SOLUTION BRIEF

Issuer Recommendations

- Correct Treatment of the 3DS Requestor Challenge Indicator
- Trusted Beneficiary and PSD2 SCA Exemption Order
- PSD2 SCA Exemption Ordering Recommendations
- Approve Authenticated Transactions at Authorization Time

Merchant Recommendations

- Use the 3DS Requestor Challenge Indicator
- Data Consistency
- Share Merchant Risk Level Indicator with Issuers

2H 2023

Arcot EMV 3DS Processing Recommendations

Welcome to the second edition of the Arcot EMV 3DS Processing Recommendations. These recommendations are published to help the industry optimize EMV 3DS processing, both worldwide and in the context of European revised Payment Services Directive (PSD2) regulations.

The ultimate objective is simple: **Improve authorization success rates for merchants and issuers by using EMV 3DS.**

EMV 3DS is the optimal way to share rich transaction metadata that can be used to improve authorization rates, orchestrate an authentication challenge where required, and 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 and has many features that can be actively exploited in order to share insights across the ecosystem, with a goal of maximizing success rates while minimizing fraud rates.

Accordingly, the Arcot division is delighted to present its second half of 2023 recommendations for EMV 3DS optimization for issuers and merchants. Additionally, the Arcot team will continue to publish recommendations in the future with the intention of helping the entire ecosystem receive the benefits of improved authorization rates using EMV 3DS.

Issuer Recommendations

Correct Treatment of the 3DS Requestor Challenge Indicator

Scope: worldwide.

Merchants are advised to make proper use of the 3DS Requestor Challenge Indicator field. This is a field that merchants can use to signal a preference to the access control server (ACS) with respect to cardholder challenges. This field was discussed as part of the broader recommendation on data consistency presented in the previous version of these processing recommendations. However, in the real world, its use still shows a very high degree of inconsistency between merchants and geographies.

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 3DS Request Challenge Indicator coding, it's important for issuers to have a consistent set of behaviors that merchants can rely on.

How to Implement

- The key field is the threeDSRequestorChallengeInd (as defined by the EMV 3DS protocol), which in turn maps to the Risk Analytics element 3DS2_REQUESTOR_CHALLENGE_INDICATOR (RCI) in the Arcot platform.
- There are many values for this field. However, the most important values to highlight are shown in the table below. The column Challenge Request (CR) is a red, amber, green indication of whether the challenge rate should be highest (red), medium (amber), or lowest (green).

3DS RCI Value	Summary	CR	Recommendation
<blank> or 01	Merchant is expressing no preference.		Issuers should apply risk-based authentication, and apply SCA exemptions where PSD2 applies. Issuers should strive to minimize the challenge rate, even when the merchant expresses no preference.
02	No challenge requested.		As per the following merchant recommendations, the merchant is signaling that they consider this transaction to be sufficiently low risk that the issuer should strongly consider not challenging the cardholder. Issuers are recommended to reduce their challenge rates for these transactions, while monitoring success rates and fraud rates.
03	Challenge requested.		As per the following merchant recommendations, the merchant is signaling that they may consider this transaction to be a higher risk, and they are recommending that it be challenged. Issuers are recommended to increase their challenge rates for these transactions, while monitoring success rates and fraud rates.
04	Challenge mandated.		There are scenarios where the merchant knows, either by card scheme rules or according to PSD2, that a transaction requires an authentication challenge. Examples would be wallet and token provisioning, which card schemes require to be challenged, the initial transaction of a recurring series, and similar use cases. Issuers must challenge these transactions.
05	Acquirer TRA.		This field applies to PSD2 regions and signals the merchant is claiming the Acquirer Transaction Risk Analysis exemption. Refer to the Arcot 2Q 2023 Processing Recommendations for further information. Note: the Acquirer's ETV may be different from the Issuer's ETV so, other than verifying the transaction is no greater than EUR 500, no other amount should be checked as part of this rule.
06	Information Only.		This flow exists to enable a merchant to send rich transaction data to the issuer for risk evaluation, however an Information Only transaction cannot be challenged by the ACS. This flow guarantees the merchant a 100% frictionless allow/deny decision, in exchange for retaining liability for fraud chargebacks, contrary to the default rules for 3D Secure cardholder authentication programs. Note: EMV 3DS specifically disallows these transactions to be challenged. Therefore, unless the transaction is explicitly Denied by a rule, Risk Analytics will Allow the transaction.

