PSD2 SCA for Remote Electronic Transactions Implementation Guide

February 2023

Version 4.0
28 February 2023

VISA

Contents

Important Information

Disclaimer: Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice.

This document represents Visa's position at time of writing but should not be considered as legal advice, and it is subject to change in light of competent authorities' guidance and clarifications. Visa reserves the right to revise this guide pending further regulatory developments. We encourage clients to contact Visa if they experience challenges due to conflicting guidance from NCAs. Where it makes sense, Visa will proactively engage with regulators to try and resolve such issues.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required.

This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

References to liability protection, when used in this context throughout this guide, refer to protection from fraud-related chargeback liability under the Visa Rules.

Note on references to EMV 3DS, 3-D Secure 2.0 and 3DS 2.0: When in this document we refer to 3-D Secure 2.0 or EMV 3DS this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1.0 of the specification is referred to as EMV 3DS 2.1 and version 2.2.0 is referred to as EMV 3DS 2.2. Visa rules do not preclude Issuers and Acquirers agreeing alternative means of performing SCA.

Examples in this document show transactions processed through VisaNet. Visa supports the use of third party processors. Contact your Visa Representative to learn more.

Using this document

This guide forms part of a set of Visa guidance documents that are relevant to the implementation of Strong Customer Authentication (SCA) under PSD2 in the European Economic Area (EEA)[1] and the United Kingdom (UK). The guide is written for business, technology and payments managers responsible for the planning and implementation of SCA policies and solutions within Issuers, Acquirers, merchants, gateways and vendors. It aims to provide readers with guidance to support business, process and infrastructure policy decisions needed to ensure the successful application of SCASCA. It is supported by more detailed implementation guides and other documents that are listed in the bibliography in Section 6.

This guide covers remote electronic payments.

SCA also applies to card present payments, including contactless payments and electronic payments made using devices including mobile handsets and wearables in a "face to face" environment. Please see *Visa Contactless and Card Present PSD2 SCA: A Reference Guide to Implementation* for more details.

This guide is structured as follows:

Section	Title	Description
1	Introduction: Visa's guiding principles for PSD2 SCA	An overview of Visa's guiding principles for PSD2 and corresponding focus for SCA
2	The requirements of PSD2 Strong Customer Authentication and Visa's interpretation	Summarizing Visa's interpretation of the PSD2 SCA requirements
3	Visa's SCA Solutions	Providing the essential information needed to interpret Section 4 of this document It details the range of tools and services Visa has made available to merchants, Issuers and Acquirers to optimize the application of SCA and allowable exemptions, including EMV 3DS, authentication and authorization message fields & values and Visa Rules
4	Optimizing the payment	Providing information and guidance to help clients set their policies for application of SCA and exemptions. It describes the:

[1] Additionally, SCA may apply to transactions in regions that are associated with countries within the EEA. Examples include micro-states and city-states in Europe, along with territories of EEA Countries outside of Europe. See Appendix A.4 for more details.

Section	Title	Description
	experience under PSD2 SCA	• Key principles and considerations that govern authentication and authorization flows • Options available for clients in terms of authenticating transactions and applying exemptions • Considerations to take into account when deciding how to handle transactions Guidance on managing of out of scope transactions and individual exemptions
5	Payment use cases and sector specific guidance for merchants and PSPs	Describing the recommended authentication and authorization flows for key common and complex payment use cases The section provides merchants with additional guidance on the application of SCA to specific payment scenarios, such as split and delayed shipments and subscriptions
6	Bibliography	A list of key additional reference documents
	Glossary	A glossary of terms used in the Guide
	Appendices	Additional technical detail supporting the main text

Each section, and subsection, has been highlighted to show its relevancy to each client stakeholder group. The icons used throughout this document are as follows:

Important Note:

This document provides guidance on the practical application of SCA in a PSD2 environment in the EEA and the UK. Clients should note that this guide should not be taken as legal advice and the following take precedence over content in this guide:

- **Interpretations of the regulation and guidance provided by National Competent Authorities (NCAs)**
- **Visa core rules**
- **Technical information and guidance published in EMVCo specifications, Visa specifications and Visa Implementation guides listed in the bibliography**

Visa recognizes that clients have choices and may wish to use alternative approaches, tools and services to those referred to in this guide.

Audience

This guide is intended for anyone involved in the initiation, application and processing of e-commerce transactions in the EEA and the UK. This may include:

- Merchants and their Acquirers and third party agents and vendors looking for guidance on implementing SCA solutions
- Issuers seeking to ensure that they accurately recognize transactions that are in and out of scope of SCA so they can maintain security without their cardholders' experience being unnecessarily disrupted

Who to contact

For further information on any of the topics covered in this guide, Clients in the Visa Europe region may contact their Visa Representative or email customersupport@visa.com.

Merchants and gateways should contact their Visa Acquirer. Processors and PSPs should follow their agreed support channels and direct queries to Visa via respective Visa clients (Acquirers, Issuers).

To report EMV 3DS & SCA related issues to customersupport@visa.com or through the dedicated country numbers please provide the below, if available:

- **PSD2 SCA e-comm** in your subject line
- Provide a brief summary of the issue and impacted entities (e.g. BINs, merchants, certain transaction types),
- Specify if the issue is related to authorization, clearing processing or authentication of transactions (Visa Secure/EMV 3DS)
- For transactional analysis, provide:
    - Date and time of transaction (including time zone of time stamp),
    - Retrieval Reference number or Transaction ID, 'DSTransID' field (This information can be found in 3DS message logs)
    - Masked PAN if available,
    - Source IP address (for e-comm), impacted fields and values

Key Changes between v3.0 and v4.0

The following table summarises the major changes between this version 4.0 and version 3.0 of this guide. Please note this is not a complete listing of all changes made to the guide and it does not list the large number of minor text changes that have been made. Readers should ensure they read the text carefully to ensure correct interpretation of the guidance. Section numbers/titles refer to the section numbers/titles in this version 4.0 of the guide

Section number	Section title	Change to v4.0
	Key SCA challenges	New section added to highlight key challenges identified since enforcement of the SCA regulation and signpost the guidance addressing those challenges.
2	The requirements of PSD2 Strong Customer Authentication and Visa's interpretation	Text added to explain that the SCA requirement continues to apply in the UK following its departure from the EU and how any variations between the regulatory requirement in the EEA and UK at the time of writing of the Guide are identified in the Guide. It should also be noted that the term "PSD2 SCA" has been replaced throughout the Guide with the term "SCA" to encompass both the EEA and UK requirement – unless the text is referring specifically to a PSD2 only requirement.
2.1.2	SMS OTP plus behavioural biometric	Section changed to reflect the difference in the FCA definition as to what may constitute a behavioural biometric in the UK vs the EBA definition that applies to the EEA.
2.4	Dynamic Linking	• Updating of the text describing requirement for the authentication code and the way that EMV 3DS and VTS along with CAVVv7 and TAVV enable dynamic linking. • Addition of text to describe the difference between the FCA requirement for the UK and the EBA requirement for the EEA for reauthentication of a transaction when the final amount increases above the authenticated amount.
3	Visa's PSD2 solutions	Removal of references to Visa Trusted Listing (VTL) which is no longer offered.

Section number	Section title	Change to v4.0
3.2.2	Authorization message flows and fields	• Updating of the table: "Summary of authorization fields and messages used to communicate SCA and authorization status" to reflect technical changes in Visa systems.
3.2.3	Exemption/VDAP Requests & supplemental data in Field 34 & SCA decline code (Response Code 1A) in Field 39	Addition/updating of information on the impact for merchants, Acquirers and Issuers covering: • Transactions authenticated under VDAP • Use of the SCA decline code • Acquirer transmission of supplemental data
3.2.7.5	Use of the CAVV in account verification	Addition of information on use of the CAVV with Non-Payment Authentication (NPA) requests.
3.3	3-D Secure (EMV 3DS)	• Removal of information on 3DS 1.0 which was sunsetted as of 15 October 2022 • Addition of information on how EMV 3DS may be used to indicate Acquirer exemptions, Issuer exemptions that can be indicated by the merchant (trusted beneficiaries and SCP) and application of authentication under VDAP
N/A	Visa Trusted Listing	Section removed as this service is no longer offered.
3.6	Visa Delegated Authentication	Section updated to reflect the current structure of the program.
3.8.1.1	The requirement to use the MIT Framework in the context of SCA	Addition of information that Visa has mandated use of the MIT Framework by merchants acquired in the EEA and the UK for PAN based MITs from 14 April 2023.
3.8.2.3	Visa provided interim Tran IDs	Addition of further guidance on the use of Visa provided interim Tran IDs by merchants who have been unable to store Tran IDs of previous transactions for submission of MITs and confirmation that Visa will stop accepting interim Tran IDs for readiness purposes after 31 October 2023.
4.2.2.3	Managing variations in amount	Addition of more detailed guidance on options available to merchants to manage transactions where the final amount is not known at the time of authentication while maintaining compliance with the dynamic linking requirement. This includes:

Section number	Section title	Change to v4.0
		• More detailed explanation of the difference between the need to reauthenticate required by the FCA in the UK and the EBA for the EEA • How this applies to cross border transactions between the UK and the EEA • The combined impact of regulatory requirements and Visa rules on increases in amount between the authenticated and final amount in the UK and EEA respectively • Updated information on merchant options for handling amount variations within these constraints • How Issuer should respond to amount variations
4.2.3.1	Indicators for transactions with stored credentials	Addition of information to clarify indicators that merchants should set to correctly identify transactions using stored credentials (credential on file).
4.2.4	Reauthorizations	New section added explaining the use of MIT Reauthorization for payment scenarios where one or more authorizations take place when the cardholder is no longer present to complete a previously authenticated/exempted transaction.
4.2.5	Visa principles for implementing SCA	Updates to the Tables summarizing common CIT and MIT payment use cases and non payment use cases.
4.2.5.3	Visa authentication, authorization and clearing principles for implementing SCA	Table 21 "Fundamental Visa authentication, authorization and clearing principles for implementing SCA" updated to include: • Merchants unable to use 3RI to request a CAVV can reuse the initial CAVV up to 5 times until 18 October 2024 (Principle 1) • Applicability of the contactless exemption for a CIT undertaken at Point of Sale to set up a non-remote MIT (Principle 6) • Clarification of the steps and governing principles for use of MIT Reauthorization for delayed and split shipment authorizations (Principle 12) • Updated information on variation in amount to reflect the changes listed above (Principle 13) • That exemptions indicated via EMV 3DS must also be indicated in the subsequent authorization request (Principle 17)

Section number	Section title	Change to v4.0
4.3.3.5	Optimise use of exemptions	Addition of evidence on the benefits of indicating the Acquirer TRA exemption through EMV 3DS rather than direct to authorization.
4.4	Liability for fraud-related chargeback	Clarification of information on use of EMV 3DS and Field 34 indicators in tables 23, 24 and 25
4.5.3	Application of the trusted beneficiaries exemption	Clarification of the guidance on application of the trusted beneficiaries exemption, including addition of information on benefits of using the exemption, the processes for the managing cardholders' trusted lists, EMV 3DS message fields and values and authorization fields, indicators and values.
4.5.5	Interpreting the Secure Corporate Payment Processes and Protocols exemption	Clarification of guidance on the application of the SCP exemption to fully align the guidance with that contained in the *PSD2 SCA Secure Corporate Payment Exemption Guide*.
4.7	Use of EMV 3DS in storing credentials, setting up MITs & other key use cases: merchant & Issuer guidance	Addition of a new section providing additional guidance to merchants and Issuers on the use of EMV 3DS in specific transaction use cases to ensure that SCA is correctly applied and transactions are not unnecessarily declined.
4.8.1	Honoring step-up authentication requests	Clarification of guidance for Issuers on honoring SCA requests made using a 3DS Requestor Challenge Indicator = "04" (Challenge requested (Mandate))
4.8.3.2	Issuer processing guidelines – Account verification transactions	Clarification of requirements summarized in Table 33: Account verification use cases, associated SCA requirements and expected Issuer processing policies
4.8.3.4	Issuer processing guidelines – Reauthorizations	Clarification of the guidance for Issuers processing MIT Reauthorizations for delayed and split shipment authorizations,
4.8.3.8	Using TAVVs to prove cardholder authentication	Update to guidance to include the provision by Visa of an ECI value alongside the TAVV and the use of an "enhanced TAVV" to indicate that a cardholder has been authenticated without the need for a CAVV.
4.8.3.10	Handling transactions from merchants who are not yet fully ready for PSD2	Guidance updated to clarify that interim Visa assigned Tran IDs for readiness purpose may be utilised until 31 October 2023.

Section number	Section title	Change to v4.0
5	Payment use cases and sector specific guidance for merchants and PSPs	Section reintroduced and updated from version 2 of the guide where necessary to take account of: • Updated guidance based on final EEA and UK position with regards to variations to final amount • Use of enhanced TAVV
5.1.3	Reauthorization MIT (i.e. delayed authorization with MRC 3903)	Clarification of the detailed guidance for merchant use of MIT Reauthorizations for delayed and split shipment authorizations,
5.5	Open orders - Unknown final amount	Clarification of the definition of the scenarios when the final amount may change and of options available to merchants to manage changes to final amounts in the EEA and UK respectively.
5.7	Real-time service via mobile app with payment after service /completion	Guidance revised to clarify options available to merchants to minimise friction when collecting payment for services via a mobile app.
5.12.2	MIT Agreements established by mail order or telephone order (MOTO)	Guidance updated to include best practices and requirements guidance to Table 40 comparing MOTO and MIT transactions.
5.16	B2B Payments	Section revised to align with and references to Clarification of guidance on the application of the SCP exemption to fully align the guidance with that contained in the *PSD2 SCA Secure Corporate Payment Exemption Guide* and *PSD2 SCA Commercial Cards Guide*.
5.19.1	Adding a card to a merchant account/customer profile	Guidance clarified to align with new guidance in section 4.7 on correctly indicating transactions to add stored credentials via EMV 3DS.
5.19.2	Adding a card to an account during a purchase	Guidance clarified to align with new guidance in section 4.7 on correctly indicating transactions to add stored credentials via EMV 3DS.
A.5	Appendix 5 Trusted beneficiaries exemption – use of EMV 3DS and authorization indicators in key process flows	New appendix added containing detailed guidance on how the EMV 3DS and authorization messages and fields described in section 4.4.3.8 are used in the process flows for adding merchants to a Trusted List and applying the exemption and authorizing subsequent qualifying transactions.

Key SCA challenges

This section highlights some key SCA challenges that have adversely impacted transaction decline rates since enforcement of the SCA regulation. Merchants, Issuers, Acquirers and their technology partners should ensure they are familiar with guidance on these issues to ensure that SCA is applied with minimal consumer impact and that transactions are not unnecessarily declined.

Guidance	Relevant to	Guide section reference
Indicate out of scope or exempt transactions with the correct indicators Merchants and their Acquirers must ensure that the authorization request for any transaction that is sent direct to authorization without being submitted via EMV 3DS contains the correct out of scope or exemption indicator, otherwise the transaction may be declined.	Merchants Acquirers	2.3.1 3.2.3
Merchants collecting payments through MITs must use the Visa MIT Framework Merchants with payment models that require them to collect payment from customers' card accounts when the customer is not available to authenticate must ensure that they support the Visa MIT Framework, to minimize transaction declines regardless of whether transactions are PAN or token. This has been necessary since the enforcement of SCA regulation and will also now be mandated under Visa rules as of April 2023. Merchants should also note the following mandatory requirements for MITs: • MIT's must be correctly set up, with an appropriate customer agreement authenticated through an initial, customer initiated transaction (CIT) when set up in a remote channel • This initial CIT must be submitted via EMV 3DS with the challenge indicator set to 04 to ensure an SCA challenge is applied by the Issuer • The correct indicators must be used when subsequent MITs are submitted to authorization, otherwise transactions may be declined. Example payment types that this applies to include subscriptions, regular bill payments, and usage based merchant initiated collections.	Merchants Acquirers	4.2.3

Guidance	Relevant to	Guide section reference
Merchants/Acquirers must transition away from the use of the interim Transaction ID to indicate MITs before 31 October 2023 To assist merchants to correctly indicate transactions as MITs in time for the regulatory enforcement date, Visa had provided Acquirers with "Interim Transaction Identifiers" for use in place of a valid Original Tran ID in MITs. Visa has now announced that it will stop accepting usage of this interim Tran ID from 31 October 2023. Transitioning to the use of a valid initial or previous Tran ID in MITs before that end date is critical to minimize Acquirer non compliance fees and Issuer declines. Methods to transition are outlined in section 3.8.2.3.	Merchants Acquirers	3.8.2.3
Transactions that are manually key entered by merchants may be declined unless appropriate indicators are applied Transactions that are key entered into point of sale terminals by merchants are subject to declines as they do not contain any proof of authentication. To avoid declines where an Issuer is unable to apply an exemption. Acquirers and PSPs that provide terminals must ensure that: • Terminals are upgraded to support application of out of scope indicators where appropriate. For example the MOTO indicator must be present in a transaction that was initiated over the phone • Merchants are aware of the need to upgrade their point of sale terminals appropriately.	Merchants Acquirers	3.2.9.1
Merchants must indicate to Issuers that SCA is required for transactions processed to set up MITs When setting up MITs, SCA is required[2], therefore merchants must always set the 3DS Requestor Challenge Indicator to "Challenge Requested: Mandate (04). It is not sufficient to submit the transaction via EMV 3DS leaving the Issuer to choose to apply a challenge or not as the Issuer cannot know the purpose of the authentication request is to set up an MIT.		4.7.2.2
To minimize potential friction and SCA declines when storing credentials for use in future CITs, merchants are recommended to use EMV 3DS Adding a stored credential for future cardholder-initiated transactions (CITs) requires SCA only if there is a risk of	Merchants Issuers	4.7 3.8.3.2 Table 15 5.12.2 Table 40

[2] Some exceptions apply where SCA may not be needed for CITs done to set up future agreements. More information is available in Section 3.2

Guidance	Relevant to	Guide section reference
fraud, while a CIT used to establish an agreement for future MITs, always requires SCA. However, as Issuers are unable to differentiate between those two scenarios in the Visa authorization system, they may always request SCA on those transactions. Merchants wishing to minimize friction and limit SCA declines on "add card" scenarios are therefore recommended to submit add card use cases via EMV 3DS to indicate to Issuers the intent of the transaction.		
Stored credential transactions that are initiated by the customer are not out of scope of SCA Processing a transaction with a stored credential does not automatically qualify the transaction as an out of scope MIT or as a transaction exempt from SCA. Many CITs use stored credentials and are in scope of SCA. SCA is therefore required unless the transaction qualifies for an exemption. For example, so-called "one-click" transactions, or transactions initiated through apps used for booking ride sharing or cycle hire services, fuel purchases etc., that use stored credentials do not qualify as MITs:	Merchants Acquirers	4.2.3
Token Transactions are In Scope of SCA Visa Tokens can be used in the place of PANs throughout the payments eco-system. Therefore, any merchant or Acquirer using Visa Tokens for financial transactions should use the same criteria for their SCA decisions as they use for PANs.	Merchants Acquirers	4.2.5.3 3.2.7 3.3.9
Acquirers and merchants must be able to respond correctly to SCA decline codes (Response Code 1A) Issuers will respond to in scope transactions submitted to authorization without SCA having been applied with an SCA decline code (Response Code 1A) if they consider that SCA is required. Merchants must be able to respond to an SCA decline code (Response Code 1A) by resubmitting the transaction via EMV 3DS with the 3DS Requestor Challenge Indicator set to 04 (Challenge Requested: Mandate) to ensure that SCA is applied. Otherwise, the transaction may be declined by the Issuer.	Merchants Acquirers	3.2.3 4.7.2.3
Merchants must ensure that EMV 3DS authentication requests are fully populated with required data	Merchants	*Visa Secure Using EMV 3DS Best Practices for*

Guidance	Relevant to	Guide section reference
EMV 3DS supports the provision by merchants of transaction data that allows Issuers to make optimum risk decisions and minimize unnecessary application of SCA. Merchants should ensure they provide this data in order to minimise customer friction and abandonment.		*Merchants*" and "*Minimum Data Requirements for Merchants*" guides available on Visa Online
Merchants submitting MOTO transactions and setting up MITs via the MOTO channel must ensure that both types of transaction are correctly indicated. SCA is not required for either single purchase transactions or MIT set up transactions via the MOTO channel as MOTO is out of scope of SCA. However correct values must be set for POS Condition Code (F25) and, where required, POS Environment (F162.13). Correct indicators must also be used to identify any subsequent MIT transactions.	Merchants Acquirers	5.12.2

1. Introduction: Visa's guiding principles for PSD2 SCA

1.1 Introduction

As the digital economy plays an increasing part in all our lives, it is vital that electronic payments are secure, convenient and accessible for all. Visa aims to provide innovative and smart services to Issuers, Acquirers and merchants, so they are able to deliver best in class payments to all Visa cardholders.

The Payment Services Directive 2 (PSD2), which is now in force across the EEA and the UK, aims to contribute to a more integrated and efficient European payments market and ensure a level playing field for Payment Service Providers (PSPs). As such, it introduces enhanced security measures to be implemented by all PSPs.

1.2 Visa's guiding principles

Visa supports the PSD2 requirements for Strong Customer Authentication (SCA), and Visa programs and initiatives including 3-D Secure (EMV 3DS), and the Visa Token Service (VTS) may support PSPs to be PSD2 compliant. EMV 3DS, along with other Visa products, programs and positions that are outlined in this paper, are in line with Visa's vision for secure, compliant, advanced and convenient electronic payments, and aim to deliver a good balance between security and consumer convenience. This will benefit all participants of the commerce ecosystem; reduced levels of fraud reduce cost for all parties, while merchants in particular will benefit from a lower friction payment flow that will increase conversion rates. Consumers will benefit from a low friction purchasing experience, even when SCA is required.

Visa's guiding principles for PSD2 are:

- Innovate to give consumers choice and control to make informed decisions
- Build trust and security into every payment experience
- Expand access to data while keeping it protected
- Foster competition and innovation through open standards

Our Focus for SCA and ensuring that all players in the payment ecosystem are able to optimize both payment security and user experience are:

- Leadership: Provide clarity and education to the ecosystem
- Products: Build and evolve products and authorization messages
- Programs: Develop new programs and adjust rules as needed
- Compliance: Provide proof between parties to monitor performance

2. The requirements of PSD2 Strong Customer Authentication and Visa's interpretation

This section provides a brief summary of Visa's interpretation of the PSD2 Strong Customer Authentication (SCA) requirements.

PSD2 requires that SCA is applied to all electronic payments - including proximity and remote within the European Economic Area (EEA[3]) and the UK. Although the UK is no longer a member of the European Union, PSD2 has been transposed into UK law and the requirement to apply SCA applies to transactions taking place within the UK[4] and between the UK and the EEA as well as within the EEA.

The SCA mandate is complemented by some limited exemptions that aim to support a frictionless customer experience when a transaction risk is low. In addition, some transaction types are out of scope of SCA.

The requirement to apply SCA came into force on 14 September 2019. and has been fully enforced in the EEA since 31 December 2020 and in the UK since 14 March 2022.

Note on the definition of SCA requirements in the UK:

The requirement to apply SCA within the UK is defined in The Payment Services Regulations 2017 (SI 2017/752) and the FCA Handbook and Technical Standards.

Currently the requirements for the UK fully align with the PSD2 SCA Regulatory Technical Standards (RTS), EBA Guidance and Q&A answers, with very limited exceptions. Where there is a deviation between the requirement for the UK and the EEA at the time of writing of this guide, it is identified in the text. Otherwise it can be assumed that requirements and references to SCA, PSD2 SCA, the PSD2 SCA RTS, EBA opinions and Q&A answers stated in this guide apply to both the EEA and the UK.

2.1 The application of SCA and use of factors

SCA requires that the payer is authenticated by a PSP through at least two factors, each of which must be from a different category. These are summarized in Table 1.

[3] For more information on the territories the requirement applies to please see Appendix A.4.

[4] SCA requirements are currently expected to remain in force in the UK and will be defined in accordance with relevant technical instruments published by the FCA.

Table 1: Strong Customer Authentication Factors

Category	Description	Example
Knowledge	Something only the payer knows	A PIN code
Possession	Something only the payer has	A preregistered mobile phone, card reader or key generation device
Inherence	Something the payer is	A biometric (facial recognition, fingerprint, voice recognition, behavioral biometric[5])

Factors must be independent such that if one factor is compromised, the reliability of the other factor is not compromised.

While the PSD2 regulation allows for any combination of at least two factors, in Visa's view, the most practical SCA solutions will make use of:

- Possession as the first factor, and
- Inherence as the preferred second factor, or
- Knowledge as an alternative compliant, but much less satisfactory, factor

The EBA Opinion published 21st Jun 2019[6] makes clear that:

- Static card details and security codes printed on a card cannot be used as either a possession or a knowledge element and the opinion advises competent authorities to closely monitor their application
- Dynamic card security codes may be used to provide evidence of possession and card security codes that are not printed on the card but sent separately to a customer could constitute a knowledge element
- An OTP cannot be used as a knowledge element but may be used to prove evidence of possession
- Inherence includes both biological and behavioural biometrics, where behavioural biometrics includes examples such as keystroke dynamics (typing and swiping patterns) and the angle at which the consumer holds the device.

