requested by the merchant, who may be wanting an SCA for adding a Card on File or card tokenization for example.
04	Challenge mandated.	Merchant is operating in a circumstance where a challenge is mandated by regula-tion or scheme rules, for example during token provisioning.
acquirerBIN	ACQ_BIN	Identification code for the merchant's acquirer. May be used to apply more or less flexible thresholds based on the identity of the Acquirer PSP claiming the TRA exemption.
05	Acquirer TRA.	Discussed above.

Share Merchant Risk Level Indicator with Issuers

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

Benefits and Why

- 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

Firstly, merchants should determine a set of buckets to separate transactions into low, medium, and high-risk buckets according to their scoring process as follows:

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 follows:

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

Metrics

Combining these recommendations, Arcot encourages merchants and acquirers to consider the following Key Performance Indicators as representative of successful implementation.

Learn More

Contact your Customer Success Manager to learn more about EMV 3DS Processing Recommendations for PSD2.

Metric	KPI	Comments
Authentication Success Rate	96%	ASR > 90% is achieved in many regions today and is generally de-pendent on reducing the challenge rate.
Challenge Rate	15%	Certain schemes/issuer/merchant combinations demonstrate that very low Challenge Rates are achievable.

BROADCOM®
connecting everything®

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