Trusted Beneficiary and PSD2 SCA Exemption Order

Scope: PSD2 regions. Worldwide for the concept of cardholder trusted merchant lists.

This applies primarily to PSD2 markets. However, the concept of Trusted Beneficiaries is potentially beneficial in non-PSD2 regions. The use of the Trusted Beneficiary SCA exemption was covered in detail in the 2Q 2023 Arcot Processing Recommendations. However, this is such an important and powerful exemption that it remains on the list of issuer recommendations for now. Early adopter issuers who have deployed the Trusted Beneficiary exemption reduce challenge rates by about 40% on average, with a 20 basis point reduction in total fraudulent transactions. For further details regarding Trusted Beneficiary, refer to the 2Q 2023 Processing Recommendations.

In PSD2 markets, Trusted Beneficiary is one of several SCA Exemptions. Therefore, this version of the processing recommendations will also consider the proper ordering of exemptions (that is, the most preferable exemption to apply in a given scenario when a transaction could qualify for multiple SCA Exemptions).

Myth Busting

Another point that should be emphasized with regards to Trusted Beneficiary is that, despite the name of the Exemption, the Exemption applies solely to the consideration of whether to put a given transaction through an authentication challenge flow. There is no expectation or requirement to automatically authorize payments to Trusted Beneficiaries (other than in the following general case that is presented, which recommends that 3DS transactions be authorized more favorably in general). The ecosystem often confers assumed meaning to the idea of a "Trusted" merchant, when all this exemption refers to is the process of the cardholder recording a preference for frictionless flows when shopping with a given merchant.

Benefits and Rationale

- Exemptions to PSD2 SCA should be applied to as many transactions as feasible to offer the best cardholder experience.
- Trusted Beneficiary is the only exemption that can be applied to low-risk, high-value transactions. Arcot division analysis suggests that despite only accounting for about 6% of transaction volume, these transactions represent about 40% of cumulative 3DS value.
- Trusted Beneficiary can be applied as an SCA exemption to any transaction, 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.
- Proper ordering of SCA Exemptions under PSD2 is important to maximize the application of Exemptions to the greatest transaction volume overall.

How to Implement

- Refer to the 2Q 2023 Arcot Processing Recommendations for details of how the Arcot platform implements Trusted Beneficiary election and list management by cardholders.
- In the Arcot platform, 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.
- Other ACS platforms will have some similar process to flag that a given transaction is occurring at a previously selected Trusted Beneficiary.
- While an issuer retains the right to put a transaction at a Trusted Beneficiary merchant to a challenge flow, Arcot does not recommend putting high-risk transactions to a challenge flow as doing so may confuse the cardholder. It should be acknowledged however that this remains an issuer choice.

PSD2 SCA Exemption Ordering Recommendations

The following table gives recommendations for the application of SCA Exemptions to a transaction, from most preferable to least preferable. There is a "Secure Corporate Payment" Exemption (RTS Article 17), however, this is not considered in the following table, which focuses on retail card payments. Additionally, the "Payments to self" (Article 15) exemption is not considered, as this would almost never apply to a card payment.

Exemption	Comments
Trusted Beneficiary (Article 13)	Because Trusted Beneficiary has no additional qualification criteria, and because it represents a cardholder's recommendation to skip being challenged at the merchant, and also because it performs extremely well in the real world in terms of reduced challenge rate and low fraud rate, Trusted Beneficiary should be applied to qualifying transactions in preference to most other SCA Exemptions.
Acquirer TRA (Article 18)	This was covered in detail in the 2Q 2023 Arcot Processing Recommendations. If the merchant is indicating that the transaction qualifies for an SCA Exemption under Acquirer TRA then this should be considered in preference to Issuer TRA (as follows) because the merchant retains fraud liability.
Issuer TRA (Article 18)	This was also covered in detail in the 2Q 2023 Arcot Processing Recommendations. Low Risk transactions should next be considered for the Issuer TRA Exemption subject to the ETV and fraud rate qualification and reporting criteria for this exemption.
Low Value Transaction (Article 16)	This should be the "last resort" SCA Exemption because it only applies to the lowest value transactions €30/£25, and it is subject to a usage cap of either five times or a cumulative total value of exempted transactions of €100/£85, after which SCA must be applied even if the transaction is of a low value. If a low value transaction qualifies for an Exemption under any other Exemption above it should be applied in preference in order to retain the greatest number of "slots" to use for transactions that would otherwise only be exempt under the LVT rules.