The EBA also confirmed via their Q&A tool on 12 July 2020[7] that tokenised card details can be used to provide evidence of possession where the process of tokenisation binds the cardholder and the token to a preregistered device. Visa proposes - and has been engaging with

[5] For the UK only, the FCA has confirmed that inherence can be defined as a characteristic attributable to a person, including behavioural analytics, such as spending patterns. See section 2.1.2 for more information

[6] Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 21 June 2019.

[7] https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4827

regulators on - an SCA Authentication Factor Strategy that provides staged compliance and consumer choice by providing two primary, recommended authentication methods:

2.1.1 Biometric plus device possession

Biometric authentication can be SCA compliant, and a single device can provide both the possession factor (i.e. indicating possession of the device where the biometric is stored) and an inherence factor (the verification of the biometric captured). This approach has the additional advantages that:

- Consumers are getting more comfortable using biometrics
- Both Visa and MasterCard have requirements for Issuers to support biometrics
- The industry is aligned on this, and progress is underway

This method, also known as Out of Band (OOB) app plus biometric authentication uses a registered smart phone capable of supporting a relevant biometric (for example fingerprint or facial recognition) in conjunction with a mobile banking or other authentication app. The technology provides for two distinct and independent authentication factors, possession and inherence, both of which are facilitated using a biometric.

2.1.2 SMS OTP plus behavioural biometric

Behavioural biometrics can be used as a second factor (proving inherence) alongside OTP (proving possession) to provide an SCA solution that is significantly easier for customers to use and far more secure than OTP combined with a knowledge factor. This provides a potentially compliant evolution solution for existing single factor SMS OTP solutions that delivers a familiar and secure customer experience and is relatively straightforward for Issuers to implement.

Behavioural biometrics uses physical behaviour indicators that are unique to an individual customer. These can include the angle at which a device is held, the way keystrokes are entered, gesture analysis and swiping speed. Indicators are analysed and used to build dynamic user profiles and authenticate users.

The use of behavioural biometrics is in line with the EBA opinion on elements for SCA which identifies inherence elements such as keystroke dynamics (identifying a user by the way they type and swipe) and the angle at which the user holds the device. In the UK, the FCA and the industry (as represented by UK Finance) also consider behavioural biometrics to be a compliant and viable solution.

Note that there is a divergence between the EBA and FCA in what may constitute a behavioural biometric in the EEA and the UK respectively. In it's June 2019 opinion, the EBA stated that behavioural biometrics could constitute inherence and that inherence 'relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these'. It excluded other individual properties such as spending patterns. In the UK, the FCA has concluded[8] that behavioural analytics (for example detailed shopping patterns) could potentially be used to verify the behavioural characteristics of an individual for the purpose of SCA. It has clarified that for the UK inherence does not need to be linked to a physical attribute to constitute a valid inherence factor under SCA. It is the extent to which an inherence-based approach prevents the unauthorised use of the SCA

[8] FCA Policy Statement PS21/19 November 2021

elements that is important in determining whether those elements constitute a valid inherence element or not.

A challenge solution that uses behavioural biometrics will help Issuers to be compliant with the regulation, while fraud protection can be maximised by combining the behavioural biometric indicators with EMV 3DS data, which include device, location and purchase history data, and provides a proven, accurate basis for assessing fraud risk.

2.1.3 Tactical and Inclusivity solutions

While biometrics based SCA solutions are recommended as the primary SCA solutions for the majority of customers, alternatives may be considered in the following circumstances:

- It is not possible for an Issuer to deploy one of the recommended solutions to all of its customers by the enforcement date and a Tactical Solution needs to be employed
- A minority of customers are unable or unwilling to access mobile phone based solutions and an Inclusivity Solution needs to be deployed

Tactical Solutions will normally use a knowledge element to provide a second compliant factor alongside a possession factor provided either through an SMS OTP or a securely device bound banking authentication app.

Issuers need to focus on serving the majority of customers with the recommended SCA solutions, however Inclusivity Solutions should also be made available for limited deployment to those customers unable to access or use mobile phones for authentication. A number of two-factor options are available including card readers and hardware tokens that generate an OTP to prove possession of the device in response to entry of a knowledge factor such as a PIN.

2.2 Exemptions

The main exemptions to the application of SCA relevant to Visa e-commerce transactions are summarized below. It should be noted that not all exemptions are available to all PSPs. For more detail please refer to Section 4.5.

2.2.1 Transaction risk analysis (TRA)

The TRA exemption allows for certain remote transactions to be exempted from SCA provided a robust risk analysis is performed (based on the requirements in Article 18 of the SCA RTS), and the PSPs meet specific fraud thresholds. TRA is key to delivering frictionless payment experiences for low-risk remote transactions. Issuers and Acquirers can both apply the TRA exemption so long as they meet certain requirements, including that their fraud to sales rates are maintained within the specific fraud thresholds for remote card payments, set out in Table 2.

The SCA RTS[9] also lays down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs.

[9] See Recital 14 and article 2 of the Regulatory Technical Standards.

Table 2: Specific fraud thresholds for remote card payments

Transaction value band EEA	Transaction value band UK	PSP Fraud Rate
≤€100	≤£85	13 bps / 0.13%
€100 ≤ €250	£85 ≤ £220	6 bps / 0.06%
€250 ≤ €500	£220 ≤ £440	1 bps / 0.01%

2.2.2 Low value transactions

Remote transactions up to and including €30 (£25 in the UK) do not require SCA so long as the cumulative number of previous remote transactions using the exemption does not exceed five, or the cumulative value of previous remote transactions using the exemption does not exceed €100, (£85 in the UK) since the last application of SCA. Issuers should select either the cumulative or consecutive limit. If Issuers do not select a limit, they must apply both limits on a per transaction basis.

2.2.3 Trusted beneficiaries

Under the trusted beneficiaries exemption, once a customer performs SCA in order to add a qualifying merchant to their Trusted List, subsequent purchases with that merchant generally will not require SCA.

2.2.4 Secure corporate payments

Under SCA-RTS Article 17, PSPs are allowed not to apply SCA for payments made by payers who are both legal persons and not consumers. This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers. Subject to the view of NCAs, these payments may:

- Originate in a secure corporate environment, including for example, corporate purchasing or travel management systems
- Be initiated by a corporate customer using a payment method or process such as a virtual card or lodged account, so long as this payment method is not available to consumers and the NCA is satisfied that security levels are at least equivalent to those provided for by PSD2

In many cases it will not be possible to authenticate transactions originating in a secure corporate environment and requesting SCA may result in valid transactions being declined.

In order to apply the exemption, Issuers must ensure that, and NCAs must be satisfied that, the processes or protocols used guarantee at least equivalent levels of security to those provided for by PSD2. NCAs may have their own procedures or processes for assessing the use of this exemption.

Issuers are encouraged to (and, for some NCAs, may be required to) demonstrate to NCAs that applicable processes and protocols meet the requirements of the regulation and Visa recommends that Issuers liaise with NCAs over the procedure for this as required.

2.2.5 Recurring Transactions

Please note Visa does not support the recurring transactions exemption for Visa card transactions. Visa's view is card transactions that would otherwise be covered by the recurring transaction exemption are typically Merchant Initiated Transactions (MITs) and are therefore out of scope of SCA.

2.3 Out of scope transactions

2.3.1 Transactions considered out of scope

The following transaction types are out of scope of SCA and do not require the application of SCA, so long as certain conditions are met:

- **Merchant Initiated Transactions (MITs) -** Are transactions of a fixed or variable amount and fixed or variable interval, governed by an agreement between the cardholder and merchant that, once set up, allows the merchant to initiate subsequent payments from the card without any direct involvement of the cardholder. As the cardholder is not present when an MIT is performed, cardholder authentication is not possible. A transaction can only be an MIT if the cardholder is not available to (I) initiate; or (II) authenticate the transaction. If the cardholder is available to either initiate or authenticate at the time of initiation of the transaction, the transaction is not an MIT and should therefore be subject to SCA unless an exemption applies. This should be the case independently of whether the transaction is processed at that exact moment or later in the time. A consumer is available to initiate or authenticate if they are physically present at the merchant's point of sale or, in the case of a remote payment, interacting with the merchant's web page or app. From a Visa processing perspective, an MIT can only be submitted after a previous cardholder initiated transaction (CIT) has been performed with appropriate authentication to establish the initial agreement with the cardholder specific to the MIT (even if that CIT is a zero-value transaction). Subsequent qualifying MITs are out of scope of SCA and therefore do not require authentication.
- **Mail Order/Telephone Order (MOTO)** - Payments made through Mail Order/Telephone Order are out of scope and do not require the application of SCA. Note, "voice commerce" payments initiated through digital assistants or smart speakers are not classed as MOTO. In Visa's view, transactions initiated via telephone through Interactive Voice Response (IVR) can be considered as telephone initiated and therefore MOTO. If the IVR is internet based, the transaction cannot be classed as MOTO.
- **One-leg-out-** It may not be possible to apply SCA to a transaction where either the Issuer or Acquirer is located outside the EEA[10] or the UK. However, SCA should still be applied to OLO transactions on a "best-effort" basis. Further text on one-leg-out transactions and best efforts is provided below. If the Issuer is not technically able to apply SCA, the Issuer is not obliged to decline. The Issuer should make their own approval decision based on risk and liability considerations. A transaction at a merchant that is located outside the EEA or UK but that is acquired from within the EEA or UK is not classed as one-leg-out and is in scope of SCA.
- **Anonymous transactions -** Transactions through anonymous payment instruments are not subject to the SCA mandate, for example anonymous prepaid cards. In the Visa system,

[10] Refer to Appendix A.4 for a list of EEA countries.

these can include non-reloadable prepaid cards on which no KYC has been done and thus where the Issuer cannot authenticate the identity of the cardholder.[11]

2.3.2 Identifying one-leg-out transactions and understanding use of best efforts to apply SCA

The EBA has set out that SCA applies on a best-effort basis for one-leg-out transactions. We set out two scenarios below.

2.3.2.1 Issuer within the EEA/UK, Acquirer outside the EEA/UK

Where a transaction uses a card issued in the EEA or the UK, but is acquired outside of the EEA or the UK:

- If an Issuer receives a transaction request that does not enable them to apply SCA, the Issuer is not obliged to decline the transaction.
- The Issuer should make its own approval decision based on risk, customer experience and liability considerations.

2.3.2.2 Acquirer within the EEA/UK, Issuer outside the EEA/UK

Where a transaction uses a card issued outside of the EEA or the UK, but is acquired within the EEA or the UK:

- Visa recommends that Acquirers/merchants send transactions for authentication in an SCA compliant way, for example by submitting the transaction via EMV 3DS, where this is supported by the non-EEA/UK Issuer.
- If a non-EEA/UK Issuer receives such a transaction request, it is not under any obligation to apply SCA.

2.4 Dynamic linking

For electronic remote payment transactions, where PSPs apply SCA, both the amount and the payee must be clear to the payer when they authenticate a purchase. This typically means the cardholder is presented with the payee name and purchase amount. Therefore a means to link and identify the authenticated purchase must be produced for the non-repudiation of the transaction. This can be achieved through an authentication code produced by the PSP, but this authentication code does not need to be visible to the cardholder.

The regulation requires that the authentication code accepted by the PSP corresponds to the original amount and payee agreed to by the payer at authentication. Visa's programs such as EMV 3DS, and Visa Token Service (VTS), support the delivery of an authentication code – in the form of the Cardholder Authentication Verification Value (CAVVv7) and/or Token Authentication Verification Value (TAVV) - which corresponds to the amount of the transaction and the payee at time of authentication and must be present in the authorization. Other solutions or methods for dynamic linking are possible but are beyond the scope of this guide.

In the case of transactions initiated in the EEA, when the final amount is unknown at the time of authentication, the EBA has confirmed that the final amount should not increase above the

[11] The fact that no KYC has been done and/or that it is a non-reloadable prepaid card will not necessarily mean the card is anonymous in all cases.

authenticated amount.[12] Re-authentication is required for any increases above the authenticated amount.

In the UK, the FCA has confirmed that that re-authentication is not required if the final amount is higher than the original authenticated amount so long as:

1. The final amount is within the customer's reasonable expectations
2. That the increase between the authenticated final amount is no more than 20%
3. The customer was made aware that the amount could increase

The FCA has also confirmed that the final amount is defined as the total amount that the customer pays, which includes any shipping costs and taxes.

The same does not apply where the final, authorized amount is lower than the authenticated amount. In these cases, no re-authentication is required.

If, in the case of a payment made in the EEA, the final amount is higher than the authenticated amount, or in the UK the increase does not meet the above conditions set by the FCA several options exist to handle amount variation. One of them is that the merchant may wish to set up an MIT to allow incremental amounts to be taken if the authorized amount is insufficient, rather than seek further authentication from the cardholder.

With regard to variations in merchant name, the EBA has confirmed[13] that the information included in the authentication code does not necessarily need to be the full or exact merchant name, and that while the RTS 'Regulation does not specify how the payee should be identified for the purpose of the dynamic linking requirements, it can be a unique identifier corresponding to the identity of the payee agreed to by the payer. The identifier agreed to by the payee at authentication may differ to the merchant name at authorization. For example:

- When there is a difference in the name used to identify a merchant between authentication and authorization such as use of a trading name vs. a legal entity name, use of different abbreviations or acronyms or a combination of the Acquirer and merchant name vs. the merchant name.
- When a transaction is the result of a booking via an agent who initiates authentication on behalf of a third party merchant that subsequently requests authorization, the name in the authentication request may be that of the agent only, or that of the agent and the merchant, whereas the name in the authorization request may be that of the merchant.

Note that Merchant IDs, and Acquirer IDs are irrelevant to the dynamic linking requirement and may therefore also change between authentication and authorization, for example where a merchant submits a transaction via different Acquirers for authentication and authorization.

For additional guidance on managing variations in merchant name, merchant ID, Acquirer ID and amounts within the constraints of these requirements please see section 4.2.2

[12] Response to EBA Q&A 2020_5133.
[13] Response to EBA Q&A 2019_4556.

2.5 Visa PSD2 Solutions and GDPR

Visa's PSD2 solutions process data elements that are considered to be personal data under the GDPR. Merchants, Issuers and Acquirers should seek legal advice when considering the GDPR consequences of providing and processing data that may be considered to be personal information.

Specific principles to consider include:

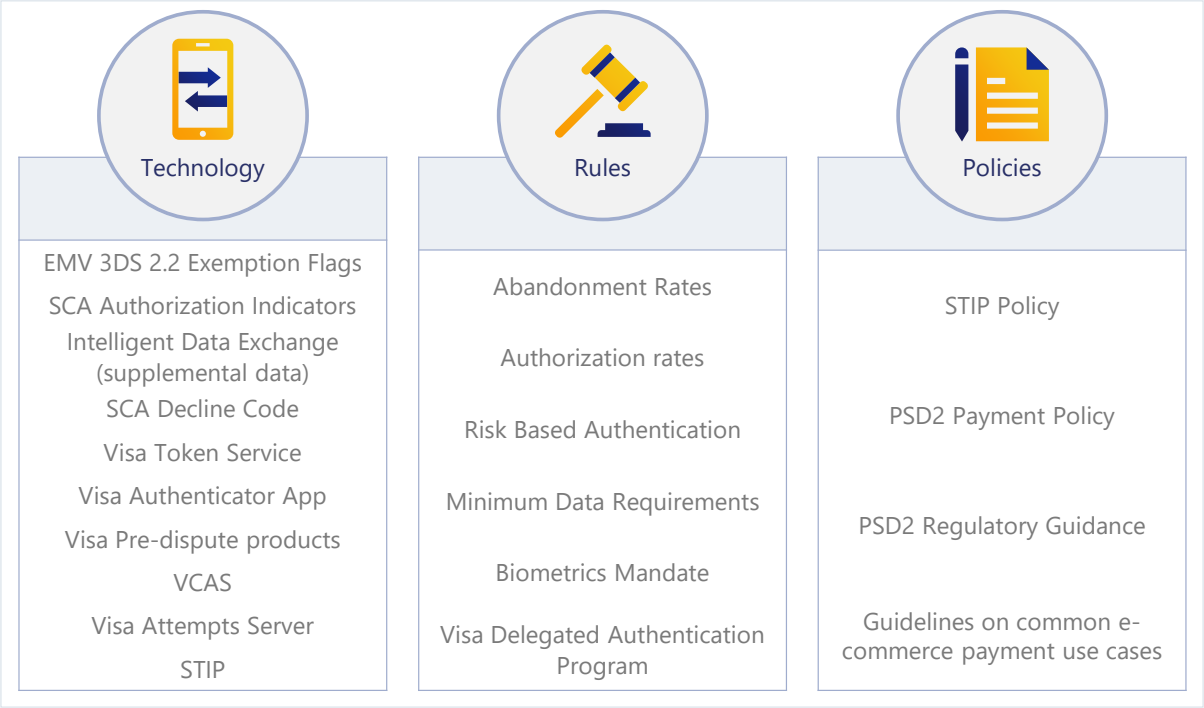
- Lawful basis for processing: Merchants, Issuers and Acquirers should ensure they can rely on a lawful basis under the GDPR to process personal data in the context of Visa's PSD2 solutions. For most of these solutions, Merchants, Issuers and Acquirers may rely on legal bases other than consent including legal obligation, contract and legitimate interest for using personal data for fraud prevention purposes.
- Purpose limitation: Data provided by merchants for EMV 3DS authentication must not be used for any purpose other than authentication and fraud prevention. Specifically, this data should not be used for sales, marketing or other purposes.
- Data storage and security: Merchants, Issuers and Acquirers should ensure that the requirements for data storage, security and international transfers under GDPR are applied to any personal data that is collected for Visa's PSD2 solutions.
- Transparency and Individual Rights: Issuers, Acquirers and Merchants should ensure that Terms and Conditions, Privacy Policies and Privacy Notices reflect the capturing and processing of data for fraud prevention purposes in the context of Visa's PSD2 solutions. This includes information on purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. In addition, Issuers, Acquirers and Merchants should ensure that they can respond to individuals' requests under the GDPR.

3. Visa's PSD2 solutions

3.1 Solution summary

Visa has implemented a portfolio of solutions to help support the application of SCA and exemptions. These comprise a combination of technology solutions, enhanced rules and policies which are summarized in Figure 1 below.

Figure 1: Summary of Visa's PSD2 solutions



The technology-based solutions include a suite of products and programs that will support the application of SCA and exemptions. These are all based on a core set of foundational security technologies, illustrated in Figure 2 below.

Figure 2: The foundational and SCA products & programs

The application of SCA and the approval of transactions depends on two processes:

- Authentication: Allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials. Where authentication is required, it takes place before authorization, using the Issuer's selected authentication method, which in most cases is facilitated through EMV 3DS
- Authorization: Is a separate process used by a card Issuer to approve or decline a Visa payment transaction submitted by a merchant/Acquirer or other card acceptor

In a standard flow, merchants will submit a transaction for authentication, in some cases with an indicator requesting an exemption from SCA requirements. If the authentication is successful, the result will be returned along with a cryptogram (CAVV), and the merchant will submit the transaction to authorization along with the cryptogram and the correct indicators.

EMV 3DS 2.2 may also be used by merchants to indicate that they would like certain exemptions, and data indicates that in the case of the Acquirer TRA exemption, submission of these transactions via EMV 3DS reduces challenge rates, increases authorization approval rates and reduces fraud rates (see section 4.3.3.5 for more information).

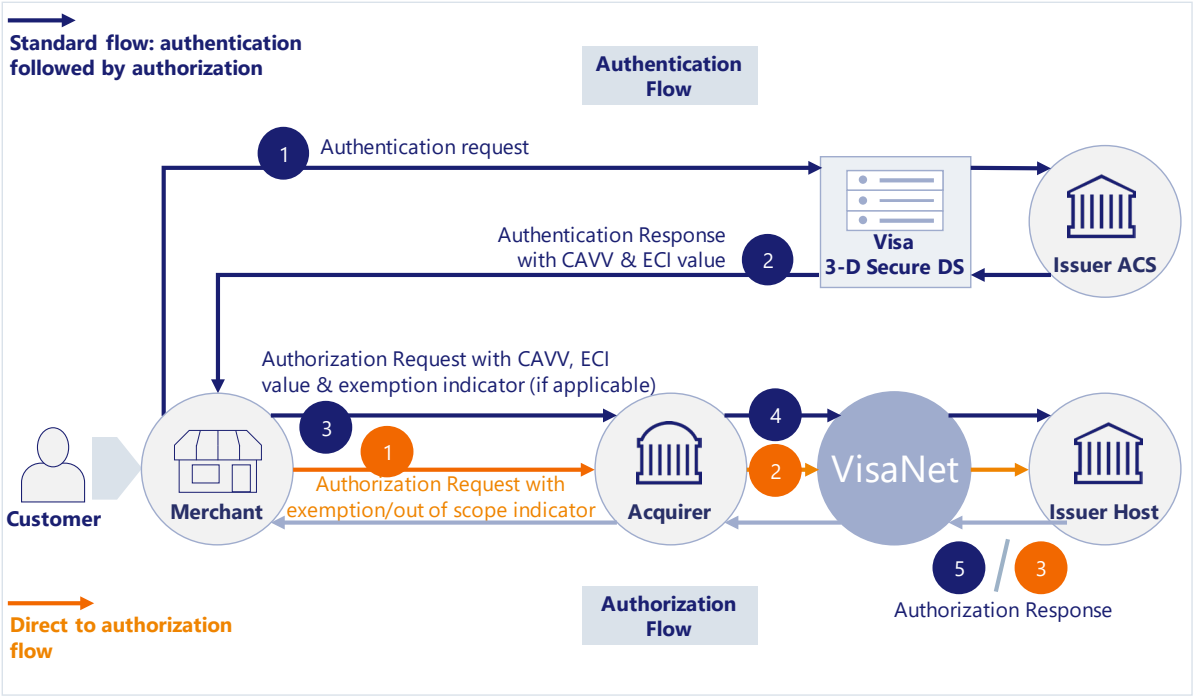
Visa also supports the option for transactions to be submitted direct to authorization, with an appropriate indicator. This may occur when:

- A transaction is out of scope of SCA
- An Acquirer applies an exemption such as low value

Factors to consider when selecting the appropriate option are summarized in section 4.3.

These basic flows are summarized in Figure 3 below:

Figure 3: Simplified summary of authentication and authorization flows



The following sections describe the authorization and authentication technologies and indicators offered by Visa.

3.2 Authorization options

3.2.1 Overview

Indicators in the authorization request message will be used by Issuers to identify:

- Transactions that are identified by merchants as being out of scope
- Acquirer exemptions (TRA and low value)
- Issuer applied exemptions that can be indicated by the merchant or Acquirer (trusted beneficiaries[14] and SCP)
- That authentication has been applied under the Visa Delegated Authentication Program
- That authentication was not possible due to an outage in the acceptance domain
- There was no connectivity at the time of authorization

If a merchant would like to indicate that an Acquirer exemption is to be applied, or that an Issuer exemption should be considered (for SCP and trusted beneficiaries), an exemption indicator should be submitted in the authorization request. If the transaction is out of scope, the merchant must also ensure that the correct data is used to identify that it is out of scope.

[14] Note – merchants indicating to an Issuer that the trusted beneficiaries exemption is to be applied must first submit the transaction via EMV 3DS with the trusted beneficiaries indicator set. Such transactions cannot be submitted direct to authorization

Key Point

Indicators in the authorization request message can be used by merchants to indicate certain out of scope transactions and exemptions. Merchants must ensure that the correct mechanism and indicators are used to identify exemptions being requested and transactions that are out of scope of SCA.

This section describes the Visa authorization message flows and fields and how these are used to support the application of exemptions and management of out of scope transactions.

3.2.2 Authorization message flows and fields

The main messages in the authorization flow are the Authorization Request and the Authorization Response messages. These enable merchants and Acquirers to request transaction authorization and Issuers to respond with the authorization result.

Table 3 summarizes the key relevant message fields in the authorization message flow.

It should be noted that some transaction status indicators must be indicated by Issuers and some by Acquirers. It is mandated that merchants use MIT indicators for MIT transactions and essential that they use the correct MOTO information for MOTO transactions.