Approve Authenticated Transactions at Authorization Time

Scope: worldwide.

All of the major card networks report that authorization rates for successfully authenticated transactions are higher than for non-authenticated transactions. For example, data presented by one of the major card brands in October 2023 demonstrated that authorization rates on authenticated e-Commerce transactions in Europe are approximately 3% higher than for non-authenticated transactions. That is a huge difference in performance, and one that must continue to be focused on. Accordingly, correct and preferential treatment of authenticated transactions at authorization time is, and will remain, a vital focus area for the time being.

This is a technically complicated topic and will be described further in the following sections. However, the recommendations for issuers can be summarized as follows:

1. Consider applying higher authorization approval rates to fully-authenticated transactions.
2. Consider any additional supporting data regarding the fully-authenticated status that is available in the authorization message.

The following descriptions summarize the specific authorization message variations between Visa and Mastercard that allow these high-level recommendations to be implemented.

Benefits and Rationale

- The benefits are simple: a higher authorization approval rate translates directly to the bottom line for merchants and issuers, boosting sales revenue, interchange, and credit lending interest.

How to Implement

A full breakdown of authorization data elements and fields by payment network is outside the scope of this document. However, some general recommendations about the proper identification of authenticated transactions in the authorization stream can be given, as well as guidance on some more specific data points issuers may wish to consider at authorization time.

In the following descriptions, the Authorization Message Data Elements (DE) and/or Sub-Elements (SE) (Mastercard parlance) or Fields (Visa parlance) have been noted for reference. Complete references can be found as follows:

- **Mastercard Identity Check:** Appendix I of the Identity Check Program Guide, as well as the spreadsheet "MCIdentityCheckProcessingMatrix", and the "Single Message System Specifications".
- **Visa Secure:** Visa Secure Program Guide, section 1.5.2 Authorization Flow; Visa Secure CAVV Guide; and the VisaNet Authorization Only Online Messages Technical Specifications.

The principal fields to consider at authorization time are the e-Commerce Indicator (ECI) and the Authentication Value (AV). The AV is a cryptogram which provides a proof of the authentication outcome and, usually, some additional contextual data about the authentication transaction to the authorization host.

The payment networks define their AV and ECI fields differently. Visa uses the Cardholder Authentication Verification Value (CAVV) Usage 3 Version 7 for EMV 3DS Payment Authentications and Mastercard defines the SPA2 Accountholder Authentication Value (AAV). The networks also use different "private use" field specifications for transporting the Authentication Value in the authorization message. Visa uses Data Element/Field 126.9 to transport the CAVV and associated data. Mastercard uses Data Element 48 Subelement 43 to transport the AAV in the UCAF field.

Authentication Values are intended to be validated from the transaction data in real time to protect against fraudulent misrepresentation of fully authenticated transactions. Most issuers use in-network services for this verification. However, it is possible for the authorization host system to perform the verification.

- Issuers are recommended to identify ECI 02/05 transactions for higher approval rates.
- At the highest level, authenticated transactions are identified by the ECI field. The different scheme encodings for the ECI are shown in the following table:

Scenario	Visa	Mastercard
Fully, successfully authenticated, frictionlessly or using challenge	05	02
Authentication attempted by the merchant, but a stand-in process was applied (for example, card range not enrolled, ACS could not be reached, and so on.)	06	01
Authentication was declined, not available, not attempted at all.	07	00
"Information Only" 3DS flow (also, Mastercard: PSD2 Acquirer TRA Exemption claimed)	07	06

- Mastercard maps the ECI value to Position 3 (UCAF Collection Indicator) of DE48 SE42. Visa maps the ECI to Positions 9-10 of Field 60.8.