Table 3: Summary of authorization fields and messages used to communicate SCA and authorization status

Field	Set by	Function	Field Value/Indicator
F19	Acquirer	Populated with the Acquiring Institution Country Code allowing the Issuer to determine whether the transaction is in or out of scope of SCA	Acquiring Institution Country Code
F25	Acquirer	Point-of-Service Condition Code – required for CAVV processing which in addition can be used to indicate MOTO transactions	Existing values as defined in the Visa technical specification[15]
F34	Acquirer	Allows Acquirer to indicate that authorization is being requested without the application of SCA because one of the following exemptions applies: Trusted Beneficiary Low Value Secure Corporate Payments Transaction Risk Analysis or that the transaction has been authenticated under the terms of the Visa Delegated Authentication Program allows Visa to indicate to Issuers that a transaction is an MIT out of scope of SCA Allows Acquirers to indicate that there is an outage in the acceptance environment, and it is not possible to authenticate.	The following tags are used to carry the SCA exemption indicators in the new TLV Field 34 Dataset ID Hex 4A: Tag 84 - Trusted Merchant (Beneficiary) Exemption Indicator. Possible values: **0** (Trusted merchant exemption not claimed/requested) **1** (Trusted merchant exemption claimed/requested) **2** (Trusted merchant exemption validated/honored) **3** (Trusted merchant exemption failed validation/not honored) NOTE: *If the trusted merchant exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.* Tag 87 - Low Value Exemption Indicator Possible Values **0** (Low value exemption not claimed/requested)

[15] For more details, refer to the *V.I.P. Base 1 Technical Specifications, Volume 1 & Volume 2.*

Field	Set by	Function	Field Value/Indicator
			1 (Low value exemption not claimed/requested) **2** (Low value exemption validated/honored) **3** (Transaction risk analysis exemption failed validation/not honored) NOTE: *If the low value exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.* Tag 88 - Secure Corporate Payment (SCP) Indicator Possible Values: **0** (Secure Corporate Payment exemption not claimed/requested) **1** (Secure Corporate Payment exemption claimed/requested) **2** (Secure Corporate Payment exemption validated/honored) **3** (Secure Corporate Payment exemption failed validation/not honored) NOTE: *If the SCP exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.* Tag 89 - Transaction Risk Analysis (TRA) Exemption Indicator Possible Values: **0** (Transaction risk analysis exemption not claimed/requested.) **1** (Transaction risk analysis exemption claimed/requested.) **2** (Transaction risk analysis exemption validated/honored) **3** (Transaction risk analysis exemption failed validation/not honored) NOTE: If the TRA exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely Tag 8A - Tag indicates that the transaction is using Visa Delegated Authentication during authorization; also referred to as the Delegated Authentication indicator Possible Values: **0** (Delegated authentication not claimed/requested) **1** (Delegated authentication claimed/requested) **2** (Delegated authentication validated/honored) **3** (Delegated authentication failed validation/not honored) NOTE: *If the delegated authentication does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely*

Field	Set by	Function	Field Value/Indicator
			Tag 8C - Tag indicates reasons for the Issuer not Honouring the Trusted Merchant (Beneficiary) Exemption (Tag 84) and TRA Exemption (Tag 89) Possible Values: **8473** (Cardholder has not trusted the merchant (Issuer supplied) **8474** (Did not meet the exemption criteria (Issuer determined/supplied) **8976** (Did not meet the exemption criteria (Issuer determined/supplied) **8A76** (Did not meet the exemption criteria (Issuer determined/supplied) NOTE: *Tag only optionally present if the Issuer responded with a value of 3 in Tag 84 or Tag 89, if no Issuer response in this tag, it is omitted entirely* Apart from the exemption tags present in Dataset ID Hex 4A, two additional tags are present in Dataset ID Hex 02: Initiating Party Indicator – Tag 80 This is used to indicate to the Issuer that this transaction was indicated as an MIT. This field cannot be populated by an Acquirer. Visa net will populate this value if the Acquirer has indicated the transaction is an MIT using the MIT Framework. Possible Values: **1** (Populated by Visa if Acquirer indicated this transaction as Merchant Initiated) Acceptance Outage Indicator – Tag 87 The indicator means that authentication was attempted for a transaction but there was an authentication outage in the authentication flow between the merchant, gateway (3DS) server, and directory server, which means an authentication request was not possible and an authentication response could not be received. (This indicator cannot be used to indicate an outage in the Issuer processing domain, including agents acting on behalf of the Issuer). Possible Values: **0** (No authentication outage) **1** (Authentication outage) If there is no Authentication outage, the value of 0 is optional and the tag may be omitted entirely. In Dataset ID 01, there is Tag 86 called 'Authentication data'. This will include the EMV 3DS Protocol version number and is populated by Visa. Values: **1.x.x** (3DS 1.x.x) **2.x.x** (EMV 3DS 2.x.x) **2.2.x** (EMV 3DS 2.2.x) **UNKNOWN** (Unknown 3DS protocol version number)

Field	Set by	Function	Field Value/Indicator
F39	Issuer	Response to F34 exemption request indicating additional customer authentication required	Response code 1A – SCA Decline Code
F44.13	Acquirer	CAVV /TAVV Results Code	One-character code indicating classification of the CAVV / TAVV and the pass/fail result. For token transactions, if no CAVV, the TAVV result code can be populated here. If both are present, then the CAVV Result Code is in this field and the TAVV Result Code is in field 123
F60.8	Acquirer	Mail/Phone/Electronic Commerce and Payment Indicator indicating the ECI Value	Existing values as defined in the Visa technical specification[15]
F60.10	Acquirer	Indicates a transaction performed with an estimated amount	2 or 3
F62.2	Acquirer – when submitting an MIT (Otherwise set by Visa on every single transaction)	May be used by Acquirers to indicate a transaction is an MIT: Acquirers may indicate the Tran ID of the initial CIT (or in some instances of a previous MIT) associated with the current MIT in either F62.2 or F125. Visa forwards this information to Issuers only in F125 The Tran ID seen by Issuers in F62.2 is that of the current MIT, as sent by Visa, and not that of the initial CIT	This is a 16 digit value
F63.3	Acquirer	Indicates if the transaction is an out of scope MIT of the following type: Incremental Delayed Charges No Show Resubmission Reauthorization Indicates the transaction is deferred.	Values 3900 to 3904 indicate MITs Value 5206 indicates the transaction is deferred, i.e. that it could not be submitted at the time of the Transaction due to no connectivity, system issue or other limitations.
F123	VisaNet	Contains additional data relating to a token transaction	Includes the TAVV Results Code in Dataset 67, tag 08.
F125	Acquirer	Acquirers may indicate the Tran ID of the initial CIT (or in some instances of a previous MIT) transaction associated with the current MIT in either F62.2 or F125. Visa forwards this information to Issuers only in F125	For Issuers in an MIT transaction, the Tran ID associated with the initial CIT (or in some limited instances the with a previous MIT) where agreement was set up (and SCA performed) see Section 3.8.2.1 for more details
F126.13	Acquirer	Used to indicate (with F125 or F62.2) if the transaction is a Recurring, Installments/Prepayment or Unscheduled Credential on File out of scope MIT	Value R, I or C
F126.20	VisaNet	3DS Indicator: optional field that identifies the authentication method used by the Issuer ACS (e.g. Risk Based Authentication). For more details see below	Values 0 to F – see Table 5 in Section 3.2.6

Field	Set by	Function	Field Value/Indicator
F126.8	Acquirer	TAVV Data	If CAVV and TAVV are present, then TAVV Data is in this field. If only TAVV is present, then Acquirer can populate in this field of field 126.9
F126.9	Acquirer	CAVV / TAVV Data	Usage Field 3 supported for EMV 3DS If CAVV is present, this field contains the CAVV. For token transactions without a CAVV, the TAVV can optionally be delivered in this field

The function of each of these fields and the values/tags is described in more detail below.

Table 4 summarizes the key relevant ECI values returned by EMV 3DS. The format and role of the CAVV is summarized in more detail in Section 3.2.7.

Table 4: ECI values

ECI Value	Description	Fraud Liability
ECI 05	Cardholder authentication successful	Issuer
ECI 06	Merchant attempted to authenticate the cardholder but • The Issuer does not participate in Visa Secure or • The Issuer's ACS is unavailable	Issuer
ECI 07	Non authenticated e-commerce transaction or, in the EEA/UK, an SCA exemption or VDAP was used	Acquirer

3.2.3 Exemption/VDAP Requests & supplemental data in Field 34 & SCA decline code (Response Code 1A) in Field 39

Visa has implemented Field 34 to support SCA requirements by indicating an Acquirer applied exemption. Additionally, an SCA decline code (Response Code 1A) in Field 39 is available to Issuers to indicate that the transaction cannot be approved until SCA is applied.

Requirement

Acquirers should specify only one SCA exemption indicator per authorization request.

If an Acquirer requests an exemption in the authentication process, it must be mirrored during authorization. The Acquirer is responsible for this monitoring activity and ensuring that the correct indicator is used throughout the authorization process.

Issuers are required to consider SCA exemption indicators and out of scope information when deciding whether or not to approve an authorization request.

Issuers who receive an Acquirer exemption indicator or a Visa Delegated Authentication Programme (VDAP) indicator in an authorization request must respond with whether they honored the requested exemption/delegation or not.

Acquirers can use Field 34 to submit e-commerce transactions that may include one of the SCA exemption indicators in order to communicate to the Issuer why SCA was not performed on an e-commerce transaction. However, Acquirers should specify only one SCA exemption indicator per transaction message. In the event that the Acquirer specifies multiple SCA exemption indicators, V.I.P. will pass all the SCA exemption indicators available in the transaction to the Issuer, however this may have an adverse impact on Issuers' approval rates. Issuers are required to consider SCA exemption indicators, VDAP indicator, and out of scope information when deciding whether or not to approve an authorization request.

Tags listed in Table 3 above, are used to carry the SCA exemption indicators in the Field 34 Dataset ID 4A. These tags are ISO specification compliant and are not Visa specific.

Issuers and Acquirers in Europe are mandated to support all SCA tags in Field 34 Dataset Hex4A. The right to apply and/or accept the exemptions indicated in Field 34 remains that of the Acquirer and Issuer, and all parties must be technically capable of sending and receiving these fields.

Issuers must complete VisaNet Certification Management Service (VCMS) certification before the field is activated.

Table 23 in section 1264.4 provides a simple summary of the indicators for the key exemptions along with the liability for fraud related chargebacks.

Note that Visa is also making available to Issuers supplemental data in various tags of Field 34 to enrich Issuer's transactional risk management decisioning for card-not-present (CNP) transactions. For example, the consumer device IP address, the Risk Based Analysis (RBA) score and the Visa Consumer Authentication Service (VCAS) score. This is available via

subscription to the Visa Intelligent Data Exchange Service (IDX). For more details, refer to Appendix A.6)

3.2.3.1 Impact for Acquirers

Acquirers in the Europe region must be able to:

1. Support Field 34—Electronic Commerce Data, Dataset ID 4A—Supplemental Data in TLV format with tags to indicate whether an e-commerce transaction is exempt from the PSD2/RTS SCA mandate or has been authenticated under VDAP. This includes the ability to submit exemption / or VDAP requests as well as receive responses in exemption/ and VDAP tags
2. Receive the SCA decline code (Response code 1A - Additional customer authentication required) in existing Field 39
    - Acquirers must be able to pass the SCA decline code on to merchants and ensure the reason of the decline is clearly communicated
    - The SCA decline code will be converted to 05 (Do not honor) in Field 39 if the non-EEA/UK Acquirer's parameter is not activated in VisaNet to receive the SCA decline code.

Certification is required for Acquirers to support TLV Field 34, which contains the SCA exemption/delegated authentication indicators in Dataset ID 4A**.** Additional certification is not required for Acquirers to receive the SCA decline code in existing Field 39.

3.2.3.2 Impact for merchants

Issuers will respond to in scope transactions submitted to authorization without SCA having been applied with an SCA decline code (Response Code 1A) if they consider that SCA is required. This applies to transactions submitted with an exemption indicator if the Issuer decides that the transaction does not qualify for the exemption or meet their acceptable risk criteria.

Merchants must be able to respond to an SCA decline code by

- Resubmitting the transaction via EMV 3DS with the 3DS Requestor Challenge Indicator set to 04 (Challenge Requested: Mandate) to ensure that SCA is applied.
- Resubmitting the transaction to authorization with the CAVV and ECI value received

When a merchant receives an SCA decline code, the merchant must not re-submit the same transaction for authorization with an alternative exemption indicator. They must first submit the transaction for authentication before attempting a new authorization request. If they are unable to submit to authentication or if the authentication request fails, they must interpret the SCA decline as a hard decline and they cannot complete the transaction.

Issuers should not respond to correctly indicated out of scope transactions with an SCA decline code.

3.2.3.3 Impact for Issuers

1. Issuers in the Europe region must be able to receive TLV Field 34—Electronic Commerce Data - Dataset ID 4A—Supplemental Data in TLV format with tags to indicate whether an e-commerce transaction is exempt from the PSD2/RTS SCA mandate or has been authenticated under VDAP.
2. Respond with whether they honored the requested exemption/delegation or not when receiving an Acquirer exemption indicator or a VDAP indicator in an authorization.
3. Be able to use the SCA decline code (response code 1A) to request authentication for a transaction received directly in the authorization environment that the Issuer considers requires SCA.

The following rules apply to the application of the SCA decline code:

- An Issuer may use the SCA decline code (response code 1A):
  - When declining a transaction due to the absence of SCA
  - Only where no other decline code is applicable, and only when SCA is required, or
  - If the amount submitted for authorization is higher than the amount authenticated[16]
- An Issuer may not use an SCA decline code on the following transactions:
  - A transaction that is out of scope of SCA (see section 2.3.1) and not requiring SCA:
    - An Issuer may use an SCA Decline Code on a transaction indicated as out of scope when they believe the Transaction has been incorrectly flagged /is not permitted under regulation to be out of scope
    - Note that if a SCA decline code is sent to a non-EEA/UK Acquirer whose BIN is not registered to receive it (it is optional for Acquirers outside of the EEA and the UK to receive it), VisaNet will convert this decline code into the decline code 05 (Do not Honour)
  - An Original Credit Transaction (OCT) that does not contain a CAVV as it is not necessary to authenticate the recipient of an OCT and nor is it possible
  - A refund authorization request that does not contain a CAVV as it is not necessary to authenticate the recipient for this type of transaction and nor is it possible
  - An authorization request where an exemption request was granted at point of authentication. The presence of a CAVV in the authorization field, with either an ECI 05 or 07, implies that the Issuer has approved the requested exemption in the authentication request
  - A non-DAF authorization request containing an ECI 05 and valid CAVV as SCA has already been applied[17]

[16] Or in the UK if the increase does not meet the conditions set by the FCA and detailed in section 2.4

[17] Except if SCA has not been applied at authentication but at authorization the Issuer determines it is required based on new information available.

- An Issuer should not use an SCA decline code on a DAF transaction that is not using VDAP and that went to EMV 3DS before coming to authorization – "Issuer SCA Required" declines are possible at time of authentication. An Issuer in need of declining those transactions due to SCA should do so at time of authentication (i.e. before it reaches authorization)
- An Issuer should not use an SCA decline code solely on the basis of a mismatch between the merchant names, merchant IDs and amounts submitted during authentication and authorization as there are legitimate reasons why this may occur

An Issuer should consider carefully the purpose of an account verification (zero value authorization) before declining with an SCA decline code due to lack of CAVV as many scenarios for which an account verification is used do not require SCA (refer to section 4.8.3.2 for more details).

- The only use case where an Issuer can, with certainty, know that SCA is required is in an initial recurring or instalment request, which can be recognized by the presence of the MIT identifier "R" or "I" in Field 126.13, but with no original transaction identifier in Field 125
- Where the Identifier "C" (stored credential) is used in Field 126.13 but with no transaction identifier in Field 125, the use case may be that of:
    - Adding a card on file for future CITs – in which case SCA is required if risk of fraud. While it is legitimate to determine there is no risk of fraud as no financial transactions, it remains the Issuers assessment and choice and so some Issuers may determine there is a risk and request SCA

    or

    - Setting up an MIT of the type "Unscheduled Credential on File" (i.e. usage based type subscriptions) – in which case SCA is always required.
        - It is the Acquirers responsibility to ensure SCA is provided when setting up an MIT agreement and it is legitimate for an Issuer to assume that if there is no SCA in a transaction with a "C" in POS Environment Field 126.13 it is because it is possibly an "add card" scenario

For more information on Visa Rules governing the use of the SCA decline code please see *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements*. For information on identification of transactions that do not require SCA see sections 3.2.9 and 4.2.5.2.

Issuers should also consider whether they wish to receive supplemental data in F34 to assist their risk decisioning within authorization. See appendix A.6 for more details on this supplemental data. Issuers that choose to receive the supplemental data must be able to receive the associated tags in Field 34 - Electronic Commerce Data and must be aware of processing rules to support this supplemental data.

3.2.4 MIT out of scope indicator for Issuers in Field 34

Visa has introduced an indicator[18] to help Issuers to identify a transaction that is an MIT and out of scope of SCA. The indicator is a value of "1" in Field 34 (Tag 80, Dataset ID 02) i.e. the same field Issuers use to check for exemptions to SCA.

Visa will automatically populate the value of "1" in TLV Field F34, Tag 80, Dataset ID 02 when receiving a transaction indicated as an MIT by the Acquirer using the MIT Framework. Refer to section 3.8 for more details.

An Issuer activated to receive F34 will automatically receive this value when the Acquirer has indicated the transaction as merchant-initiated using the MIT Framework.

This enables Issuers to recognize a transaction as an out of scope MIT by simply looking for the value of "1" in that tag. Issuers may alternatively decide to recognize an MIT out of scope by looking at the indicators from the MIT Framework. See section 3.8 for more details.

An Issuer must not use an SCA decline code in a transaction legitimately indicated as an MIT as the cardholder is not available to be authenticated.

An Acquirer cannot use Field 34, Tag 80, Dataset ID 02 to indicate an MIT out of scope. Only Visa can populate this Tag.

3.2.5 Acceptance environment outage indicator in Field 34

Visa has introduced an indicator in Field 34 that enables Acquirers to indicate that it is not possible to authenticate a transaction due to an outage in the acceptance environment.

More specifically, the indicator means that authentication was attempted for a transaction but there was an authentication outage in the authentication flow between the merchant, gateway 3DS server, and Directory Server, which means an authentication request was not possible and an authentication response could not be received (this indicator should not be used to indicate an outage in the Issuer processing domain, including agents acting on behalf of the Issuer).

3.2.5.1 Issuer impact

Using this indicator is optional for Acquirers. Receiving this field is mandated for Issuers However acting on it is optional. Both Acquirers and Issuers need to consider regulatory requirements and resilience imperatives before deciding to use this indicator. While transactions containing this indicator do not represent transactions that can be considered exempt or out of scope of the SCA regulation, the presence of the indicator enables the Issuer to understand that this is a transaction where an authentication is expected but could not be performed due to an outage. This provides Issuers with the ability to explain to a regulator why they may have decided to authorize an in-scope transaction without authentication, on an exception basis, to support resilience.

[18] See *Article 9.1.4 Changes to Identify Merchant-Initiated Transaction as Out of Scope for Strong Customer Authentication, Oct 19* for more details.

Approving transactions with this indicator and without authentication is at the Issuer's discretion. It is recommended that in deciding their authorization policies with respect to this indicator, Issuers:

- Consider regulatory requirements balanced with the intent to support resilience/business continuity/cardholder experience. Issuers could for example decide to support the indicator every time it is sent or could decide to authorize indicated transactions only when the outage is major/longer than unusual. Each Issuer needs to determine its own policies
- Perform risk-based analysis on each transaction and decline if the transaction is high risk
- Ensure that reasons to decline other than lack of authentication are considered first as usual (e.g. declines for insufficient funds, block card or similar that would inform the merchant there is no opportunity for an approval)

Considering that authentication is not available due to an outage, European Issuers are recommended to carefully consider whether use of an SCA decline code is appropriate. An SCA decline code may indicate to the merchant that if the option is available to resubmit with authentication once the 3DS environment is accessible, the Issuer may reconsider the response if authentication is provided. Issuers should note however that authentication may not be possible if the customer is no longer available.

3.2.5.2 Acquirer impact

The use of the indicator is optional for Acquirers. Acquirers need to consider regulatory requirements and resilience imperatives before deciding to use this indicator. Acquirers must be aware of additional conditions that will apply for their merchants to be permitted to use this indicator, including Acquirer monitoring requirements[19].

3.2.5.3 Deferred authorization indicator in F63.3

This indicator (value of 5206 in Field 63.3) indicates that a transaction was deferred, i.e. it could not be submitted because there was no connection available or there was another system issue at the time of authorization. This prevented authorization from occurring at the time of the transaction, which also meant there was no ability to authenticate. Merchants should collect the transaction information and send a deferred authorization request at the earliest possible opportunity. Such a connectivity issue may occur for example when airlines or train operators make sales in transit.

3.2.5.4 Issuer impact

Recognizing and acting on this indicator is optional for Issuers. Issuers should consider their regulatory obligations before deciding whether to use this indicator. Transactions containing this indicator do not represent transactions that can be considered exempt or out of scope of the SCA regulation, but the presence of this indicator enables Issuers to understand that this is a transaction where authentication could not be performed due to lack of connectivity at the time of the transaction. The transaction can be submitted by the merchant when

[19] These conditions are documented in *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom : Visa Supplemental Requirements.*

connectivity is restored, which may be when the customer is no longer available to authenticate, and the goods and services may have already been provided.

3.2.5.5 Acquirer impact

Merchants are required to include this indicator on all deferred authorization requests. Merchants are recommended to use the indicator in any deferred authorization so that Issuers can recognise that the transaction has been deferred due to lack of connectivity.

This may minimise, but not eliminate cases where the Issuer responds to an authorization request with an SCA decline code as approving transactions with this indicator and without authentication is at the Issuer's discretion. To optimise the chance of approval, merchants should consider requesting an exemption if one is applicable to that transaction.

3.2.6 VisaNet 3DS Indicator Field 126.20

Visa has included an optional field in authorization – 3DS Indicator (Field 126.20) – to identify the authentication method used by the Issuer's ACS to authenticate the cardholder (e.g. risk-based authentication or OTP).

This field provides Issuers with more visibility into the authentication process during authorization for use in decisioning.

The 3DS Indicator value is derived from Position 2 of the CAVV present in Field 126.9.

Issuer host systems can now choose to receive the 3DS Indicator (Field 126.20). Issuers planning to utilize the 3DS Indicator Field 126.20 must complete VisaNet Certification Management Service (VCMS) certification before the field is activated.

The field is optional, so there is no impact on Issuers that do not wish to receive this field.

Best Practice

Issuers are strongly encouraged to use Field 126.20 as it provides valuable information about the authentication to help better authorization decisioning.

Field values are shown in Table 5 below. For the latest updates to 126.20 refer to the *VisaNet Authorization-Only Online Messages Technical Specifications* available on Visa Online.

Table 5: The values for Field 126.20

3DS Indicator Value	3DS Description
0	3DS 1.0.2 or prior all authentication methods
1	Challenge flow using Static Passcode
2	Challenge flow using OTP via SMS method
3	Challenge flow using OTP via key fob or card reader method
4	Challenge flow using OTP via App method
5	Challenge flow using OTP via any other method
6	Challenge flow using KBA method
7	Challenge flow using OOB with Biometric method
8	Challenge flow using OOB with App login method
9	Challenge flow using OOB with any other method
A	Challenge flow using any other authentication method
B	Unrecognized authentication method
C	Push Confirmation
D	Frictionless flow, RBA Review
E	Attempts Server responding
F	Frictionless flow, RBA
G	Issuer defined ACS-specific authentication method 1[20]
H	Issuer defined ACS-specific authentication method 2[20]
I	Issuer defined ACS-specific authentication method 3[20]
J	Issuer defined ACS-specific authentication method 4[20]
K	Issuer defined ACS-specific authentication method 5[20]

3.2.7 CAVV / TAVV Support and Fields 126.8, 126.9 and 44.13

3.2.7.1 Use of the CAVV

The CAVV is a unique cryptogram created for each 3DS authenticated transaction. It provides proof that cardholder authentication occurred or that the merchant attempted authentication. Visa requires Acquirers to include CAVV data for all 3DS authenticated transactions (ECI 05 and ECI 06). Any ECI 05 or ECI 06 transactions without a CAVV will be downgraded to ECI 07 and the Acquirer will no longer benefit from fraud liability protection. The use of a CAVV helps

[20] CAVV v7 only.

secure the integrity of 3DS transactions, enables end-to-end transaction traceability and further streamlines the dispute/chargeback process.

The CAVV is generated and populated as follows:

- The CAVV is generated by the Issuer's ACS when a successful authentication is completed, or by Visa when the Visa Attempts Server when it stands in for the Issuer's ACS (ECI 06)
- Each step in the authentication process is validated by the Issuer or the Issuer's ACS on their behalf and should the validation fail at any point, a CAVV would not be generated
- Measures should be in place to ensure the CAVV cannot be compromised
- The CAVV is a cryptographic representation of the amount and payee as agreed by the payer and as such may not necessarily include the actual raw data (CAVV version 7 only)
- Visa's authentication code is dynamically linked to the amount and the payee
- The merchant populates F126.9 with the CAVV which is then validated by the Issuer (or Visa where CAVV keys are provided) during authorization

For more information on CAVV creation, current supported versions, verification and use in authorization please refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

Issuers can use the CAVV to link to the authentication message, thus meeting the dynamic linking requirement. Issuers can check that the amount submitted for authorization does not exceed the amount authenticated, as required under dynamic linking[21], by checking the Authentication Amount in the CAVV. Note that Authentication Amount is only available in CAVV U3 V7. For more details on how to do this please refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

Issuers may additionally choose to:

- Investigate specific transactions such customer disputed transactions
- Validate the (hashed) merchant name and transaction amount from the authentication message in real time.

Merchants must ensure that the EMV 3DS authentication request is accurately populated with the following information:

- Total transaction amount
- Merchant descriptor name[22] (where required)

[21] In the EEA, the PSD2 SCA dynamic linking provision requires that reauthentication is required if the final amount to authorize exceeds the amount authenticated. In the UK, the final amount may be up to 20% higher than the authenticated amount so long as certain criteria are met. Please refer to section 4.2.2.3 for more information.

[22] For more information on populating the merchant name when the party requesting authentication is not the merchant that will request authorization see Section 4.8.3.7. Detailed guidance on dealing with merchant naming in travel agent booking use cases is given in the supplement to this guide:

- 3DS requestor ID

Visa requests that until 18 October 2024, Issuers allow a CAVV to be used up to five times. Note that if a CAVV is used in a transaction that is declined, this instance does not count as one of the five allowed instances[23].

3.2.7.2 TAVV Data in Field 126.8

A token cryptogram is a unique encrypted value that is dynamically generated by Visa and used for authentication of tokenized transactions that are processed through Visa Token Service. Also referred to as Token Authentication Verification Value (TAVV).

Field 126.8 allows Acquirers to:

- Send the TAVV data received from VTS in the authorization and full financial request messages with the ECI value

Acquirers must be capable of sending the TAVV data as described above for token based EMV 3DS transactions.

Visa also strongly recommends that Acquirers send TAVV Data in Field 126.8 when this is the only cryptogram data sent in token transactions without EMV 3DS. However, Visa will continue to process the token transaction if TAVV was sent in Field 126.9, Usage 3.

For token transactions that go straight to authorization without first performing EMV 3DS, Field 126.9 can optionally be populated with the TAVV.

3.2.7.3 CAVV / TAVV Data in Field 126.9

Field 126.9 allows Acquirers to:

- Include the CAVV data in the authorization and full financial request messages with the ECI value

Acquirers must be capable of sending the CAVV data as described above. If an Acquirer does not include CAVV data in field 126.9 for an ECI 05 or ECI 06 transaction, the ECI value will be downgraded to ECI 07 (non-authenticated).

For token transactions that go straight to authorization without first performing EMV 3DS, Field 126.9 can optionally be populated with the TAVV, however, Visa strongly recommends that Acquirers send TAVV Data in Field 126.8.

3.2.7.4 Field 44.13 CAVV Results Code

Field 44.13—CAVV Results Code contains a one-character code that indicates the following:

Implementing Strong Customer Authentication (SCA) for Travel & Hospitality. This methodology is not restricted to travel booking agent: it can also be used by merchant servicers.

[23]Visa has temporarily permitted, under waiver, the reuse of the CAVV up to five times. for split shipment scenarios and scenarios where transactions are associated with bookings via travel agencies. The previous waiver to allow CAVV reuse expired on 1 September 2022 and has now been extended to 18 October 2024 and to use cases where Merchant Servicers may be authenticating on behalf of other merchants. For more information please see VBN Article ID: AI10292 *Update to CAVV—Exceptions to Reuse in Europe* 20 August 2020 and VBN Article ID: AI12280 *New Rules and Updated Guidance to Support Transaction Processing in Line with SCA Requirements in the EEA and UK*

- The classification of the transaction (either an authentication transaction where the Issuer ACS has created the CAVV or an attempts transaction where the Visa Attempts Server has created the CAVV)
- For an authentication transaction, where the Issuer ACS has created the CAVV
- For an attempts transaction, where the Visa Attempts Server has created the CAVV
- The CAVV verification result:
    - CAVV verification passed
    - CAVV verification failed

For token transactions that go straight to authorization without first performing EMV 3DS, Field 44.13 can optionally be populated with the TAVV results code, but only if the Issuer does not support field 123.

CAVV Results code values and descriptions are included in the *VisaNet Business Enhancements Global Technical Letter and Implementation Guide October 2018 Version 3.0 (Major Release) and January 2019 Version 2.0 (Minor Release) – effective 6 September 2018*.

3.2.7.5 Use of the CAVV in account verification

Non-Payment Authentication (NPA) requests were introduced in EMV 3DS to enable a merchant to submit an authentication request when the transaction is initiated for a non-payment use case such as adding a card to a merchant's website, modifying stored cardholder information, or Issuer identification and verification of a cardholder during Visa token provisioning. This is particularly important in the SCA context.

If a 3DS Server sends an NPA AReq with 3DS Requestor Authentication Indicator of "06 = Cardholder Verification as part of EMV token ID&V" an Issuer must respond with a challenge request and the 3DS Server must proceed with initiating the challenge.

All fully authenticated NPA transactions, including those in a frictionless flow, must contain proof of authentication in the form of an electronic commerce indicator (ECI) 05 and a Cardholder Authentication Verification Value (CAVV) with the NPA indicator (1: Authentication Successful, NPA Transaction) in position 1.

To support the account verification transaction where SCA is performed all Acquirers and Issuers in Europe are required by Visa to receive the CAVV Results Code when it is present in account verification transactions. Clients should refer to Article 9.1.2— Mandate to Support CAVV Results Code Field in Account Verification Transactions in the Europe Region in the *October 2020 and January 2021 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 18 June 2020* for more information on the change and its processing impact. For more information on account verification use cases please refer to section 4.8.3.2. An account verification may include a CAVV that is either NPA or PA.

For more information of the CAVV creation, verification and use in authorization please also refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

3.2.8 Acquirer support of ECI and CAVV Data

Acquirers that support e-commerce, or application-based e-commerce transactions for PANs or tokens must be prepared to support the following:

- ECI 07 in existing Field 60.8—Mail/Phone/Electronic Commerce and Payments Indicator in authorization request messages
- ECI 07 in existing Field 63.6—Chargeback Reduction/BASE II Flags, position 4, MOTO/ECI Indicator in full financial request messages
- CAVV data in existing Field 126.9—CAVV Data, Usage 3: EMV 3DS CAVV, Revised Format in authorization and full financial request messages
- ECI 07 in BASE II Draft Data

Issuers will continue to have the option to receive existing CAVV and ECI fields to support CAVV processing.

3.2.9 Identifying Out of Scope & other transactions not requiring SCA

The following transaction types are out of scope of SCA

- Mail Order/Telephone Order (MOTO)
- Merchant Initiated Transactions (MITs)
- One-Leg-Out (OLO) transactions[24]
- Anonymous transactions

Out of scope transactions are identified as summarized in Table 6 below.

[24] Although One-Leg-Out transactions are out of scope, Acquirers and merchants are reminded that SCA should still be performed on a best effort basis.

Table 6: Out of scope of SCA transaction indicators

Out of Scope Transaction Type	Indicators
MOTO	Mail order and telephone order (MOTO) transactions are out of scope of SCA and are indicated in the Visa processing system by a value of: • 08 in Field 25 (Point-of-Service Condition Code), and/or • 01 or 04 in Field 60.8 (Mail/Phone and Electronic Commerce and Payment Indicator) • In cases where a value of 08 is being used in Field 25 Acquirers must not use a value 02 or 03 in Field 60.8 (refer to Table 40 in section 5.12.2 for more details on this) and are recommended to also populate value 01 or 04 in F60.8
Merchant Initiated Transactions (MITs)	Merchant Initiated Transactions identified by Acquirers through the use of the Visa MIT Framework and by Issuers either by the use of the MIT Framework or by the MIT out of scope indicator (value 1) in Tag 80, dataset 2 of Field 34 (Electronic Commerce Data)[25]
One-Leg-Out (OLO)	In the Visa processing system, these transactions are recognized by: • An Issuer BIN outside of the EEA or UK, or • An Acquirer location outside of the EEA or UK (Field 19 – Acquiring Institution Country Code) In EMV 3DS these transactions can be recognized by • The Acquiring Institution Country Code (ACC) indicator in the EMV 3DS ACC extension, which is available for EMV 3DS 2.1 and 2.2 Note that in these cases, SCA should still be applied on a 'best effort' basis so SCA may be performed. For more information on one-leg-out use cases and application of best efforts please see section 2.3.2
Anonymous	Transactions performed with anonymous cards[26] are out of scope of SCA; however, they cannot be recognized as such by merchants. In this case, the following approaches are possible for merchants: **Option 1 -** They can proceed to authentication - in which case, • When the card is not enrolled and not participating in EMV 3DS, the response, in EMV 3DS, will be an ARES = N with an ECI 07 and "Not Authenticated/Account Not Verified" message and a transaction status response code will be sent with a Transaction Status Reason

[25] See Section 3.8 for more details. Note that in addition to transactions not initiated by the payer (and which are therefore out of scope), the MIT field will also indicate transactions which are not out of scope but where SCA has already been performed or an exemption was applied before the transaction was executed – only for specific cases outlined in Section 3.8.

[26] In the Visa system, these can include non-reloadable prepaid cards on which no KYC has been done and thus where the Issuer cannot authenticate the identity of the cardholder. The card is not enrolled in EMV 3DS. The fact that no KYC has been done and/or that it is a non-reloadable prepaid card will not necessarily mean the card is anonymous in all cases.

	Code 87 "Transaction is excluded from Attempts Processing e.g. non-reloadable, TRA, etc." • When the card is enrolled but not participating in EMV 3DS, the response will be an ARES = N with an ECI 07 and a Transaction Status Reason code of the Issuer's choosing conveying the card cannot be authenticated Upon receiving such responses, the card may be an anonymous one so merchants should send transaction to authorization **Option 2 -** They can proceed direct to authorization in which case Issuers are being asked to recognize BINs/account ranges for out of scope cards and should not request SCA on anonymous cards

Visa considers that SCA may not be required to be performed by the cardholder for the following additional transactions summarized in Table 7:

Table 7: Identification of additional transactions not requiring SCA by the cardholder

Transaction Type	Indicators
OCTs & refunds	Original Credit Transactions (OCTs) and refunds do not require SCA to be performed by the recipient of the funds (i.e. the cardholder). Therefore, an Issuer may not use the SCA decline code in response to authorization requests properly identified as OCTs or refunds. • Issuers can identify an OCT by checking for processing code value of 26 in Field 3.1. For more information, refer to Section 4.10. Issuers can identify a refund transaction by value 20 in Field 3.1 (if processed via authorization – most refunds are processed via clearing only).
Zero value authorization/account verification requests	Transaction where amount is zero. An Issuer will not be able to tell which of these transactions requires SCA (some legitimately do not). Issuers should refer to section 4.8.3.2 to recognize scenarios where they should/should not request SCA when the transaction is of zero value.

3.2.9.1 Recognition of out of scope transactions - Acquirer impact

1. If a payment transaction is out of scope of SCA, then the merchant / Acquirer must submit an authorization request ensuring that appropriate information is present that allows the Issuer to recognize that the transaction is out of scope, for example, by including relevant MIT indicators, or properly flagging as MOTO as described in the above table. Transactions that are not correctly indicated are at risk of being declined by Issuers. For example:
    - For MITs, this means supporting the MIT Framework for both PAN and token transactions
    - Transactions that are key entered in a PoS system and submitted without any MOTO or MIT indicators(s) may not be recognized by Issuers as MOTO or MIT out of scope transactions. If they are MOTO or MITs, the appropriate indicator must be added to the transaction.

- Transactions that are key entered by merchants into a PoS system in order to complete a transaction initiated by the cardholder over the phone must have a MOTO indicator in the transaction.
- Transactions that are key entered by merchants into a PoS system in order to complete a transaction associated with an indirect sales travel booking may often be MITs (subject to authentication being performed by the third party agent at the time of booking, to create the MIT mandate). The ability to indicate MITs may require upgrading of and additional integration between PoS and booking systems used by booking agents, intermediaries and merchants in order to pass the required authentication data. If this cannot be done yet, an interim solution allows these transactions to be indicated as MOTO as long as authentication has been applied at the time of booking (which is required unless the transaction qualifies for the secure corporate payments exemption) and other relevant requirements are met.[27] Visa has updated its rules to reflect the conditions for the usage of the MOTO indicator in the travel & hospitality sector as part of this interim solution. These rules aim to ensure the indicator is not abused and that use of the solution does not result in increased fraud. Improper usage will be subject to removal of the right to use the indicator. An end date after which the interim solution can no longer be used will be announced with a minimum of one year's notice when there is an understanding of a realistic travel & hospitality ecosystem implementation timeline. However, implementing fully integrated solutions enabling appropriate flagging as MITs may take longer than this, merchants/Acquirers are therefore encouraged to plan/implement the use of appropriate solution as soon as possible.

- MIT and MOTO indicators (with the exception set out above) can only be used for legitimate MOTO and MIT transactions. Appropriate indicator usage for MOTO and MIT transactions are further detailed in Table 40, section 5.12.2

2. Transactions that are acquired across the EEA and the UK are considered in scope, even if the merchant is outside the EEA and/or the UK. In this case, Acquirers should work with their merchants to ensure that SCA can be applied.
3. Where the Acquirer is inside the EEA or the UK but the Issuer is outside (one-leg-in), SCA should be applied on a best effort basis and Acquirers are recommended to send transactions for SCA, for example by submitting the transaction via EMV 3DS, where this is supported by the non-EEA/UK Issuer. Merchants can identify whether Issuers support EMV 3DS and which version is supported through their gateway or 3DS server provider[28].
4. Acquirers are reminded to ensure that F19 is populated with the correct Acquiring Institution Country Code in the authorization message. If the Acquiring Institution Country Code is not present or is incorrect, the Issuer will not be able to determine whether or not SCA is required and may decline the transaction. The "correct" Country Code to use in F19 is that of the location associated with the Acquirer BID (which reflects where the Acquirer

[27] Refer to VBN Article ID 10295 *Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions* for more details.

[28] For more information on identifying whether Issuers support EMV 3DS and which version they support, see section3.3.12.

is domiciled and therefore regulated) and not the location associated with other potential Acquirer BINs.

5. Acquirers should note that the EMV 3DS ACC extension should not directly impact merchants and does not require any changes. The ACC will be populated by Visa upon receipt of the acquiring BIN in 3DS.

3.2.9.2 Recognition of out of scope transactions Issuer impact

Issuers in the Europe region must:

1. Be able to recognize every type of out of scope transaction. For MITs, they can do so using either the Visa MIT Framework or using the new MIT out of scope indicator in F34.
    - In the case that an Issuer selects to recognize MITs using the Visa MIT Framework, they must be able to receive the original Transaction ID in Field 125 if they do not already receive it (currently optional).[29]
2. Not use an SCA decline code, or equivalent, for authorization requests for transactions that[30]:
    - Are deemed out of scope from a regulatory perspective, as specified in Table 6, or
    - Do not otherwise require SCA as specified in Table 7

    This is especially important as merchants are not in a position to obtain SCA on those transactions. Note that when Issuers receive a transaction without SCA they must always check the BIN before deciding whether to decline, in order to determine whether the card is anonymous.
3. Identify transactions acquired outside the EEA and the UK through the Acquiring Institution Country Code in F19 of the authorization request, not by the merchant country code (Field 43).
4. Recognize both indicator options identified in Table 6 above to ensure recognition of all MOTO transactions as merchants can use either or both options.
5. Issuers and their ACS vendors are impacted by the introduction of the EMV 3DS ACC extension. Issuers should work with their ACS vendors to ensure that this new data element is supported and implement appropriate processing rules.
6. In the case of a one-leg-out transaction, if the EEA/UK Issuer receives a request for authentication from a non-EEA/UK acquired merchant, they should decide whether to approve, apply SCA (where possible) or decline the transaction in line with the best efforts requirement, and considering the risk, customer experience and liability implications.

[29] For more information on the reception and use of the original Transaction ID please refer to Section3.8.2.1.

[30] For more information please refer to: *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements applying to the EEA and UK*

3.3 3-D Secure (EMV 3DS)

This section provides a brief summary of the key features of EMV 3DS. More details and the full specifications are available from EMVCo at https://www.emvco.com/emv-technologies/3d-secure.

EMV 3DS is the industry standard solution adopted by card schemes, Issuers and Acquirers to enable the application of SCA. Merchants must support EMV 3DS to facilitate the application of SCA which is required under PSD2. Visa rules do not preclude Issuers and Acquirers agreeing alternative means of performing SCA.

3-D Secure 2.0 (referred to in this guide as EMV 3DS, but also known as 3DS 2.0) is the latest global specification for card payment security developed by EMVCo. It is designed to deliver frictionless payment authentication across a range of devices, including mobile handsets. Unlike previous versions of 3DS, it allows for more seamless integration with merchants' e-commerce customer experiences, and has been universally adopted across the card payment ecosystem. .

Three versions of the EMV specification have so far been released. Version 2.1 (EMV 3DS 2.1) was released in October 2017 and went live Q4 2018. Version 2.2 (EMV 3DS 2.2) was released December 2018 and went live Q4 2019. EMV 3DS 2.2, delivers optimised solutions for the application of Visa products and SCA compliant functionality, is implemented by all Issuers and Acquirers and all merchants are strongly encouraged to support it. Visa is currently assessing the latest version (2.3, published September 2021) and will provide dates for testing and support when confirmed.

EMV 3DS is used both for authenticating payment transactions and verifying the identity of the cardholder when the cardholder is setting up an arrangement for one or a series of Merchant Initiated Transactions.

EMV 3DS may also be used by to indicate:

- Acquirer exemptions (TRA and low value)
- Issuer applied exemptions that can be indicated by the merchant or Acquirer (trusted beneficiaries and secure corporate payments)
- That authentication has been applied under the Visa Delegated Authentication Program (VDAP) (see section 3.6.3 for more information)

If a merchant would like to indicate that an Acquirer exemption is to be applied, or that an Issuer exemption should be considered (for SCP and trusted beneficiaries), the appropriate exemption indicator should be set in the Transaction Challenge Exemption field of the Authentication Request. For more information on the 3DS exemption application flow please see section 4.2.7. Merchants should note that when they indicate an exemption through EMV 3DS they must still include the corresponding exemption indicator in the subsequent authorization request along with the CAVV and ECI value.

Merchants may choose to use EMV 3DS to indicate application of an exemption to reduce the risk of the cardholder no longer being present to complete an SCA challenge if the Issuer determines that SCA is required.

Visa has adopted the brand name "Visa Secure" for Visa EMV 3DS in consumer branding and communications. For simplicity this guide just refers to EMV 3DS.

The original version of 3-D Secure, 3DS 1.0.2, was sunsetted on 15 October 2022. It has seen a significant decline in usage compared to EMV 3DS, due to limited SCA application, poorer user experience and the eco-system preference for EMV 3DS when applying SCA.

Information about Visa's EMV 3DS program can be found in the *Visa Secure Issuer Implementation Guide for EMV 3-D Secure and Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure on Visa Online and on* the Visa Technology Partner site https://technologypartner.visa.com/Library/3DSecure2.aspx.

3.3.1 The benefits of EMV 3DS

EMV 3DS is a fundamental upgrade of the global standard for card-based e-commerce transaction authentication. The benefits it brings include:

- Use of Risk Based Authentication, utilizing a significantly increased number of transaction and customer data elements to securely authenticate the majority of transactions, without the need for additional customer friction
- Full compatibility with mobile and native app environments allowing mobile in-app, as well as mobile and computer browser transactions to be authenticated through a seamless user experience, even when SCA is required
- Integration with the merchant checkout user experience, including merchant branding options to further support a seamless customer journey
- Additional functionality which underpins the move to biometrics,
- Supports the SCA required request required when authenticating a new MIT agreement or responding to an SCA decline code
- Provides the ability to take advantage of SCA exemptions (EMV 3DS 2.2) and data indicates that routing transactions via EMV 3DS can increase transaction success rates for the Acquirer TRA exemption
- Accommodates the delivery of a cryptogram in complex merchant use cases such as travel.

3.3.2 EMV 3DS version feature comparison

The following Table 8 provides a comparison of the main features of EMV 3DS 2.1 and EMV 3DS 2.2.

Table 8: 3DS version notable feature comparison

Notable Features	3DS 2.1	3DS 2.2
Capable of providing two factor authentication (2FA – static data, OTP)	Y	Y
Dynamic linking - CAVV generated links authentication to the payment	Y	Y
Basic Issuer TRA (provided by the Issuer ACS)	Y	Y
Mobile banking app integration	Y	Y
Biometric authentication	Y	Y
Real time Dynamic linking + - CAVV includes merchant name and amount	Y	Y
Mobile Device Compatibility	Y	Y
• Native	Y	Y
• HTML	Y	Y
3RI		
• Non-Payment authentication	Y	Y
• Payment authentication with ability to obtain, refresh and regenerate CAVV	Y[31]	Y
• Decoupled authentication	N	Y
Decoupled authentication[32]	N	Y
Acquirer Exemption indicators		
• TRA performed prior to authentication	N	Y
• Trusted beneficiaries	N	Y
Merchant/Acquirer request for SCA to be applied	Y	Y
Secure corporate payments (SCP) exemption	Y	Y
Acquiring Country Code (ACC) extension	Y	Y
Enhanced TRA plus data (100+ data elements)	Y	Y

Merchants should utilise the information received in the PReq/Pres exchange to determine the versions of EMV 3DS that are supported by the Issuer ACS.

[31] Visa has defined a method for EMV 3DS 2.1.0 to support 3RI purchase transactions. Please note this approach is specific to Visa cards and is not included in the EMV 3DS specification.

[32] Functionality in EMV 3DS 2.2 that allows for authentication of cardholders independent from the purchase flow.

EMV 3DS 2.2 introduces five new values for the 3DS Requestor Challenge Indicator field in the Authentication Request message to support application of exemptions and delegated authentication. For details of these indicators please refer to *the Visa Secure Program Guide*.

3.3.3 3DS Requestor Initiated (3RI)

The 3RI functionality allows the merchant to initiate an authentication request without the cardholder being present. This enables several merchant use cases. For example;

- It enables a merchant to obtain authentication data (CAVV, ECI) for transactions that have been previously authenticated and where the CAVV is no longer valid. For example, in the case of a delayed shipment which delays the authorization beyond 90 days. This allows the merchant to maintain their fraud liability protection under legitimate circumstances.
- It allows a merchant to obtain additional CAVVs associated with a single authentication interaction with the cardholder in the case of a split shipment where more than one authorization is needed.
- It allows an authorised entity in a Multi-Party Commerce scenario to request a CAVV on behalf of merchant(s).
- Non-payment (NPA) messages can be used to confirm an account is still valid for cardholder authentication.

Merchants and 3DS Server vendors should note that for some 3RI transactions the 3DS Server should provide 3DS Requestor Prior Transaction Authentication Information including:

- 3DS Requestor Prior Transaction Authentication Method: This is the mechanism used by the Cardholder to previously authenticate to the 3DS Requestor
- 3DS Requestor Prior Transaction Authentication Timestamp: The date and time in UTC of the prior cardholder authentication
- 3DS Requestor Prior Transaction Reference: This data element contains an ACS Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).

This additional data allows Issuers to identify the requests and improves risk management and provides a secondary evaluation of the previously authenticated transaction. The subsequent request to the Issuer may not always result in an approved transaction as the Issuer may reassess the transaction and merchants should cater for this in their systems.

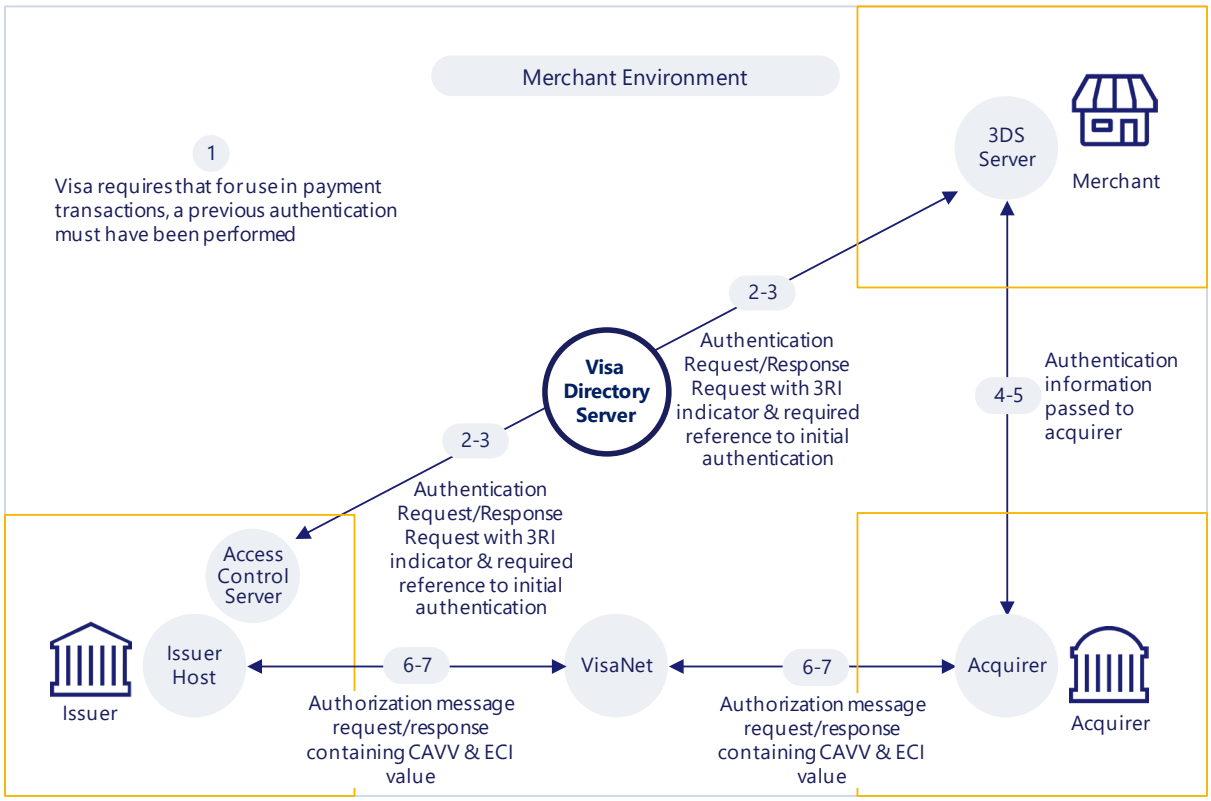
Examples of where this may be used for specific transaction types are included in sections 5.4 and 5.17.