Additional Data to Consider at Authorization Time

When considering fully authenticated transactions for higher authorization rates, issuers may also wish to consider additional insight data that may be available in the authorization stream. For example, some networks can encode the device IP address; all the networks can communicate information about the authentication type, or type of exemption for a frictionless transaction. Examples of additional data by payment network are listed in the following table:

Visa Field 126.9 CAVV U3v7 Additional Data Summary	
Byte 1 Authentication Results Code	Outcome of 3DS Authentication, detailing whether fully authenticated, attempted, declined, or whether merchant SCA Exemptions were claimed (for example, Acquirer TRA), Data Share Only transactions.
Byte 2 Authentication Method	For challenged transactions, the specific challenge method that was applied. An issuer with multiple challenge methods (for example, mobile app and SMS OTP) could apply higher approval rates for stronger authentication methods less susceptible to social engineering.
Bytes 17-20 IP address (if encoded by the ACS)	Can be used to encode the cardholder device IP address that was seen by the ACS.
Mastercard Data Element 48 Summary	
SE 22 Low Risk Merchant Indicator	Indicates the type of PSD2 SCA Exemption applied in the case of a frictionless transaction.
SE 42 Security Level Indicator	The SLI could be viewed as a more granular form of ECI and, in conjunction with the first two leading bytes of the AAV, helps to differentiate a variety of 3DS flows at authorization time, such as frictionless scenarios, challenge failure scenarios, and so on.
SE 43 AAV	The AAV value is generated and validated in-network by Mastercard, however the first two bytes are referred to as the "Leading Indicator" and in conjunction with the SLI, are useful in having a granular understanding of the specific 3DS flow that was applied. The fields are also important in determining liability shift rights.
SE 66 DS Transaction ID	Although not necessarily useful at authorization time, the DS Transaction ID is nonetheless useful to record as it can aid matching of transactions subsequently, for example, in fraud reporting to ACS providers, dispute processing, and so on.

Merchant Recommendations

Use the 3DS Requestor Challenge Indicator

Scope: worldwide.

As discussed in the Issuer Recommendations section, merchants are advised to make proper use of the 3DS Requestor Challenge Indicator field. This is a field merchants can use to signal to the ACS a preference with respect to cardholder challenges. This field was discussed as part of the broader recommendation on data consistency presented in the previous version of these Processing Recommendations, however in the real world its use still shows a very high degree of inconsistency between merchants and geographies.

Merchants outside of PSD2 regions, such as North America, should pay particular attention to the value 06 "Information Only", which is a 3DS flow that guarantees no issuer challenge in exchange for the merchant retaining fraud chargeback liability.

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 the current transaction is fraudulent. Merchants should pass these insights and preferences to issuers in order for them to challenge at an appropriate rate for the type of transaction.

How to Implement

The key field is the threeDSRequestorChallengeInd (as defined by the EMV 3DS protocol). This field will be referred to by the shorthand "RCI" in the remainder of this section.

There are many values for this field. However, the most important values to highlight are shown in the following table. The column "CR" is a red, amber, or green indication of whether the challenge rate should be highest (red), medium (amber), or lowest (green).