Figure 4 below shows the standard 3RI flow.

For more information on the application of 3RI please refer to sections 3.3.3, 4.2.5.3 (Table 21 principle 3), and 4.8.2.

For the split-shipment/delayed shipment/multi-party ecommerce use cases (including travel), usage of 3RI is complex and further guidance on this will be provided. Until 18 October 2024, merchants can re-use a CAVV (permitted for a maximum of 5 times).

Figure 4: 3RI flow



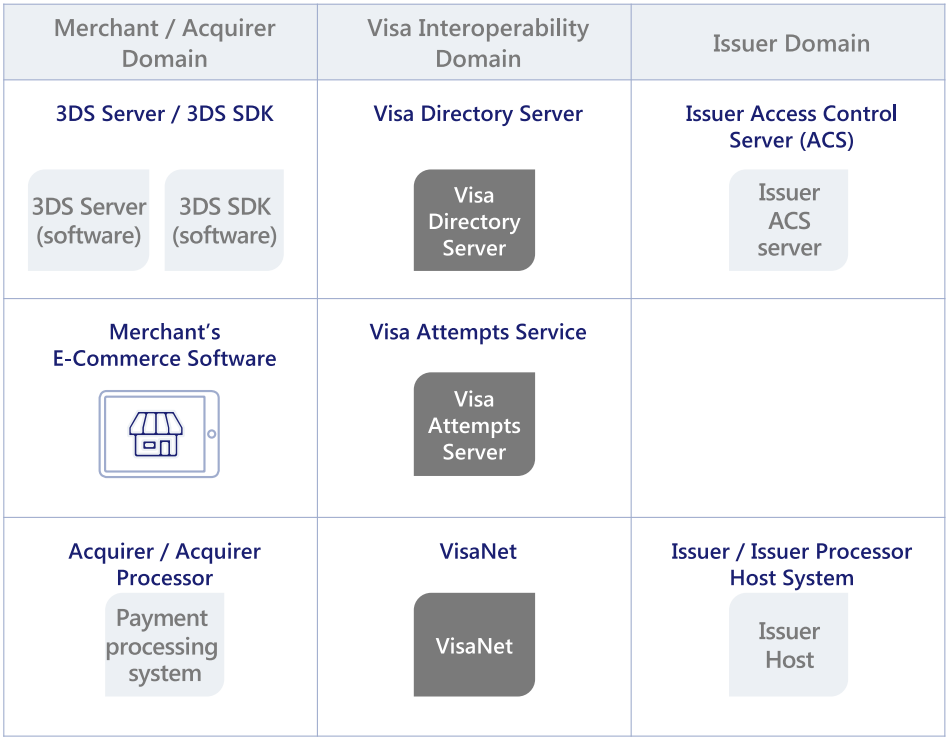
3.3.4 EMV 3DS domains and components

Visa's EMV 3DS Program defines three distinct domains that interact to support authentication and authorization:

- The merchant/Acquirer Domain
- The Visa Interoperability Domain
- The Issuer Domain

These domains and the main components acting in each domain are illustrated in Figure 5 below:

Figure 5: EMV 3DS domains and components



For more details on the domains and components, please consult *Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure* and *Visa Secure Issuer Implementation Guide for EMV 3-D Secure 2.0*.

Table 9: The role of the main components

Component	Role
3DS Requestor	The initiator of the EMV 3DS Authentication Request. For example, this may be a merchant.
3DS Client	The consumer-facing component supports consumer interaction with the 3DS Requestor for initiation of the EMV 3DSprotocol.
3DS Server	The 3DS Server provides the functional interface between the 3DS Requestor Environment flows and the DS. The 3DS Server is responsible for: • Collecting necessary data elements for EMV 3DS messages • Authenticating the DS • Validating the DS, the 3DS SDK, and the 3DS Requestor • Ensuring that message contents are protected
3DS Requestor App	An App on a Consumer Device that can process an EMV 3DS transaction through the use of a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK
3DS Requestor Environment	The 3DS Requestor-controlled components (3DS Requestor App, 3DS SDK, and 3DS Server) are typically facilitated by the 3DS Integrator. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator

Component	Role
3DS SDK	The mobile-device-side component of 3DS is the 3DS Mobile SDK. 3DS Requestors integrate this SDK with their mobile commerce or 3DS Requestor app and the SDK facilitates the sending and receiving of 3DS messages and the displaying of challenge screens to the cardholder
3DS Integrator	An EMV 3DS participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer
Directory Server (DS)	The DS performs a number of functions that include: • Authenticating the 3DS Server and the ACS • Routing messages between the 3DS Server and the ACS • Validating the 3DS Server, the 3DS SDK, and the 3DS Requestor • Defining specific program rules (e.g., logos, time-out values) • Onboarding 3DS Servers and ACSs • Maintaining ACS and DS Start and End Protocol Versions and 3DS Method URLs • Interacting with VTS to de-tokenize messages originating from tokens
Issuer Access Control Server (ACS)	The ACS contains the authentication rules and is controlled by the Issuer. ACS functions include: • Verifying whether a card number is eligible for 3DS authentication • Verifying whether a Consumer Device type is eligible for 3DS authentication • Authenticating the cardholder or confirming account information
Visa Attempts Server	Stands in for the Issuer's ACS and responds to the 3DS Requestor if the Issuer's ACS is unavailable
VisaNet	Routes 3DS messages between the appropriate 3DS Requestor and Issuer ACS

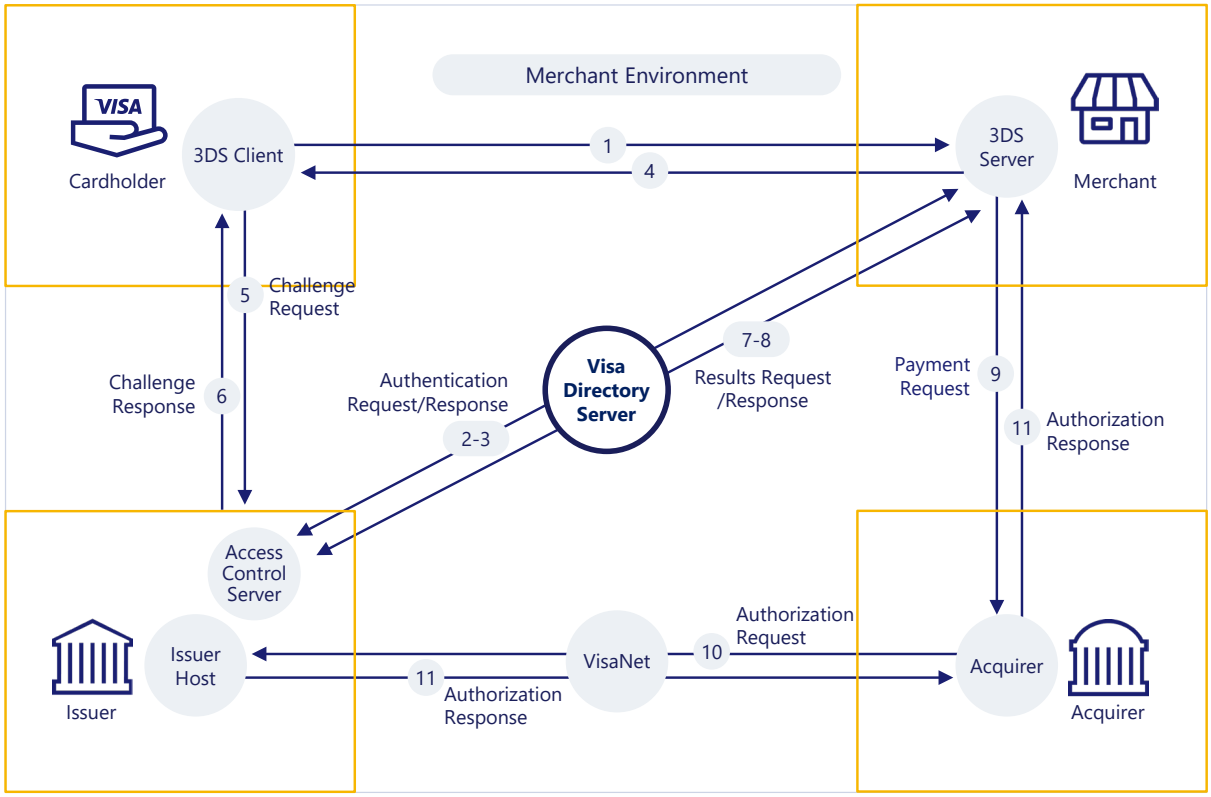
For a more comprehensive definition of EMV 3DS terms please refer to the EMV 3-D Secure Protocol and Core Functions Specification Version 2.2 Table 1.3.

3.3.5 The EMV 3DS messages and process flow

EMV 3DS enables merchants to send a message to an Issuer to carry out the authentication process.

The environment and basic message flow that comprises EMV 3DS and underpins both the frictionless and challenge flows is summarized in Figure 6. Familiarity with this will help readers understand the concepts around application of EMV 3DS, discussed in this guide.

Figure 6: The EMV 3DS secure environment and message flows



EMV 3DS supports two primary authentication flows:

- Frictionless Flow: occurs when the Issuer authenticates the cardholder without cardholder involvement by evaluating the transaction's risk level using Risk Based Authentication (RBA)
- Challenge Flow: occurs when the Issuer assesses the risk of the transaction during the frictionless flow and determines that the transaction requires additional cardholder authentication through application of a SCA challenge

How the 3DS authentication process works:

- Step 1: The cardholder initiates the transaction
- Step 2: The merchant's 3DS Server initiates an authentication request by sending an Authentication request (AReq) message via the Visa Directory Server to the Issuer's ACS. This message contains all the data elements that the Issuer requires to risk assess the transaction. It may also contain indicators requesting that an exemption is applied
- Step 3: The Issuer's ACS undertakes a risk-based assessment of the transaction using the data elements provided and determines whether the transaction is out of scope/an exemption can be applied or an SCA challenge is required. The ACS responds via the DS to the 3DS Server with an Authentication Response (ARes) message advising that either the cardholder is authenticated, or further cardholder authentication is required

- Step 4: If further authentication is required, a SCA challenge is triggered, and the cardholder provides additional information
- Step 5: A Challenge Request (CReq) message is sent between the 3DS SDK or 3DS server and the ACS with the additional authentication information provided by the cardholder
- Step 6: A Challenge Response (CRes) message is sent by the ACS in response to the CReq message indicating the result of the cardholder authentication
- Step 7: Results Request Message (RReq) is sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server
- Step 8: A Results Response Message (RRes) is sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message
- Step 9: If the cardholder is successfully authenticated, the merchant sends a payment request to the Acquirer, along with the ECI and CAVV
- Step 10: The Acquirer sends an authorization request to the Issuer which is provided along with the ECI and CAVV
- Step 11: The Issuer responds via the Acquirer with the authorization response (approve or decline)

Steps 5 to 8 are only required if a SCA challenge is required.

Note, while the Issuer's ACS will respond to Authentication requests on behalf of the Issuer, the Issuer will set the rules and policies applied by the ACS and the ACS may refer some transactions to the Issuer for review. The Issuer may also manage the application of an SCA challenge such as an SMS OTP or push message to a mobile banking app, where this is required.

For more detail on the messages, refer to the Visa Merchant/Acquirer and Issuer Implementation Guides for Visa's EMV 3DS Program.

3.3.6 Visa Authentication Data

Visa Authentication Data is used to communicate information about authentication between the Issuer ACS, the merchant, VisaNet, and the Issuer Host. Table 10 provides full details:

Table 10: Visa authentication elements

Data Elements	Created by	Purpose
Electronic Commerce Indicator (ECI)	Issuer ACS, or Visa's Attempts Server	Indicates the level of authentication that was performed on the transaction. The ECI value is passed to the merchant and included by the merchant in the authorization request.
Cardholder Authentication Verification Value (CAVV)	Issuer ACS, or Visa's Attempts Server	Unique cryptogram generated for each 3DS authenticated transaction and linked to the transaction amount and payee. The CAVV is passed to the merchant and submitted with the authorization request to prove authentication has occurred.
CAVV Results Code (Field 44.13)	Issuer or VisaNet	Communicates the results of the CAVV verification performed during authorization (e.g. PASS/FAIL) and indicates if the CAVV was created by the Issuer's ACS, the Issuer's Attempts Server, or Visa's Attempts Service.
3-D Secure Indicator (Field 126.20)	VisaNet	Optional field that the Issuer or Acquirer can choose to receive in authorization. Communicates the EMV 3DS version number and the EMV 3DS authentication method used to authenticate the cardholder. This can be used to improve risk assessment in authorization processing, reporting and analytics etc.

For more details on these data fields please refer to the *Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure*.

3.3.7 Risk Based Authentication

3.3.7.1 Introduction to RBA

Risk Based Authentication (RBA) is a process used to risk assess and score 3DS transactions, helping to reduce the volumes that require SCA.

It enables Issuers and Acquirers to apply the TRA exemption to remote transactions (where their fraud rate is below the relevant PSD2 reference fraud rate threshold and they meet the other requirements of the TRA exemption).

RBA allows Issuers to risk assess any authentication request, whether it has an Acquirer exemption indicator or not. The outcome may result in frictionless, challenge or failed authentication. As a result, RBA can help Issuers to:

1. Optimise cardholder experience
2. Increase approvals
3. Reduce false declines
4. Balance fraud control objectives

Visa considers RBA to be critical to reducing unnecessary challenges and friction and Issuers globally are required to support it.

Key Point

The Difference between RBA and the TRA exemption:

- RBA is a process applied as part of the EMV 3DS flow to risk assess all transactions submitted for authentication. The Acquirer may use RBA to decide whether to request application of the TRA exemption. The Issuer, or its ACS, uses the RBA risk assessment to decide whether the risk is sufficiently high that an SCA challenge needs to be applied regardless of whether the transaction may otherwise qualify for one of the SCA exemptions; or whether the risk is low enough that a qualifying exemption may be applied.
- The TRA exemption is one of the four Visa supported SCA exemptions. It may be applied by the Issuer or Acquirer based on a compliant RBA based transaction risk assessment so long as the PSP applying the exemption has a fraud rate within the defined threshold for the value of the transaction. The risk assessment may be undertaken by the Issuer or its ACS provider; the Acquirer, or the merchant on behalf of the Acquirer,

RBA uses transaction data to assess fraud risk without the need for the cardholder to complete an SCA challenge. RBA is an integral element of EMV 3DS and enables "frictionless" authentication of low risk transactions. The EMV 3DS specification defines many data elements that can be included in the initial authentication request (AReq) message and used by the Issuer's ACS fraud engine to assess each transaction with a high degree of confidence. For the latest version of data elements and their requirement please refer to the latest version of the *Visa Secure Program Guide*. The elements are fully defined in the EMVCo specification: EMV 3-D Secure Protocol and Core Functions Specification.

Where transaction risk is assessed as low, and the Issuer's fraud rate is within the reference fraud rate for the transaction value, the Issuer may apply the TRA exemption to a remote transaction without the need to apply a challenge. Where the risk is not assessed as low, the Issuer's fraud rate is outside the reference fraud rate, or the other requirements of the TRA exemption are not met, a challenge will need to be completed. In some cases, Issuers will need to apply an SCA challenge to the authentication request regardless of fraud risk and TRA considerations. For example where a new MIT mandate is being established.

3.3.7.2 Benefits of RBA

Risk Based Authentication has already delivered significant benefits in the markets where it has been deployed. In the UK in the pre-PSD2 environment, 95% of transactions that undergo a risk-based assessment have not required additional customer authentication. Since the introduction of a risk-based approach there has been a 70% reduction in abandonment rates. At the same time, fraud rates have fallen, indicating that risk-based assessments are an effective tool to detect and prevent fraud. The use of a significantly greater number of risk scoring data points under EMV 3DS will increase the effectiveness of RBA even further. Visa analysis shows that the addition of just one of those data points – device ID information – can make a significant improvement to fraud detection rates. In cases where it is necessary to apply SCA, this further strengthens the effectiveness of the authentication process by targeting friction at higher risk transactions.

3.3.8 Data elements

EMV 3DS also requires that merchants submit additional transaction data with the authentication request message. This data is used by Issuer's ACS providers to analyse the risk of the transaction and can reduce the number of transactions for which SCA is applied. It is critical that this data is correctly formatted, consistent and of high quality in order to avoid Issuers having to apply SCA just because they have insufficient data to risk assess a transaction.

The Data Element Types supported with EMV 3DS include those listed in Table 11 below:

Table 11: Example data types

Category	Example
Transaction & Checkout Page Information	• Cardholder Information (e.g. account number, billing/ shipping address) • Merchant Information (e.g., name, URL, ID, merchant country, MCC) • Transaction Information (e.g., dollar amount, transaction type, recurring/installment) • Device Information (e.g., browsers width, height, country, device channel: app-based browser)
Authentication Information	• 3DS Requestor Authentication method, date, time (i.e. cardholder "logged in" as guest or cardholder logged into merchant account)
Prior Authentication Information	• Prior Authentication method, time and date
Merchant Risk Indicator	• Pre-order indicator • Gift card amount, currency, count • Shipping & delivery information
Cardholder Account Information	• Cardholder account age, date, change • Password change

Category	Example
Device Information	• Platform Type • Device Model • Browser/SDK

Merchants should pay particular attention to the Browser IP, Shipping Address Postal code, Billing Address Postal code, and Address match indicator as key fields. However, in general, the more quality data that the merchant is able to supply over time (regardless of if it is optional or required), the more it can assist in the risk analysis of the transaction.

A further critical factor in the gathering of data is the use of the 3DS Method URL. If a 3DS Method URL is specified, then merchants must use this for the appropriate flows.

Requirement

Merchants are required to submit the required data elements in the EMV 3DS authentication request message. Provision of this data allows issuers to make optimum risk decisions and minimises unnecessary applications of SCA.

Visa has introduced a rule to ensure that minimum data provision standards are applied. For the latest version of data elements and their requirement refer to the latest version of the *Visa Secure Program Guide*. Further information can also be found in *Visa Secure Using EMV 3DS Best Practices for Merchants* and *Minimum Data Requirements for Merchants* on Visa Online.

3.3.9 Token transactions and EMV 3DS

EMV 3DS authentication is supported for card on file, e-commerce, and application-initiated e-commerce transactions using network tokens. This uses two separate cryptograms in the authorization message, the TAVV token cryptogram for token validation, and the EMV 3DS CAVV cryptogram for cardholder authentication. Visa requires that Acquirers submit both the TAVV token cryptogram and EMV 3DS CAVV cardholder authentication cryptogram in authorization requests for token-based transactions with EMV 3DS.[33]

Acquirers that participate in Visa Token Service (VTS) and EMV 3DS are required to support the TAVV cryptogram data in Field 126.8—Transaction ID (XID) in combination with the EMV 3DS CAVV cryptogram data in Field 126.9—Usage 3: 3-D Secure CAVV, Revised Format for token-based transactions with EMV 3DS.

[33] It is possible for some token-based transactions not to go via EMV 3DS to meet PSD2 SCA obligations. Refer to section 5.1.1 for more details.

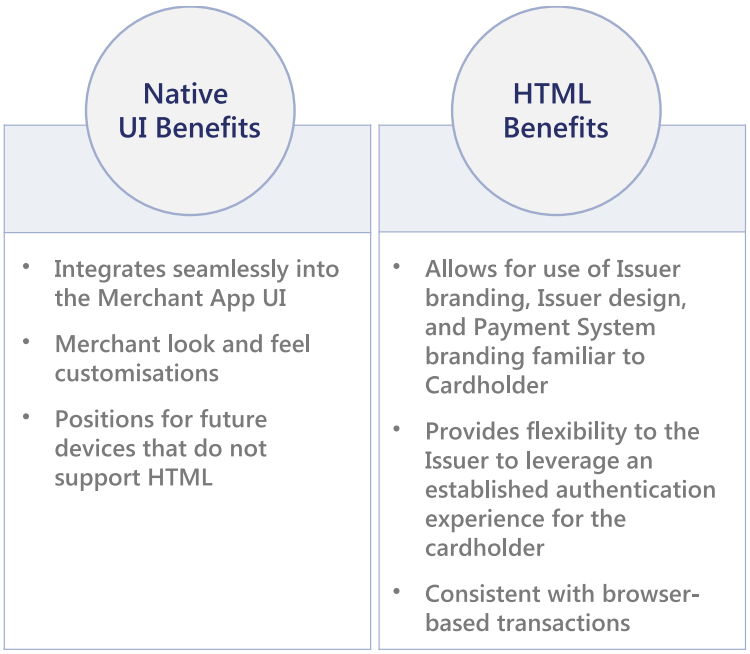
3.3.10 UX considerations

EMV 3DS provides significantly enhanced user experiences through:

- Enhanced support of mobile devices and native app environments
- Use of RBA to reduce unnecessary challenges
- Lower friction challenge methods including biometrics
- Challenge flows that are better integrated into the checkout flow with options for merchant branding of some elements

Consumer research carried out by EMVCo has shown that the presence of network and bank logos conveys more clearly to the cardholder the trusted party performing authentication. Furthermore, the standard offers the flexibility to offer two options for in-app: 1) native UI 2) HTML, more details are given in Figure 7.

Figure 7: Relative benefits of native UI v HTML



It should be noted that while the merchant has the option to brand aspects of the native UI and customize the wording of the header, the content of the challenge messages is determined by the Issuer and served by the Issuer's ACS. For more information please refer to the EMV 3DS UX Guidelines available on the Visa Developer Center[34] and the EMVCo EMV® 3-D Secure UI/UX Design Guidelines[35].

[34] https://developer.visa.com/pages/visa-3d-secure#introduction

[35] https://3ds-ux-guidelines.emvco.com/

3.3.11 EMV 3DS on different platforms

EMV 3DS supports desktop browser and mobile platforms with both HTML and native app interfaces as well as games consoles, allowing seamless support of in-game purchases. Issuers should ensure that testing of EMV 3DS transactions takes place on a broad set of devices (TVs, consoles, tablets, mobiles etc.) in order to ensure a consistent and successful cardholder experience.

3.3.12 Supporting the latest version of EMV 3DS

Support for 3DS 1.0 was withdrawn on 15 October 2022[36] and all merchants and Issuers must now support EMV 3DS.

Merchants should always aim to use the highest version of 3DS supported by the Issuer.

Merchants supporting EMV 3DS can determine which version of EMV 3DS an Issuer supports. Their 3DS Server Provider can request an update, called a Preparation Request (PReq) message, from the Visa Directory Server for the latest list of BINs and account ranges that are supported by the different EMV 3DS protocol versions. 3DS Server Providers should utilize this protocol version information to package messages accordingly and send to appropriate 3DS Directory Server as illustrated below.

In order to obtain optimal authentication performance, merchants should be using the daily Preparation Request (PReq) / Preparation Response (PRes) message in EMV 3DS to ascertain which version of EMV 3DS each Issuer is enabled on.

Merchants must use EMV 3DS in order to benefit from fraud liability protection.

For more information on the Visa Attempts Server see Section 4.9.1.

Best Practice

Merchants are strongly advised to send authentication requests to the highest version of 3DS supported by the Issuer. This enables issuers to properly risk assess each transaction. 3DS Server providers receive up to date protocol information to enable transactions to be routed to the correct DS.

3.3.13 EMV 3DS Testing

Ecosystem participants are reminded to ensure adequate testing and validation occurs prior to going live with any new EMV 3DS version. In addition to this, vendors should ensure that retesting obligations are met to ensure that products remain certified with both EMVCo and Visa.

Issuers and merchants must ensure that their ACS and 3DS Service vendors respectively have completed the full Visa product certification testing (vendor certification) for the version of EMV 3DS protocol they wish to process on and can support additional SCA use-cases to enable

[36] See VBN Article ID AI12044 *Reminder: Visa Will Discontinue Support for 3DS 1.0.2 Global* June 2022

compliant implementations for: optimized payment flows, customer experience and approval rates. This is also valid when they want to start supporting new functionality that is optional, for example the trusted beneficiaries exemption.