3DS RCI Value	Summary	CR	Recommendation
<blank> or 01	Merchant is expressing no preference.		A merchant should *never* omit a value for the 3DS Requestor Challenge Indicator, nor set the value 01.
02	No challenge requested.		Merchant is expressing a preference that no challenge be applied to this transaction. For this field to be considered by issuers, it's important that there is a rationale for merchants to request that a challenge not be performed. Merchants are recommended to request no challenge when they have a reasonable basis to consider the transaction a lower fraud risk. See also the subsequent recommendation for encoding a merchant risk indication to accompany this field.
03	Challenge requested.		As with the "No Challenge Requested" value, for this field to be considered by issuers, it's important that there is a rationale for merchants to request that a challenge *should* be performed. Merchants are recommended to request a challenge when they have a reasonable basis to consider the transaction a *higher* fraud risk. See also the subsequent recommendation for encoding a merchant risk indication to accompany this field. Scenarios where a challenge is required can be covered as follows.
04	Challenge mandated.		There are scenarios where the merchant knows, either by card scheme rules or according to PSD2, that a transaction *requires* an authentication challenge. Examples would be wallet and token provisioning, which card schemes require to be challenged, the initial transaction of a recurring series, and similar use cases. When a merchant knows that a given transaction must be challenged under scheme rules or regulations, they should set this value.
05	Acquirer TRA.		This field applies to PSD2 regions and signals the merchant is claiming the Acquirer Transaction Risk Analysis exemption. Refer to the Arcot 2Q 2023 Processing Recommendations for further information.
06	Information Only.		This flow exists to enable a merchant to send rich transaction data to the issuer for risk evaluation, however an Information Only transaction cannot be challenged by the ACS. This flow guarantees the merchant a 100% frictionless allow/deny decision, in exchange for retaining liability for fraud chargebacks, contrary to the default rules for 3D Secure cardholder authentication programs. Merchants are recommended to consider this flow, especially in non-PSD regions. Merchants should work with their acquirer as the card scheme may require advance notice of the use of this flow to ensure correct processing at the Directory Server.

Data Consistency: Specific Recommendations

Scope: worldwide.

As covered in the 2Q 2023 Arcot Processing Recommendations, Merchants, Acquirers, and Payment Service Providers should be diligent in properly encoding data using the various EMV 3DS fields. In this document, some specific fields that are often problematic are discussed in more depth.

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

Some specific frequently-problematic fields and scenarios are discussed in the following sections.

Hard-Coded and Default Values

Merchants should always use real data. For example, actual supplied transaction data, data gathered through device fingerprinting or an EMV 3DS SDK, contextual data such as timestamps, merchant IDs and names, and so on. When constructing EMV 3DS messages. "Default" or "hard coded" test, placeholder, and similar values should not be sent using EMV 3DS.

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. Scenarios in the real world include hard-coded IP addresses or device ID data, which has the effect of making single devices appear to be responsible for a merchant's entire transaction volume, which in turn drives up the challenge and deny rates for that merchant.

IP addresses

Always 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 (for example, those from a device's local network interface, perhaps from a Wi-Fi 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 will always have some concept of the remote IP of the cardholder device that is in session with the merchant and it is ideal if those 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 (Note: in EMV 3DS 2.3.1, a new appIP field is being introduced to make the inclusion of a public IP for SDK transactions).

Invoke the 3DS Method URL

The 3DS Method URL is essential where the cardholder is shopping using a web browser, as opposed to a mobile app (in certain cases a mobile app can be browser-based, therefore this recommendation would also apply to those apps).

The 3DS Method URL is used by Issuer ACSes to recognize cardholder web browsers. This is a very important input for ACS risk evaluation. Recognizing browsers helps the ACS to understand if this is a device or browser the cardholder has previously used for low risk, successful transactions, or, conversely, if this is a browser associated with higher risk, even fraudulent activity.

The 3DS Method URL for a card range is stored at the Directory Server, and is retrieved periodically by the merchant's 3DS Server using the threeDSMethodURL field of the PRes message.

It is not a ***requirement*** for an ACS to have a 3DS Method URL, however if one is present the merchant should embed it into their checkout pages and invoke it. As with any third-party scripted content the merchant may have security, integration, and other due diligence considerations prior to integrating the 3DS Method URL, and merchants should always follow organization-specific security policies and guidance. The 3DS method can be called when a payment card has been selected. At this time, any 3DS Method URL associated with the card range is known and can be invoked. There is no need to wait until the AReq message has been prepared or similar; the 3DS Method should be invoked as soon as the correct method to call based on the card is known.

Share Merchant Risk Level Indicator with Issuers

Scope: worldwide.

This recommendation was also given in the previous version of these recommendations. It is being re-presented 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 are addressing 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 using 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

- First, merchants should determine a set of buckets to separate transactions into low, medium, and high-risk, 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

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

BROADCOM®
connecting everything®

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

Arcot-EMV-3DS-Recommendations-2H2023-SB100 November 22, 2023