Issuers are reminded that Visa cannot accept project requests unless your ACS vendor has completed their full vendor testing and certification for all mandatory test cases.

Issuers and merchants should work with their ACS and 3DS vendors respectively to establish testing capabilities and a test plan to validate their processing for each version of the protocol you are enabling, this should include:

- Validation of EMV 3DS authentication message processing in all authentication flows including frictionless, challenge, exemptions, and errors
- Validation of the user experience and screen rendering
- Validation of latency and abandonment

To further assist ecosystem participants' enablement prior to go-live, Visa is making available testing facilities for participants. For more information about these facilities please contact your Visa Representative.

3.4 Visa's PSD2 solutions using Visa Token Service (VTS)

Clients can use the Visa Token Service (VTS) and its capabilities to help meet their SCA obligations. This section briefly describes the solution and the features it offers.

3.4.1 The Visa Token Service (VTS)

VTS is a technology from Visa which replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token. The token may be issued with domain controls which limit its use to the merchant, channel or consumer device to which it was issued.

Visa Tokenization helps reduce fraud and improve card authorization rates. VTS offers a robust platform with additional value-add services & features to enhance the payment flow throughout the ecosystem. It provides a complete integrated set of tokenization tools and capabilities for merchants, Token Requestors[37], Issuers, Acquirers and processors.

VTS can help address the requirements of PSD2 through:

- Maximizing the ability of PSPs to apply the TRA exemption
- Facilitating the application of SCA between customers and qualifying participants in the Visa Delegated Authentication Program (see Section 3.6 below)
- Supporting dynamic linking through the token cryptogram

3.4.2 The Visa Cloud Token Framework

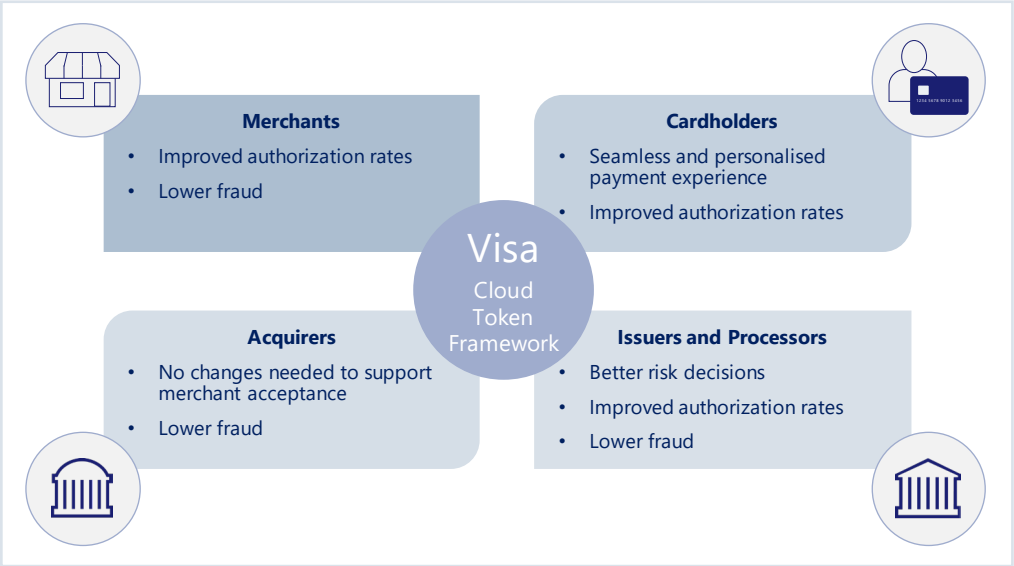
The Cloud Token Framework is a global framework which brings the advantages of device-based tokens and applies them to e-commerce and card-on-file tokens. With the features of

[37] Token Requestors are entities that request payment tokens for end-users, for example digital wallet providers, payment enablers or merchants.

device binding and cardholder verification, CTF results in a better quality credential as well as providing greater certainty and confidence for the payment ecosystem.

As with EMV 3DS, the Cloud Token Framework delivers important benefits to all stakeholders. These are summarized in Figure 8 below:

Figure 8: Cloud Token Framework benefits



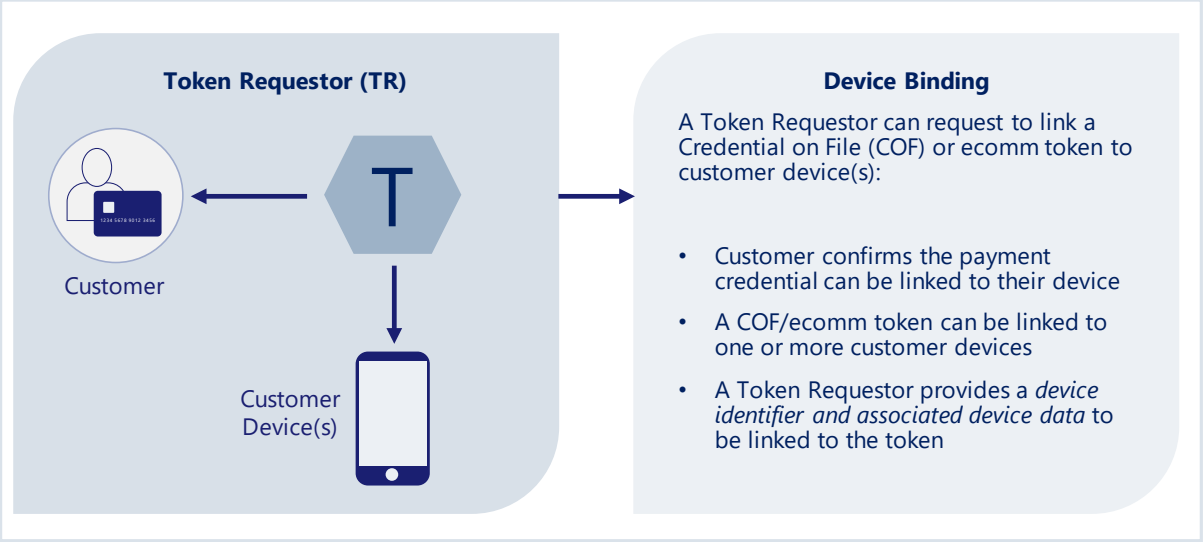
3.4.2.1 Features of the Cloud Token Framework

Device Binding and Cardholder verification are two key features of the Cloud Token Framework. The below sections describe these features, as well as other functions and benefits, in further detail.

3.4.2.1.1 Device Binding

Device binding enables e-commerce and/or card-on-file tokens which are provisioned to the consumer's account to be bound to multiple trusted devices.

Figure 9: Principles of Device Binding



The Device Binding process verifies that the Issuer's cardholder has possession of the device on which the token is being used or provisioned. It is done through performing Issuer authentication and may occur during token provisioning or as a standalone action initiated by a Token Requestor after token provisioning has occurred. The Token Requestor sends the request to VTS to bind the device, passing the data that it has gathered from the device and requesting that the device is bound to the token credential that has been previously issued. If the bound token is subsequently to be used as a possession factor for SCA, the Issuer must perform SCA in order to verify the customer before the binding of the device to the token is finalized.

3.4.2.1.2 Token Requestor-initiated cardholder verification

This allows the Token Requestor to request cardholder verification to be applied for any already provisioned e-commerce or credential on file token. Token Requestors may request cardholder verification at any time, whether or not a device binding request has been performed, to explicitly establish that the Token Requestor's customer is the Issuer's cardholder. If the verification is used to enable subsequent delegated authentication to the token requestor, then the cardholder verification performed should meet SCA requirements.

3.4.2.1.3 The Role of tokenization in the Visa Delegated Authentication Program

The CTF can be used when an Issuer elects to use the Visa Delegated Authentication Program. Initial e-commerce use cases for delegated authentication facilitated by token transactions include:

- In-app transactions,
- E-commerce transactions from Token Requestors
- E-commerce transactions using EMV 3DS

Specifically CTF:

Enables qualifying participants to provide information to Issuers on the authentication method applied at the time of the transaction. The factors used are sent in the payment transactions via field F123, Dataset id 68 tags 83 and 84.

- Caters for dynamic linking requirements through the use of a token-based cryptogram (TAVV). The TAVV supports linking of the transaction to the merchant

(payee) and the transaction amount using an encrypted, verifiable authentication code

- Provides Issuers with the ability to configure specific qualifying merchants and Token Requestors they agree to accept as qualifying participants under the Visa Delegated Authentication Program

Table 12 below summarises key fields for Visa Delegated Authentication for token transactions and dynamic linking and provides token-specific notes

Table 12: System Fields for Visa Delegated Authentication

Field	Tag Position/Field Value	Sent from Acquirer?	Sent to Issuer?	Token-Specific Information
F34	Dataset 4A, Tag 8A—Delegated Authentication	Yes	Yes (conditionally)	• For token transactions, Acquirers do not have to set this field. Visa Token Service (VTS) will extract the delegated authentication indicator from the transaction cryptogram (Token Authentication Verification Value [TAVV]) and set this value in F34 when sending to the Issuer. • VTS will ignore the Acquirer-populated value for this field; instead, this value is set by VTS based on the TAVV. Note: For device-based proximity payment token transactions, the DA indicator will not be set in Field 34.
F126.5	Visa Merchant Identifier (VMID) (It is optional for Issuers to receive this field.)	Yes	Yes	• For EMV 3DS token transactions, this field identifies the delegate.[38] • For non-EMV 3DS token transactions, the token requestor will act as the delegate and is identified by the Token Requestor ID (TRID). The VMID is not relevant in this case. Note: For non-EMV 3DS token transactions, Acquirers do not have to set this field. If this field is provided by the Acquirer, Visa will send it to the Issuer (i.e., Visa will not drop this field).
F126.8	If CAVV and TAVV are present, then TAVV data is in this field. If only the TAVV is			• For non-EMV 3DS token transactions, the TAVV will contain delegation intent set by the token

[38] For token transactions with EMV 3DS, delegated authentication transactions will be processed based on processing rules in Article 9.1.2 of the October 2019 Global Technical Letter.

Field	Tag Position/Field Value	Sent from Acquirer?	Sent to Issuer?	Token-Specific Information
	present, then the Acquirer can populate this field or Field 126.9.	Yes	Optional if TAVV	requestor. Visa will dynamically set the delegated authentication indicator in F34 based on the TAVV.
F123	Dataset ID 68: • Tag 81—Token User Identifier • Tag 83—Token Authentication Factor A • Tag 84—Token Authentication Factor B • Tag 85—Token Authentication Amount	No	Yes	• These values will be set in F123 based on the incoming TAVV. • Token Authentication Factors A and B are set by the delegate to inform the Issuer how SCA was performed. • Token User Identifier (payee identifier) and Token Authentication Amount are provided for PSD2 dynamic linking purposes. • Refer to Article 3.3—*Changes to the Visa Token Service to Support Cloud Token Framework* in the October 2019 Global Technical Letter for further details.

Note: Token transactions will require a TAVV unless they are merchant-initiated transactions (MITs). MITs are out of scope for SCA; therefore, delegated authentication does not apply. The above table does not include situations where the TAVV is not present.

For more information on use of the CTF to support delegated authentication, please refer to Visa Business News: Authentication of Token Transactions with Visa Delegated Authentication 29 August 2019.

For more information on the Visa Delegated Authentication Program see section 3.6 below, the *Visa Delegated Authentication Program Implementation Gui*de and *Article 9.1.2 in Oct 2019 GTLIG*.

3.4.2.1.4 The role of The Cloud Token Framework in Optimising application of the TRA exemption

As the CTF provides a lower risk credential than using a PAN, it may facilitate lower overall fraud rates, providing stakeholders with an opportunity to maximise their use of the TRA exemption. Furthermore each individual transaction facilitated with a cloud token has a greater likelihood of being assessed as lower risk and is therefore more likely to qualify for the TRA exemption.

3.5 Visa Rules & policies for authentication & authorization

3.5.1 Visa Rules relevant to authentication and authorization

A number of existing and new Visa Rules govern the application of SCA. These rules define some specific requirements that Issuers, Acquirers and merchants must comply with when applying or requesting authentication and authorization. The rules aim to ensure:

- That transactions are correctly identified in the authentication and authorization process flows according to whether and how SCA should be applied
- That transactions are not incorrectly authorized or unnecessarily declined due to:
  - Issuers, Acquirers or merchants responding incorrectly to relevant indicators
  - Legitimate exemptions not being recognized
- That transactions that are out of scope of the SCA regulation or otherwise do not require an Issuer to apply SCA are recognized
- That Issuers are encouraged to balance risk management with the minimization of friction

These rules which include support of exemption and out of scope indicators in authorization messages and minimum standards for authentication abandonment, the need for Issuers to apply challenges when requested by a merchant, risk analysis technology, the application of biometrics and minimum data requirements, will all contribute to a smoother authentication experience and lower fraud rates.

Relevant rules are included in *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements*.

3.5.2 Visa EMV 3DS Performance Program

All parties in the ecosystem are required to adhere to the strict requirements detailed in the Visa document *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements* and Visa has implemented a performance program to actively monitor key performance metrics and ensure transaction approval rates are maintained at the highest level. Further information on metrics that Visa will track under the program and the commencement dates for the performance program are detailed in the document referred to above. Issuers and Acquirers are reminded to familiarize themselves with that document and other Visa SCA publications to ensure they are compliant and providing the best level of service to consumers.

Visa will update these requirements from time to time and reserves the right to determine the application of any given requirement, as applicable.

3.6 Visa Delegated Authentication Program

3.6.1 Introduction to the Visa Delegated Authentication Program

Visa's Delegated Authentication Program (VDAP) provides an overarching framework for Issuers to utilise device-based authentication for SCA. It includes a comprehensive set of rules that enables Issuers, merchants, Acquirers and technology providers to work together to enable a smooth authentication process for authentication in line with PSD2 requirements. The

program is designed to facilitate that Issuers have the control and information they require to satisfy themselves that the regulatory requirements can be met, whilst enabling merchants and digital wallets ("the participants") to enable near-frictionless transactions for consumers. The participants are required to support authentication using advanced technology standards and/or a framework such as FIDO or CTF.

3.6.2 Benefits

The Visa Delegated Authentication Program is designed to support the needs of all stakeholders in the ecosystem. Merchants and digital wallets who have invested in qualifying for the program, including having the capability to apply device-based authentication, are able to deliver a consistent consumer payment experience when SCA is required.

Issuers can benefit from potential higher sales conversions with minimal incremental investment. Visa manages the program and provides the Issuer oversight and supervision so that SCA can be performed, and Issuers are capable of meeting their regulatory and risk requirements. Fraud is strictly and consistently managed within the program.

A key component of the program is the concept of verification of Issuer-trusted cardholder devices. Issuers can utilise cardholder-trusted devices in order to meet their SCA requirements whilst benefiting from seamless consumer purchase experiences.

3.6.3 Components of the Program

There are four key components to the Visa Delegated Authentication Program:

1. **Rules and Fraud Liability Framework**: The Visa Rules and the *Visa Delegated Authentication Implementation Guide* provide the framework for Issuers to perform SCA with the support of participants; Visa specifies program participant qualification criteria. Issuers should familiarize themselves with the Program, its alignment to their internal policies, and identify any steps they should take before the Program commences. Issuers are automatically enrolled in the Program but various opt out options are available.
2. **Program Qualification**: Acquirers wishing to participate must meet the qualification criteria either through working with an existing compliant provider or through the development of a compliant solution and presentation to Visa of a Readiness Questionnaire. Token requestors may submit their Readiness Questionnaire directly to Visa.
3. **Transaction Identification**: On a per transaction basis, the participants will indicate to the Issuer that SCA was performed through EMV 3DS (2.2 only) or VTS.
4. **Program Compliance:** Issuers and Acquirers are required to maintain fraud and risk monitoring and Issuers may request additional SCA or decline if a serious risk is identified. Participants are required to meet fraud performance requirements upon entry and on an ongoing basis and are required to apply SCA based on applicable regulatory requirements. Note: Visa does not certify compliance with any applicable regulatory requirements.

The Visa Delegated Authentication Program provides participants with the opportunity to use either EMV 3DS or VTS.

For more details, including technical use cases, Program qualification criteria and participant enrollment processes, please refer to the *Visa Delegated Authentication Program Implementation Guide*.

3.7 Visa Pre-dispute products

3.7.1 The benefits of reducing fraud rates attributable to unrecognized transactions and first party fraud

Disputes are often marked as fraud even when they are raised only because customers have trouble recognizing transactions and not because the transaction was unauthorised. Visa analysis indicates that fraud is reported 90% of the time a dispute is submitted.

Such disputes can artificially and unnecessarily inflate fraud counts, limiting the ability of Acquirers and Issuers to apply the TRA exemption and potentially limiting the ability of individual merchants to be considered for the application of certain exemptions.

Visa's experience has shown that a significant proportion of both disputes and transactions unnecessarily categorised as fraudulent can be avoided if customers and Issuers can be provided with additional information, such as the item purchased, to help customers validate transactions before they formally ask for a transaction to be disputed.

If merchants provide this information to Issuers, it enables them to deal more effectively with customer queries, improving customer satisfaction and removing these transactions from the fraud count. This can potentially improve the risk score of every transaction a merchant processes, while increasing the ability of Acquirers and Issuers to apply the TRA exemption. Merchants can also benefit by reducing revenue losses from disputes, as well as increasing their ability to qualify for the application of key exemptions.

Verifi, a Visa company, offers a suite of related Pre-dispute Products to help both merchants and Issuers avoid and resolve such disputes.

3.7.2 Introduction to Verifi pre-dispute services

Verifi pre-dispute solutions provide an opportunity for merchants, Acquirers and Issuers to collaborate and share data to prevent and resolve disputes at the pre-dispute stage.

3.7.2.1 Verifi Order Insight

Verifi's Order Insight® (formerly Visa Merchant Purchase Inquiry) allows merchants to share order details with Issuers through the existing Visa Resolve Online (VROL) dispute process. Enhanced transaction data is provided by merchants to Issuers for review with cardholders at first inquiry.

An overview of the Verifi Order Insight process is shown in Figure 10 below:

All Visa Issuers have real-time access to enhanced transaction details from enrolled merchants through VROL. In order to benefit directly, merchants need to enroll directly or via their Acquirer or payment facilitator.

3.7.2.2 Order Insight Digital

Order Insight Digital (formerly Visa Cardholder Purchase Inquiry) enables cardholders to access the same enhanced transaction data through an Issuer's online banking portal or mobile app.

Validating the sale with the cardholder can help prevent a dispute from being raised. Global Visa Issuers are required to receive transaction data in VROL from participating merchants before submitting a dispute.

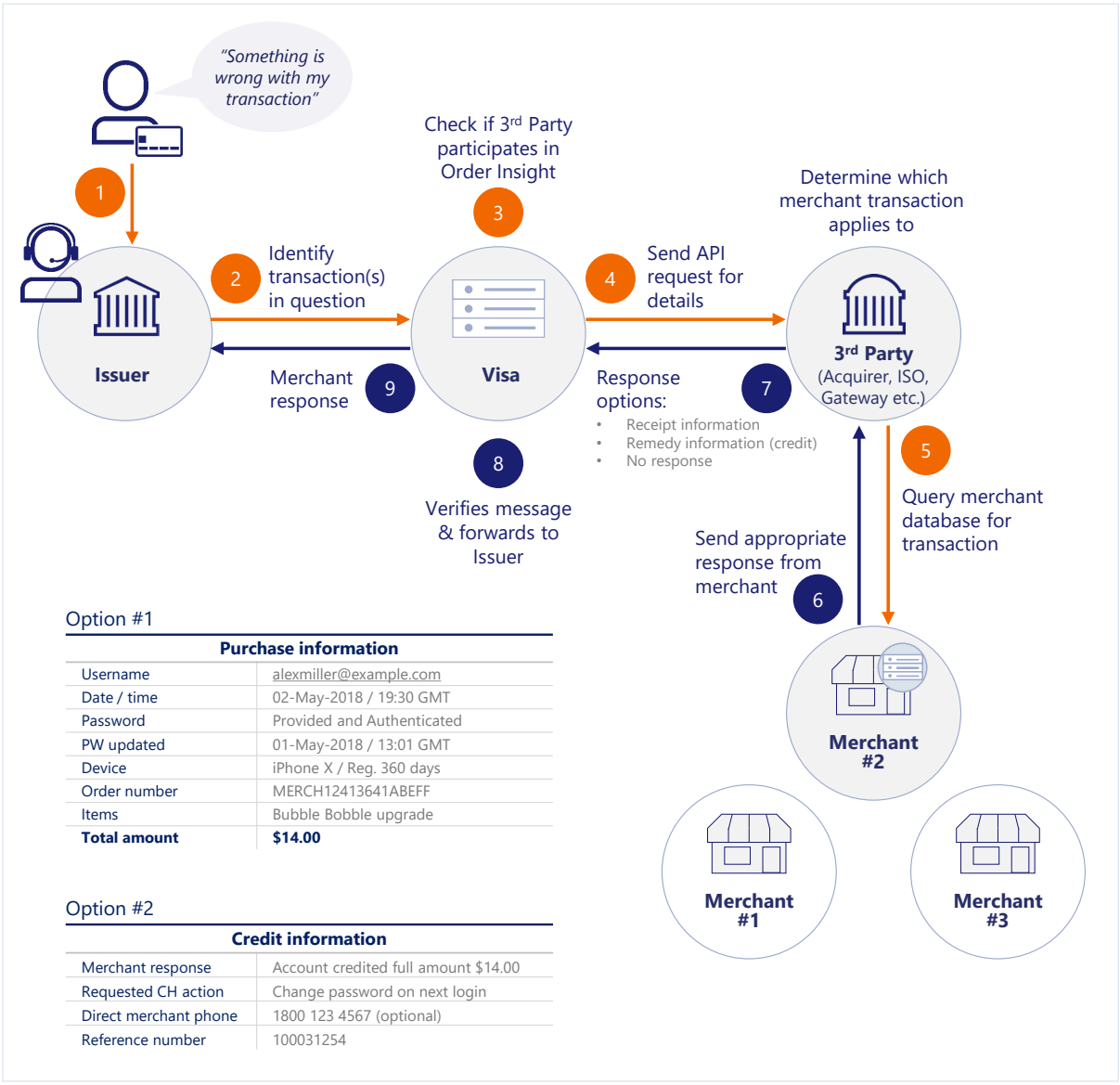
3.7.2.3 Rapid Dispute Resolution

Rapid Dispute Resolution (RDR) operates at the pre-dispute stage to resolve disputes before they escalate, as determined by seller-defined rules in the Verifi automated decisioning engine. Pre-disputes from other card brands can also be resolved through Verifi.

3.7.3 Accessing Verifi pre-dispute services

All Verifi services are available through VROL for Issuers, or through enrolment directly with Verifi for merchants. Interested parties should contact Verifi (info@verifi.com), or speak to their Visa representative. Small to medium Merchants should speak to their Acquirer about availability of these services.

Figure 10: The Order Insight process flow



Option #1

Purchase information	
Username	alexmiller@example.com
Date / time	02-May-2018 / 19:30 GMT
Password	Provided and Authenticated
PW updated	01-May-2018 / 13:01 GMT
Device	iPhone X / Reg. 360 days
Order number	MERCH12413641ABEFF
Items	Bubble Bobble upgrade
Total amount	**$14.00**

Option #2

Credit information	
Merchant response	Account credited full amount $14.00
Requested CH action	Change password on next login
Direct merchant phone	1800 123 4567 (optional)
Reference number	100031254

3.8 The Visa MIT Framework

3.8.1 Introduction to the MIT Framework

3.8.1.1 The requirement to use the MIT Framework in the context of SCA

The Visa MIT Framework enables Acquirers and Issuers to correctly indicate and identify MIT transactions.

Requirement

Merchants must use the MIT framework for any MITs if they want those transactions to be recognized as out of scope of SCA.

The Visa MIT framework was first introduced in 2016 and is a global standard to identify MITs, which, as payee initiated transactions, are out of scope of the PSD2 regulation.

The Visa MIT framework had not previously been mandated to be used by merchants for PAN based transactions[39] (it is mandated for token-based transactions). However, in the SCA context, if the framework is not used, the Issuer will not be able to recognize an MIT as out of scope of SCA and may unnecessarily decline, requesting SCA even though the cardholder is not available. To avoid this experience, the MIT Framework needs to be implemented across the ecosystem for all MITs, PAN or token based. As a result, Visa has mandated its use by merchants acquired in the EEA and the UK for PAN based MITs from 14 April 2023 to facilitate meeting SCA requirements.

3.8.1.2 Types of MITs defined within the Visa MIT Framework

The Visa MIT framework defines eight distinct types of MITs as summarized in Table 13 below and identifies each of these using two distinct identifiers:

- **Transaction type**: Located in Field 126.13 (POS Environment Code Field) or Field 63.3 (Message Reason Code Field), depending on the transaction intent of the MIT.
- **Transaction identifier (Tran ID) of the initial CIT**[40]: Located in Field 125, Usage 2, Dataset ID 03

For more details see Table 14 below.

[39] Not mandated by Visa for merchants to use for PAN based transaction, however all Acquirers were mandated to be ready to support it since October 2017 for all transactions (PAN and token) and all Issuers were mandated to be ready to receive MIT indicators since 2016 for all PAN and token based transactions.

[40] Or of the previous MIT in some cases as indicated in Table 14.

Table 13: Types of MIT defined in the Visa MIT Framework

MIT Types	Description
Installment/Prepayment	Installment payments describe a single purchase of goods or services billed to a cardholder in multiple transactions over a period of time agreed by the cardholder and merchant. Prepayment is one or many payment(s) towards a future purchase of goods/services.
Recurring	Transactions processed at fixed, regular intervals not to exceed one year between Transactions, representing an agreement between a cardholder and a merchant to purchase goods or services provided over a period of time. Note that a recurring MIT transaction is initiated by the merchant (payee) not the customer (payer) and so is out of scope of PSD2. Recurring transactions that are in scope of PSD2 (and therefore may benefit from the recurring transaction exemption) are those that are customer (payer) initiates, e.g. standing orders set up from a bank account.
Unscheduled Credential on File (UCOF)	A transaction using a stored credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date, where the cardholder has provided consent for the merchant to initiate one or more future transactions which are not initiated by the cardholder. This transaction type is based on an agreement with the cardholder and is not to be confused with cardholder initiated transactions performed with stored credentials (CITs are in scope of PSD2 whereas UCOF transactions are MITs and thus out of scope).
Incremental	An incremental authorization is typically found in hotel and car rental payment scenarios, where the cardholder has agreed to pay for any service incurred during the duration of the contract. An incremental authorization can also be used in Europe to authorize any additional amount above the authenticated amount when the price of merchandise or services, including shipping costs and applicable taxes has changed, so long as the cardholder has entered an agreement in advance to pay the additional amount.
Delayed Charges	A delayed charge is typically used in hotel, cruise lines and vehicle rental payment scenarios to perform a supplemental account charge after original services are rendered.
No Show	A No-show is a transaction where the merchant is enabled to charge for services which the cardholder entered into an agreement to purchase but did not meet the terms of the agreement.
Reauthorization	A Reauthorization is a purchase made after the original purchase and can reflect a number of specific conditions. Common scenarios include delayed/split shipments and extended stays/rentals.
Resubmission	This is an event that occurs when the original purchase occurred, but the merchant was not able to get authorization at the time the goods or services were provided. This is only applicable to contactless transit transactions.

Table 14: Key data fields of the Visa MIT Framework

MIT TYPE Description	Visa MIT Framework		
	POS environment (F126.13)	Message Reason Code (F63.3)	Transaction ID (F125[41])
Installment/Prepayment	I	--	Tran ID of first transaction (CIT)/ previous MIT
Recurring	R	--	Tran ID of first transaction (CIT)/ previous MIT
Unscheduled Credential on File (UCOF)	C	--	Tran ID of first transaction (CIT)/ previous MIT
Incremental	--	3900	Tran ID of first transaction (CIT)
Delayed Charges	--	3902	Tran ID of first transaction (CIT)
No Show	--	3904	Tran ID of first transaction (CIT)
Reauthorization	--	3903	Tran ID of first transaction
Resubmission	--	3901	Tran ID of first transaction

3.8.1.3 MITs qualifying as out of scope of SCA

An MIT is a transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval, governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder.

It is the Acquirer's responsibility to ensure that transactions indicated as MITs meet all the requirements in this section. In the EEA and the UK, a merchant can only submit a transaction indicated as an MIT with the Visa MIT Framework if the transaction meets all of the requirements of an MIT as defined in this section, including:

[41] Acquirers may submit the Original Transaction Identifier either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Transaction Identifier in Field 125 to the Issuers that participate to receive Field 125.

- The cardholder must not be available to (I) initiate; or (II) authenticate the transaction. If the cardholder is available to do either of those things, then the transaction is not an MIT.
    - Whether the transaction is processed at that exact moment or later in time is irrelevant. If a consumer is available to initiate or authenticate when they are physically present at the merchant's point of sale or, in the case of a remote payment, interacting with the merchant's webpage or app, this cannot be considered an MIT even if the payment triggered by this interaction is processed at a later time.
- SCA must be applied (exemptions cannot be used) to the initial Customer Initiated Transaction (CIT) used to establish the agreement for future MITs. This applies if the agreement was set up through a remote channel[42], unless the initial CIT:
    - Was performed prior to the enforcement date[43]
    - Is out of scope of SCA e.g. MOTO.

Where these requirements are met, an MIT does not require SCA. However, SCA must be applied when certain changes are made to the agreement, for example if the cardholder wishes to use a different card. For merchant driven changes to payment terms, such as payee changes to price due to inflation, authentication is not required provided that the original agreement T&Cs and other cardholder communications clearly cover the eventuality of such changes. If not, SCA is required.

Additionally, there is no need for SCA to have been applied to the initial CIT used to establish the agreement for future MITs in the following scenarios:

- The transaction qualifies for the secure corporate payments exemption
- The Transaction is a Resubmission or Reauthorization, as defined under the Visa MIT framework, and is simply the completion of an existing CIT (i.e. it is not an MIT for regulatory purposes). The CIT will have been authenticated, or qualified for an exemption, when it was originally initiated by the cardholder.
- Where the CIT establishing the MIT is using a contactless card and the transaction qualifies for the contactless transaction at Point of Sale exemption. For example in a scenario where the cardholder enters a shop by tapping a contactless card and will be able to walk out without going through a checkout. At time of entry/contactless tap, two actions take place: (1) the cardholder authorizes a transaction for an amount below the contactless exemption limit -and thus, SCA is not required, and (2) an MIT is set up (T&Cs disclosed to cardholder). As the MIT set-up is being performed in a face to face rather than a remote environment, SCA is not required under Article 971.c of the PSD2 regulation. Subsequent incremental transactions do not need SCA either, as they would be covered by the MIT mandate.

[42] PSD2 specifically states that SCA applies to payments initiated by the payer. The EBA and FCA have confirmed that transactions initiated by the payee are out of scope of SCA as long as SCA was applied when setting up the mandate if that mandate was set up via a remote channel and there is a risk of fraud or other abuses.

[43] Merchants, Acquirers and Issuers should note that enforcement dates were 31 December 2020 for the EEA, and 14 March 2022 for the UK.

Notwithstanding the above, in order to limit fraud risk Visa has capped the incremental amount that can be authorized without SCA to the maximum single contactless limit.

An MIT can only be submitted where it is subject to a specific agreement set up with the cardholder as part of the initial CIT and clearly disclosed to that cardholder. The agreement should clearly define the circumstances under which an MIT may be used, including, but not limited to, the following[44]:

- Name and full address of Merchant
- Purpose of the agreement / payment
- Type of payment (such as recurring, no show, prepayment)
- Timing and frequency of the transaction or the event that will trigger the transaction
- The transaction currency and amount or a description of how the transaction amount will be determined
- Total amount and currency of the agreement (or if final amount is not known, details on how the final amount will be calculated
- Amount and currency of the authentication
- Cancellation procedure
- Additional T&C clauses may be required based on the nature of the transaction, including potential expiration date
- The merchant must also provide a copy of the MIT agreement with the consumer via email

In addition to MITs that are out of scope, the MIT framework will also indicate some transactions which are not out of scope but where SCA has already been performed or an exemption has been applied before the transaction is executed.

This is the case for the following types of MITs from the Visa MIT Framework because in these cases the transactions are simply the completion of an existing transaction where SCA was already performed (or the transaction was exempt), and so no further authentication of the cardholder is required. The CIT does not require SCA if an exemption is applicable, even if the transaction may be subsequently completed with the MIT indicator.

- *Resubmission*: This is the case for a contactless transit transaction where an exemption applied. The transaction may have been initially declined due to insufficient funds, but as the service was already rendered, it is permitted by Visa Rules to be resubmitted for completion.
- *Reauthorization* (used in delayed or split authorizations): this is the case where the merchant is permitted or required to either repeat or split an authorization in order to complete an existing payer initiated transaction under Visa Rules (e.g. because the original authorization has expired, or because the order cannot be delivered in one shipment).

[44] Refer to the Visa rules for specific required T&Cs for different transaction types (for example for guaranteed reservations).

This is also the case when:

- A cardholder agrees to pay a No Show fee with an eligible merchant and the agreement is made during a booking made via a secure corporate payment process that qualifies for application of the secure corporate payments processes and protocols exemption. In Visa's view, it is permissible that SCA is not performed on the CIT that sets up the No Show agreement providing that the secure corporate payments exemption is applicable, and the PSP considers there is no risk of fraud[45].
- An MIT is set up via MOTO as MOTO transactions are out of scope of SCA.

Requirement

The initial CIT used to establish an agreement for future MITs is in scope of SCA, and it is required that SCA is applied in most cases (for exceptions see above), For more details on how to establish an agreement, refer to Section 5.12

3.8.2 Acquirer use of the Visa MIT Framework

To avoid inadvertent declines, Acquirers / merchants must use the existing Visa MIT Framework to enable Issuers to properly identify transactions which are out-of-scope MITs and where the Issuer should not request SCA. It is their responsibility to ensure that any transactions they indicate as MITs are legitimate MITs, as per the criteria listed above.

3.8.2.1 Populating the original Transaction ID for MITs

The Visa MIT framework requires that an Acquirer includes a transaction ID relating to previous relevant transaction in Field 125 or 62.2 as follows:

- For recurring, installment and unscheduled COF transactions, Visa MIT framework processing requirements allow Acquirers to use either the initial CIT or previous MIT Transaction ID. In Europe, Visa recommends using the initial Transaction ID to link to the transaction where the mandate to process MITs was set up.
- For Incremental, No Shows, Delayed Charges, Resubmission and Reauthorization, the Transaction ID of the initial CIT must be used.

3.8.2.2 Grandfathering

For MITs covered by cardholder agreements that were established prior to the regulatory enforcement date, those transactions should be able to continue to be processed without SCA as long as they are identified as MITs using the Visa MIT Framework. If the transaction ID of the initial transaction where the mandate was set up is not available, the transaction ID of any related MIT processed before the regulatory enforcement date can be used. Visa recommends that clients store the transaction ID of the selected transaction and include it in future related MITs to represent the "initial" transaction. However, as stated above, the transaction ID of the

[45] For example use cases please Sections 5.12.1 and 5.18.

previous MIT is also acceptable to use for recurring, installment and unscheduled COF transactions.

3.8.2.3 Visa provided interim Tran IDs

Visa is aware that enhanced system development may be required to store Tran IDs of previous transactions. Accordingly, to assist with merchant readiness in time for the regulatory enforcement date, if the merchant was unable to obtain an initial or previous transaction ID to pass on to the Acquirer, Visa provided Acquirers, on request, a Visa Acquirer-assigned interim Tran ID for use in place of a valid Original Tran ID on an interim basis. This interim identifier can be used by any merchant acquired in the EEA and the UK providing its Acquirer supports this feature. This gives the Acquirer and the merchant additional time to make the necessary system changes[46].

Table 15 provides a view of the impact of using this Visa Acquirer-assigned interim Tran ID.

Transitioning to the use of a valid transaction identifier in MITs is critical to maintain the data quality of these transactions and allows Issuers to make better processing decisions on transactions initiated by the merchant, as it references a previous successful transaction. With this objective in mind, Visa has now announced that it will stop accepting usage of the interim Tran ID for readiness purposes from 31 October 2023.

- Non-compliance assessment fees (NCAs) will begin to accrue as of August 2022 and will be applicable to Acquirers for any use of the interim Tran ID as of 1 November 2022. Acquirers who are using an interim Tran ID must ensure that merchants using them are aware of the final date of usage.

Until 31 October 2023, when an interim Tran ID provided for readiness purposes is used in an MIT, Visa will replace it with the ID "0100000000000000" before sending to Issuers. Issuers have been informed this value means the merchant/Acquirer is not ready to send a valid Tran ID for this MIT and has been asked to accept this value for an interim period of time to process and identify MIT's successfully. Refer to section 3.8.3.2 for more details

After 31 October 2023, Visa will no longer replace the interim value provided for readiness purposes and Issuers may start declining any transactions that are still sent with an interim Tran ID.

After this date Visa will continue to support grandfathering to ensure that subscriptions set up prior to enforcement can continue without requiring reauthentication. However to take advantage of this, merchants using an Interim Tran ID for subscriptions need to transition to a valid transaction ID before the end date. To do this, merchants (or their gateway provider or Acquirer) must, prior to the final date, be in a position to store a valid Tran ID for an MIT that has been populated with the interim identifier and successfully approved..

Two transition options are available to these merchants:

1. The merchant or its Acquirer/gateway captures a valid transaction ID returned in the authorization response received when submitting a MIT with the interim transaction ID.

[46] Refer to Article 2.17 of the *October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019* for more details.

This valid transaction ID can then be populated in the original Tran ID Field (F125) of subsequent MITs[47].

2. The merchant subscribes (via their Acquirer) to the Visa Network MIT Service which works as follows:

   - The interim Tran ID sent with an MIT acts as a request to Visa to store the transaction ID issued in the successful response to this MIT authorization request.
   - For future MITs, Visa populates the authorization request on behalf of the merchant/Acquirer with the valid/stored Tran ID.

   For more information, refer to the *Visa Network Merchant Initiated Transactions Service – Implementation Guide*[48].

Merchants using an interim Tran ID for annual subscriptions should take particular care to ensure that they have obtained a valid Tran ID sufficiently well in advance of the expiry of the interim Tran ID. This is necessary to ensure they are able to process subscription payments due after the final date.

After 31 October 2023, Visa is aware of certain circumstances where a merchant may no longer have a valid Tran ID in its possession to continue processing its ongoing MITs. For example in case of switching acquirer/processor/gateway or when a credential is updated via the Visa Account Updater due to an Issuer switching scheme. In such cases acquirers can request Visa for a different Interim Tran id to be used for these purposes under specific conditions (More details on this to be provided via Visa Business News in April 2023). When this Interim Tran ID is used, Visa will continue to replace it with the ID "0100000000000000" before sending to Issuers.

3.8.2.4 Populating the POS entry mode for MITs

Note that while the POS entry mode field (Field 22) is not part of the MIT Framework, it is important it is populated appropriately as presented in Table 15.

- Note that for any of the transactions in Table 15, be they first (CIT) or subsequent transactions (MITs), the merchant should use POS entry mode 10 (which means "stored credentials") for the transaction if it is performed using an existing stored credential. As Recurring, Installment, or UCOF MITs can only be performed when credentials are stored, those MITs always require the use of POS Entry Mode 10.
- However, Incremental, No Shows, Delayed Charges, Reauthorization, or Resubmission MITs should only use POS entry mode 10 if the merchant stored the payment credentials for future purchases as part of an agreement with the customer. POS entry mode 10 should not be used if the credential is only stored to complete this specific transaction. For more information about the Stored Credential Framework and what is required to use it, see Appendix A.1.

[47] Merchants must work with their Acquirers (or gateways) to understand how the Visa MIT Framework is made available through their implementation.

[48] Merchants should check with their Acquirers to determine whether they support the Visa Network MIT Service and, if so, how to register for it.

3.8.3 How Issuers identify MITs

Issuers must be able to recognize MITs to avoid requesting SCA which cannot be performed due to cardholders not being available to authenticate the transaction. They can do so using one of the following ways:

- Using the Visa MIT Framework, (see Table 15), or
- The initiating party indicator introduced in Field 34 (see Table 15), as documented in *Article 9.1.4 of the October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019.*

Whichever method is used to identify an MIT, Issuers may not use an SCA decline code in response to an authorization request for a properly identified MIT, to avoid any associated friction and inadvertent declines due to the cardholder not being available for authentication.

3.8.3.1 Issuer identification of MITs using Field 34

Issuers can select to identify an MIT as out of scope of SCA by checking the Initiating Party indicator in Field 34 (Tag 80, Dataset ID 02) i.e. the same field Issuers use to check for exemptions to SCA.

The Acquirer must continue to use the existing Visa MIT Framework to indicate MITs. When receiving transactions that are indicated as MITs using the framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02), as depicted in Table 15. This enables Issuers to recognize a transaction as a MIT out of scope in real time by simply looking for the value of "1" in that tag. Visa does not validate whether the initial CIT referenced with the MIT was authenticated. However Acquirers are required to ensure a transaction indicated as an MIT meets all requirements, including SCA at set-up. Issuers using this method at time of authorization may wish to receive and store the Tran ID populated in F125 for every MIT to provide an audit trail in case they are ever required to prove that SCA took place at MIT set up.

3.8.3.2 Issuer identification of MITs using the Visa MIT Framework

The Issuer can alternatively recognize an MIT using the existing Visa MIT framework. This is done by looking for the presence of the MIT type identifier in Field 126.13 or F63.3 and the Tran ID of the initial CIT (or previous MIT in some cases) in Field 125.

Only Issuers that are enabled to receive Field125 will get this value. Issuers must check with their account executive/customer support regarding how they can technically enable their system to receive Field 125.

Issuers that choose to use the existing Visa MIT Framework to identify these transactions as out of scope of PSD2 / SCA requirements must be aware that:

- The number populated in Field 125, Usage 2, Dataset ID 03 generally represents the Tran ID of the initial CIT or of a previous MIT transaction. However, Visa has assigned alternative Tran IDs to Acquirers for use in this field (prior to October 31, 2023 to

assist with PSD2 readiness, after that date for various use cases where a merchant may temporarily no longer have access to a valid Tran ID for pre-existing MITs). Therefore, in those cases, Issuers will see a value of "0100000000000000" in Field 125[49], indicating that the merchant/Acquirer was not in possession of a valid Tran ID for this pre-existing MIT agreement with the cardholder. Issuers are asked to accept this value.

- The transaction ID the Issuer will see in F125 of an MIT will therefore be one of the following:
  - The valid Tran ID of a valid initial CIT or previous MIT. This may include:
    - The Tran ID of a previous MIT processed with the interim identifier of "0100000000000000" which is the case when a merchant that was initially not ready (and was thus using an Acquirer assigned Tran ID) starts to use a valid Tran ID of a previous MIT
    - The Tran ID of an initial CIT which has been reversed. Issuers are asked to consider valid the Tran ID of a reversed initial CIT as a reversal often does not mean the agreement set up at initial successful approval has been cancelled. The cancellation may be only for the financial transaction made at the same time. Illustrative examples include:
      i. A cardholder may enter into an agreement with a hotel authorizing the collection of delayed charges after the stay is over. If this is done through a CIT processed as an estimate at time of check in and at checkout the known amount of charges due are less than the full estimate, the transaction may be partially or fully reversed. If additional charges subsequently need to be collected post checkout, using an MIT delayed charges, the Tran ID provided may be for the CIT that is now reversed
      ii. The transaction to set up an MIT for recurring services from a retailer also includes the purchase of unrelated goods. The goods may be returned and so the sale will be reversed, yet the recurring agreement may still be valid and subsequent MIT authorization requests may contain the Tran ID of the reversed CIT
  - The interim Issuer transaction id of "0100000000000000"

    Until 31 October 2023
    - Used when a merchant was not ready to send a real Tran ID but did send one assigned to them by Visa for this purpose

[49] For further details, refer to Article 2.17 of the *October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019*. From November 2023, any transaction still sent with an Interim Tran ID that is no longer valid will be sent as is to Issuers. This Interim Tran ID will not represent a valid transaction identifier previously processed with this card and Issuer and thus transactions with an Interim Tran ID may be declined.

- This can represent a MIT that is being grandfathered, or an MIT put in place after enforcement date (with SCA applied) but where the merchant is still not ready to send a valid Tran ID

  After 31 October 2023

- Used when a merchant temporarily no longer has a valid Tran Id to process a pre-existing MIT and has been granted a Visa assigned interim Tran Id to enable continuity of ongoing MITs (one off per merchant per credential). A merchant can be in this situation due to, for example, switching acquirer/processor/gateway or due to having received via the Visa Account updater an updated credential due to an Issuer scheme switch. The interim Tran Id is permitted by Visa to "bridge the gap" and re-obtain a valid Tran Id for future MIT processing.

Or

- Any other number populated by the merchant/Acquirer and not considered as a valid transaction ID
  - This may be a number sent in error, attempted fraud or, after 31 October 2023, a now invalid Interim Tran ID

It is an Issuer's decision whether to check the validity of the Tran ID present in this field before making the approval decision

- For transactions indicated as recurring, installment or unscheduled credential on file (UCOF) by a value in Field 126.13, these can be either customer-initiated or merchant-initiated. It is the presence of a value in Field 125, Usage 2, Dataset ID 03, which will allow Issuers to identify these transactions as MITs: a CIT, unlike an MIT, will carry no value in Field 125. The value "10" in Field 22 (POS Entry Mode) indicating the transaction is performed with stored credential does not necessarily indicate that a transaction is a MIT, as it may also be present in a CIT.

Please refer to Table 15 to identify all the key data fields and values to be used in authorizations to identify CITs used to set up MIT agreements and MITs.

Table 15: Key data fields and values for MIT transactions and CITs used to set up MIT Agreements

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34[i])	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125[ii])			
Installment/ Prepayment	First Transaction (CIT) (May be of zero value if set up only)	I	--	--	Any valid[iii] (10 if stored credential)	--	Required when in a remote channel

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34[i])	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125[ii])			
	Subsequent Transactions (MIT)	I	--	Tran ID of first transaction/ previous MIT *(Or interim Tran ID)*	10	1[i]	N/A
Recurring	First Transaction (CIT) (May be of zero value if set up only)	R	--	--	Any valid[iii] (10 if stored credential)	--	Required when in a remote channel
	Subsequent Transactions (MIT)	R	--	Tran ID of first transaction/ previous MIT *(Or interim Tran ID)*	10	1[i]	N/A
Unscheduled Credential on File (UCOF)	First Transaction (CIT) (May be of zero value if set up only)	C	--	--	Any valid[iii] (10 if stored credential)	--	Required when in a remote channel
	Subsequent Transactions (MIT)	C	--	Tran ID of first transaction/ previous MIT *(Or interim Tran ID)*	10	1[i]	N/A
Estimated/Incremental	First Transaction (CIT) (Estimated transaction[iv])	--	--	--	Any valid[iii] (10 If stored credential)	--	Required when in a remote channel. When card present, only required by Visa rules to enable processing of incremental(s) that may bring the total of the estimated &

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34[i])	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125[ii])			
							incremental(s) above the CVM limit
	Incremental/ Subsequent Transactions (CIT or MIT)[v]	--	3900	Tran ID of first transaction	Any valid[iii, v] (10 if stored credential)	1[i]	Required, when both: • The estimated transaction was Card Present and • The total of estimated and incremental > CVM Limit and SCA not previously obtained at time of estimate
Delayed Charges	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Required when in a remote channel
	Subsequent Transactions (MIT)	--	3902	Tran ID of first transaction *(Or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A
No Show	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Required when in a remote channel (Except if secure corporate payment exemption applies)
	Subsequent Transactions (MIT)	--	3904	Tran ID of first transaction *(Or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34[i])	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125[ii])			
Reauthorization	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Exemption may be used. CAVV, may or may not be present as the merchant has the option to provide in the initial CIT or in the MIT reauthorization [vi]
	Subsequent Transactions (MIT)	--	3903	Tran ID of first transaction *(Or interim Tran ID)*	01 or 10 if stored credential		Not required but CAVV may optionally be present
Resubmission	First Transaction (CIT)	--	--	--	Any valid[iii] (10 if stored credential)	--	Contactless exemption applies[vi]
	Subsequent Transactions (MIT)	--	3901	Tran ID of first transaction *(Or interim Tran ID)*	01 or 10 if stored credential	1[i]	N/A

Notes:

i. The new initiating party indicator indicates a transaction is an MIT out of scope of SCA indicator and is populated in Field 34 Tag 80 and is for Issuer use only. Visa will automatically populate the value 1 in Field 34 Tag 80 for Issuer usage when a transaction is submitted by an Acquirer using the existing Visa MIT Framework.

ii. Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that participate to receive Field 125. The Transaction ID in F62.2 which is presented in the authorization request to Issuers and response back to Acquirers is the one of the current MIT and not that of the initial CIT as Visa always generates a new, unique, Tran ID for each transaction, including subsequent MITs, in this field (except in the case of incremental authorizations where the initial Tran ID is kept).

iii. Any valid value because these transactions can also originate in card present channels.

iv. Incremental transactions must be preceded by an estimated/initial authorization. The estimated authorization indicator with a value of 2 or 3 must be included in Field 60.10 - Additional Authorization Indicators.

v. An Incremental transaction can be conducted either in card present or card not present mode. When a card is present, it is a CIT processed to complete another CIT and chip data **must** be present. When conducted in card not present mode, it is considered an MIT processed to complete the initial estimate: chip data must not be present (i.e. cannot be reused) and POS entry mode must be 01. When Incremental(s) are used, one single clearing is required for the total of the initial estimate and all associated incrementals.

vi. The associated subsequent MITs are simply the completion of an existing transaction, no further authentication of the cardholder is required as long as the CIT was compliant, i.e. if exemptions were applicable, they can be used. However, note that application of exemptions for qualifying CITs that will be followed by MIT reauthorization(s) must be processed via EMV 3DS so that the amount against which the exemption is requested can be the total purchase amount. Processing via EMV 3DS is required so the Issuer can take the decision on whether to allow the exemption based upon the full purchase amount, not the value of an initial partial authorization. Refer to section 5.1.3 and Figure 21 for various options with regards to placement of the CAVV in this transaction.

Refer to Table 16 for a visual representation of the impact of the usage of interim Tran IDs in MITs, both from an Issuer and Acquirer perspective.

Table 16: Acquirer and Issuer View of MIT Transactions with usage of Visa Acquirer assigned interim Tran IDs

CIT Types	Visa Existing MIT Framework – Acquirer View[50]			MITs – Issuer View			
	POS Env. (F126.13)	Reason Code (F63.3)	Field 125 or F62.2	POS Env. (F126.13)	Reason Code (F63.3)	Field 125[51]	Initiating Party Indicator (F 34, Tag 80 Dataset 02[52])
Standing Instruction MITs (Recurring, Installments/ Prepayments & UCOF)	R, I or C	-	Tran ID of initial CIT or previous MIT	R, I or C	-	Tran ID of initial CIT or previous MIT	1
	R, I or C	-	Visa Acquirer assigned Interim ID	R, I or C	-	01000000 00000000[53]	1
Industry Specific MITs – except Incrementals (Resubmission, Delayed Charges, Reauthorization, No Show)	-	3901 to 3904	Tran ID of initial CIT	-	3901 to 3904	Tran ID of initial CIT	1
	-	3901 to 3904	Visa Acquirer assigned Interim ID	-	3901 to 3904	01000000 00000000[53]	1
Incrementals[54]	-	3900	Tran ID of initial CIT	-	3900	Tran ID of initial CIT	1

[50] It is the Acquirer's responsibility to ensure that any transactions they indicate as MITs meet the requirements defining an MIT. Acquirers may also use the Visa MIT Framework to indicate some transactions that are in scope but where SCA was performed or an exemption applied, notably in the cases of resubmitted transit transactions (resubmission MIT type) or delayed or split authorizations (reauthorization MIT type).

[51] Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that participate to receive Field 125.

[52] When Visa receives a transaction indicated as an MIT, it will automatically populate the value of "1" MIT out of scope of SCA in F34.

[53] Issuers are asked to continue to accept this value representing pre-existing MITs.

[54] An Acquirer assigned transaction identifier must not be used on incremental transactions.

3.9 Visa Biometrics

Visa has designed various products and services to help our clients to utilize biometrics to authenticate customers.

For clients that need support in getting started with the technology, Visa has a discovery program that explores various biometrics technologies available, helps clients to test the user experience and understand security, risks and implementation considerations.

Visa provides an easy to implement authenticator app for clients who use Visa Customer Authentication Service (VCAS) and are looking to launch an app plus biometric solution with minimum deployment of internal resources. The app can be Issuer branded and launched in a short timescale. It also supports other authentication use cases such as account recovery and remote customer verification for call centres.

Please contact your Visa representative if you would like more information on VCAS and Visa's authenticator app solution.

3.10 Visa Consumer Authentication Service

Visa Consumer Authentication Service (VCAS) is a data-driven hosted ACS solution designed to support an Issuer's authentication strategies delivered through EMV 3DS.

At the core of the product are Risk Based Authentication (RBA) capabilities, which work behind the scenes to evaluate each transaction based on data exchanged between the merchant, the Issuer and Visa. This can help to considerably reduce friction during checkout, whilst also providing greater levels of security. To deliver this, VCAS assesses the risk of a transaction in real-time using predictive risk analysis based on a number of enhanced inputs, including device and transaction information and behaviors. This network-wide level of intelligence gives Issuers more information to decide if and when additional authentication is needed.

The VCAS Compliance Manager application provides Issuers with insight into what transactions may need SCA, identifies transactions that may qualify for exemptions, may help prevent collision between compliance and risk rules and also gives an Issuer the flexibility to override exemptions with additional rules. Issuers will maintain control over whether they approve transactions. When SCA is required, VCAS supports multiple methods for Issuers to perform SCA, including biometrics, one-time passcodes and push notifications to the Issuer's Mobile Banking App.

The VCAS Portal gives Issuers unprecedented flexibility to refine risk strategies through custom rules based on multiple parameters and to anticipate or respond to new fraud trends as they emerge.

The VCAS solution has been built in partnership with CardinalCommerce, an industry leader in digital payment authentication that is fully owned by Visa. VCAS will fully support EMV 3DS along with the other authentication products in the Visa portfolio. Issuers seeking support in migrating to EMV 3DS may wish to consider VCAS as an option to enable the transition.

For more information please see https://www.cardinalcommerce.com/products/visa-consumer-authentication-service.

4. Optimizing the payment experience under PSD2

4.1 Introduction

Under PSD2, SCA is not required for all electronic transactions. Some transactions are out of scope of the regulation or exempt and where this is the case, SCA is optional and in some cases should not be used.

Clients will need to assess and decide how to treat each transaction with regards to the application of SCA based upon a combination of factors including:

- Whether a transaction is out of scope or qualifies for an exemption
- Fraud risk
- Optimization of user experience
- Liability protection

It is critical that merchants and Acquirers indicate transactions correctly to ensure Issuers are able to identify transactions where SCA is not needed and authorize appropriately.

Merchants and Acquirers who wish to request or apply an exemption should only apply or request one exemption per transaction by setting one exemption indicator in the appropriate EMV 3DS and/or authorization request fields.

Visa provides a number of tools and services (described in Section 3) to enable clients to take full advantage of the application of exemptions while keeping fraud rates low.

This Section 4 provides guidance on:

- Key principles that clients should apply when assessing, routing, flagging and processing transactions
- The main decision points in a basic transaction flow for both merchants/Acquirers and Issuers and on the assessment and treatment of a transaction at each point
- Use of the MIT framework for managing out of scope Merchant Initiated Transactions
- Practical application of the main exemptions (building on previous sections)
- Issuer deployment of EMV 3DS including selection of challenge methods and optimization of user experience
- Issuer processing
- EMV 3DS and authorization fall back options (The Visa Attempts Server and STIP)
- The application of SCA in the context of Visa Direct transactions

More detailed guidance on the application of SCA, authentication and authorization flows for specific transaction use cases is included in section 5 of this guide.

4.2 Key principles

4.2.1 Transactions that may be submitted for Authentication or direct to Authorization

Transactions that are out of scope or qualify for an Acquirer exemption may be submitted for authentication or sent directly to authorization, with the appropriate indicators as described in section 3.2.9.

Factors to consider when selecting the appropriate option are summarized in section 4.3.

4.2.2 Managing variations in amount, merchant name & merchant/ Acquirer ID

4.2.2.1 The regulatory requirement

The PSD2 SCA dynamic linking requirement, which is summarised in section 2.4 requires that (i) the payer is made aware of the amount of the payment transaction and of the payee and that (ii) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction; and that (iii) any change to the amount or payee results in the invalidation of the authentication code generated.

Visa's view is that the authentication code requirement can be achieved by the sharing and validation of the CAVV or TAVV which gives cryptographic proof that the authentication completed successfully. For more information on the use of the CAVV and TAVV please see section 3.2.7.

There will be legitimate scenarios where there are variations between the merchant names, merchant IDs, Acquirer IDs and amounts submitted during authentication and authorization and Issuers should not decline transactions just because there is not an exact match. This is on the proviso that if the transaction is initiated in the EEA, the final amount does not exceed the authenticated amount or if the transaction is initiated in the UK, the final amount meets the criteria summarised in section 2.4 and that any name or merchant ID variations are legitimate. The following sections expand on these points.

4.2.2.2 Managing variations in merchant name and/or merchant/Acquirer ID

As described in section 2.4, the payee information included in the authentication code may not necessarily need to be the full or exact merchant name but can match a unique identifier corresponding to the payee at authentication.

Where there are differences to the merchant name, or merchant ID between authentication and the final transaction submitted to authorization, Acquirers should ensure that there is a clear rationale for this. For example, the merchant name should be clearly recognizable as being the same merchant in both flows but character for character matching should not be required.

For example, in Travel and Hospitality bookings, when a transaction is the result of a booking via an agent who initiates authentication on behalf of a third party merchant that subsequently requests authorization, the name in the authentication request may be that of both the agent and the merchant, whereas the name in the authorization request may be that of the merchant only.

Note that Merchant IDs, and Acquirer IDs are irrelevant to the requirement of dynamic linking and Merchant IDs and Acquirer IDs may change between authentication and authorization, for example where a merchant submits a transaction via different Acquirers for authentication and authorization.

4.2.2.3 Managing variations in amount

As described in section 2.4, the for the EEA, the EBA has confirmed that the final amount should not increase above the authenticated amount. In the UK, the FCA has confirmed that that re-authentication is not required if the final amount is higher than the original authenticated amount so long as:

1. The final amount is within the customer's reasonable expectations
2. That the increase between the authenticated final amount is no more than 20%
3. The customer was made aware that the amount could increase

In this section for brevity, we refer to an increased final amount that meets these requirements as an "allowable increased final amount"

In the UK it is possible for a merchant to request authorization for an amount that is higher than the amount authenticated only so long as the above criteria for the allowable increased final amount are met, and funds have not been blocked (i.e. have not yet been authorized in the Visa system). Once the transaction has been authorized, the final amount settled against that authorization may be lower, but must not be for a higher amount than the authorized amount. If a merchant wishes to increase the amount charged for an authorized transaction, they will need to authorize the additional amount via an MIT incremental as defined in section 4.2.2.4 below.

In the EEA, re-authentication is required for any increases above the authenticated amount and in the UK, for increases above the allowable increased final amount. The same does not apply where the final, authorized amount is lower than the authenticated amount. In these cases, no re-authentication is required.

In the case of cross border transactions between the EEA and the UK where the Issuer is in the EEA, reauthentication is required if the final amount increases above the authenticated amount. If the Issuer is in the UK, the final amount may increase within the allowable increased final amount even if the transaction is acquired in the EEA.

Options to enable merchants to process transactions for which the final amount is unknown without the need to authenticate are summarised for various payment use cases in section 4.2.2.4.

To address use cases where the final amount is higher than the authenticated amount, with the publication of the October 2020 Visa Rules[55], Visa removed existing authorization tolerance limits for the EEA and expanded the availability of its existing estimated / incremental authorization framework to additional merchant segments for EEA and UK transactions by:

[55] For details, please refer to *Visa Business News Expanded Eligibility for Estimated and Incremental Authorization in the EEA and UK to Support Amount Variation*, (AI106007).

- Eliminating for EEA transactions, existing authorization tolerance limits that allow e-commerce and certain other specific merchants to clear an amount greater than the authorized amount
- Allowing all e-commerce merchants in the EEA and the UK to use initial / estimated and incremental authorizations in the event that the final transaction amount is anticipated to differ from the initial authorized and authenticated amount (Visa Rules ID#: 0025596)

Merchants submitting transactions where the final amount is unknown and could exceed the amount initially authenticated should take account of both the regulatory limits on increased amounts but also of Visa rules governing fraud liability and settlement before deciding how to handle the variation. The combined impact is summarised in Table 17 below:

Table 17: Limitations on final amount increase imposed by regulation and Visa rules

	Regulatory Limits	Visa Secure Amount Variation Rule	Visa Settlement Amount Variation Rule	Impact
Visa Rule Definition		Issuer bears fraud liability so long as authorized amount is ≤ 15% of authenticated amount	Except in the EEA, settlement amount may be up to 15% higher than authorization amount	
EEA Transactions	Final amount must not exceed authenticated amount	Transaction value above authenticated amount in breach of regulation but if an Issuer authorizes it assumes liability for up to 15% higher as per Visa rule	Visa has removed the tolerance allowed by the rule for the EEA so settlement amount must not exceed authorized amount to help support regulation	Merchants should apply one of the options listed in section 4.2.2.4 if the final amount exceeds the authenticated amount
UK Transactions	Final amount may exceed authenticated amount by ≤20% so long as other allowable increased final amount conditions apply, and funds have not yet been authorized	Liability protection for the merchant under Visa Rules still limited to 15%	Settlement amount may be higher than authorized amount as allowed by the rule (% varies per use case – refer to Visa Rule ID 0025596)	Merchants may want to limit final amounts to 15% above authentication amounts to maintain liability protection before applying one of the options listed in section 4.2.2.4

4.2.2.4 Merchant options for handling amount variations

Use cases where the final amount may increase after authentication[56] and options for merchants seeking to collect funds for increased final amounts without the requirement to reauthenticate are summarised below.

4.2.2.4.1 Handling amount variation due to changes not initiated by the customer

There are several use cases where the final amount the customer should be charged for is not known at checkout and can end up being higher than the amount authenticated due to circumstances after checkout that are not initiated by the cardholder. Examples include:

- Purchases where final shipping costs and/or taxes are not known at the time the customer checks out and authenticates[57]
- Online grocery shopping, where the actual cost of weighed goods is not known until the order is picked or when pre-agreed substitutions are made for ordered goods that are unavailable.

In such cases the final amount cannot be calculated until the fulfillment process is complete and/or the order is prepared for dispatch, at which time the cardholder is no longer available for reauthentication.

Merchants have two options for dealing with such cases, where the regulation would require re-authentication. They should consider the technical, operational and customer experience impacts of each option.

[56] Recurring payments, unscheduled credential-on-file and Installment transactions are MITs and therefore are not impacted. Amounts can vary in line with the terms and conditions agreed upon with the customer for those transactions.

[57] Note in the UK, the FCA has confirmed that the definition of the final amount is the amount including taxes and shipping costs.

Option 1—Merchant-initiated transaction (MIT) incremental authorization:

This is the Visa-preferred option from a customer experience perspective.

When a merchant knows that a final amount may vary when the cardholder is no longer available to authenticate, they process the initial authorization with the "known" amount at checkout as an "initial or estimated"[58] amount and the additional unauthenticated authorization amount as an MIT—Incremental[59]. More specifically:

At the time of authentication:

- Terms and conditions specifying how the final amount will be calculated and when the charges will be collected must be disclosed and agreed to by the customer.
- Authentication is performed on a "known" initial amount with the application of an SCA challenge; no exemption can be used when setting up an agreement in a remote channel for the merchant to process a future MIT.

At the time of authorization:

- The authenticated amount is authorized as a CIT with the authentication data ECI values and CAVV and an "estimated authorization request indicator"[60] informing the Issuer that this is an estimated authorization that may be followed by an MIT—Incremental, if required.
    - If an Issuer opts to inform the cardholder of an authorization request via for example alert or online statement it must ensure that when such request include an "estimated indicator" or is an MIT incremental, the notification communicates clearly that this is an estimate, and the final amount may differ[61]
- If the final amount is higher than the authenticated / authorized amount in the EEA, or in the UK is higher than the allowable increased final amount, the additional amount is authorized as an MIT—Incremental, which includes a reference to the initial CIT. No additional authentication is needed as long as the final amount is within the terms and conditions agreed upon with the cardholder at mandate setup. Depending on when the initial or estimated authorization takes place (which, dependent on business process, may be straight after authentication or at a later time), an MIT—Incremental may be submitted shortly after the initial or estimated authorization or later. Multiple additional incremental authorizations may also occur before the transaction is finalized for clearing and settlement.

---

[58] An amount is considered as "initial or estimated" in the authorization request due to the presence of the estimated indicator in the request. In this first option, it is recommended to use the "known" amount at the time of checkout as the "initial or estimated" amount. (The Visa Rules also allow for the use of an "estimated" amount prior to an MIT—Incremental, but in the context of PSD2 SCA, estimated amounts are recommended for use with option 2 rather than option 1).

[59] A transaction can only be processed as an MIT when the cardholder is not available to initiate or authenticate the transaction at point of interaction. If the cardholder is available to do either of these, the transaction cannot be processed as an MIT and option 2 must be considered instead.

[60] Merchants should contact their Acquirers for details of the rules associated with the use of initial or estimated authorizations and incremental transactions as well as appropriate flagging.

[61] Refer to Visa Rule ID # 0029466.

- Note that if the final amount is lower than the authenticated / authorized amount, merchants must process partial reversals for the amount of the difference.

Clearing and settlement:

- When the final amount is cleared / settled, the cardholder will see a single transaction for the total amount on their bank statement / mobile banking transaction history.

Option 2—Perform initial authentication for a highest estimated amount:

An alternative method for handling potential amount variation, which may avoid requesting an authentication step-up, is to authenticate at checkout for the highest possible amount that would cover any anticipated amount variation. This option may, however, cause customer confusion or cart abandonment if the cardholder is unclear why they are being asked to authenticate for a higher amount than the checkout value of the goods or services. It is essential for merchants pursuing this option to clearly communicate to the customer (i.e., including prior to presentation of the EMV 3DS challenge window if SCA is required) that:

- They are being authenticated for a maximum authorization amount.
- They will only be charged for what they purchase (which may be lower than the authenticated amount) and for any other relevant charges not yet known (e.g., shipping and taxes).
- No charges will appear on their card statement until the order is finalized.

In the EEA, the final amount processed at the time of authorization can only be lower than or equal to the authenticated amount. In the UK the final amount can only be lower than or equal to the allowable increased final amount. If the final amount is higher, a new authentication will be required (i.e., the customer must be re-contacted if they are no longer available to authenticate).

If the final amount is lower, and the authorization has already been processed, a reversal must be processed for the difference.

Note that with this option, an SCA exemption may be applied at authentication as long as the transaction qualifies.

If the merchant considers that there is any possibility that the actual final amount will exceed the authenticated amount and does not want to have to re-contact the customer, option 1 should be selected.

4.2.2.4.2 Unplanned Higher Amount

In the event that the final amount is higher than the authenticated amount, or in the UK the allowable increased final amount, and the merchant had not planned for it using either of the options above, the merchant will need to contact the cardholder to authenticate the additional amount. The merchant then has the choice to:

- Authenticate for the new total final amount and submit one final authorization with this final amount (exemptions can be used if applicable), in which case, if an initial authorization had been processed prior to this, it must be reversed in full, or
- Authenticate only for the additional amount (exemptions can be used if applicable) and submit two authorizations, one for the initial amount and one for the additional

amount, each with their respective authentication value or exemption indicators, as applicable.

An additional amount cannot simply be processed by the merchant as an additional authorization with an exemption indicator: even if a transaction for this amount would qualify for an exemption. The customer must initiate a new transaction. This is the case because if the transaction is initiated by the merchant, it would be an MIT, which cannot be processed without prior customer consent and authentication. Exemptions can only be applied to customer initiated transactions.

4.2.2.4.3 Amount variation due to a customer adding to a basket

In some use cases, a customer may be able to make changes to an order after they have checked out and authenticated, and these changes may increase the final amount that the merchant submits for authorization. For example, an online grocery shopping service or a food delivery service may allow customers to checkout and authenticate to secure their delivery slot and then change items in their basket until a cut-off time a set number of hours before delivery. In this case, the final amount would be calculated, and the authorization submitted after the cut-off time when the customer is no longer available to authenticate. A customer making several incremental changes to an order in this way may not know which will be their final change that determines the final amount of the order. In this case, the following two options are available.[62]

- Option 1 - Re-authenticate every time the cardholder adds to the basket
- Option 2 - Authenticate at checkout for a highest estimated amount

These options are defined in detail in section 5.5

4.2.2.5 Impacts for Issuers

Issuers are not expected to be aware of whether the final amount of a transaction is known at the time of authentication or authorization, however bearing in the mind the difference in approach between UK and EEA regulators described in the section 4.2.2.3 above they should note the following:

- UK and EEA Issuers should not decline or respond to CIT authorization requests with an SCA decline code (Response Code 1A) purely on the basis that there is not a character for character match between merchant names or merchant/Acquirer IDs submitted at authentication and authorization, so long as the name is clearly recognizable as being the same merchant.
- UK Issuers should not decline or respond to a CIT authorization requests with an SCA decline code (Response Code 1A) purely on the basis that the authorization amount is less than or more than the authenticated amount so long as any increase above the authentication amount does not exceed 20%
    - UK Issuers should note however that under Visa rules, they bear liability for any amount up to 15% above the authenticated amount. Liability protection is not available to merchants if the authorization amount is between 15% and 20% of the authenticated amount. Given this, it is down to the Issuer to decide

[62] For both option 1 and 2, remember however that if at fulfilment the amount varies due to circumstances not initiated by the cardholder, the authorization cannot be processed for a higher amount than what was authenticated. See procedures described for those scenarios in section 4.2.2.4.1.

whether to decline transactions where the final amount exceeds 15% of the authenticated amount.

- EEA Issuers should respond to any CIT acquired from within the EEA with an SCA decline code (Response Code 1A) if the authorization amount exceeds the authentication amount, with the following caveat:
    - Issuers may find that for some EEA transactions the amount for which authorization is requested is marginally different from the amount authenticated (for example a few € Cents). In this case the Issuer may, entirely at their own discretion, consider authorizing such transactions if they are confident that any marginal increase in amount is legitimate and not indicative of fraud. Issuers should consider balance between regulatory requirement and customer experience when taking this decision.
- EEA Issuers should note that the amount settled cannot exceed the amount authorized, however the settled amount may be lower than the authorized amount.
- UK and EEA Issuers should not respond with an SCA decline code (Response Code 1A) purely on the basis that the authorization amount is lower than the amount authenticated
- Merchants may use an MIT incremental to enable them to collect an incremental amount if the final value exceeds the amount initially authenticated. Issuers should not decline or respond with an SCA decline code (Response Code 1A) to MITs that have been correctly set up with a user agreement and authenticated CIT and are submitted with the correct indicators.

4.2.3 MITs, CITs, stored credentials and account verification transactions

In order to understand how to manage MITs in an SCA environment it is important to be familiar with some key concepts:

- **MITs** are transactions of a fixed or variable amount and fixed or variable interval, governed by an agreement between the cardholder and merchant that, once set up, allows the merchant to initiate subsequent payments from the card without any direct involvement of the cardholder. As the cardholder is not present when an MIT is performed, cardholder authentication is not possible. A transaction can only be an MIT if the user is not available to (I) initiate; or (II) authenticate. If they are available to do either of those things at the point of interaction (irrespective of when the transaction is processed), then it is not an MIT. See section 3.8.1.3 for a full definition of an MIT.
- **A cardholder-initiated transaction (CIT)** is any transaction that is not an MIT as defined in section 3.8.1.3, and includes any transaction where the cardholder is available to initiate or authenticate the transaction at the point of interaction. Authentication is required for all CITs, unless the transaction qualifies for an exemption or is otherwise out of scope of SCA.
- **A stored credential (**also referred to as "card on file" or "credential on file" by the industry and in this guide) is what Visa defines as information (including, but not limited to, an account number or payment token) that is stored by a merchant or its agent, a payment facilitator, or a staged digital wallet operator to process future

transactions. Visa has introduced a Stored Credential Framework to govern the use of stored credentials. More details are included in Appendix A.1. Processing a transaction with a stored credential does not automatically qualify the transaction as out of scope or exempt from SCA. Many CITs use stored credentials and are in scope of SCA. For example, so-called "one-click" transactions, or transactions initiated through apps used for booking ride sharing or cycle hire services, fuel purchases etc., that use stored credentials do not qualify as MITs. The type of credential used does not factor in the criteria to determine whether a transaction is in or out of scope. Refer to section 2.3 to see the criteria that may qualify the transaction as out of scope. Each transaction must be evaluated according to its circumstances to determine if SCA is required, whether it is out of scope or, if it is in scope, whether it qualifies for an exemption (see section 2.2).

- **Account verification transactions** are authorization requests initiated by merchants for zero value in order to verify a cardholder's account. Whether an account verification transaction requires SCA or not depends on the use case. Descriptions of use cases and when SCA is required are given in section 4.8.3.2. Acquirers are expected to enable SCA when it is required.

Key Point

Some types of MIT transaction can be performed without using a stored payment credential.

Processing a transaction with a stored credential does not qualify a transaction as out of scope or exempt of SCA. Many CITs use stored credentials and are in scope of SCA. Each transaction must be evaluated according to its own circumstances to determine if SCA is required.

4.2.3.1 Indicators for transactions with stored credentials

The following summarises the indicators that merchants should set to correctly identify transactions using stored credentials (credential or card on file).

Transactions processed with a Credential on file are indicated with a POS entry mode of "10" in Field 22 (POS Entry Mode).

When storing the credential on file for the first time, the value "C" must be used in Field 126.13 (POS Environment) of the authorization request, but this value can also be used for other use cases. Usage of the value "C" in Field 126.13 (POS Environment) must be used as follows:

1. Putting a Credential on File for use in future CITs. An example is the use of a Credential on File to enable a so called "one-click" checkout experience where the stored credential is used so that the cardholder does not have to re-enter their card details. Merchants should note the following:
    - The value "C" is needed only once when putting the credential on file. It is not necessary to set the value for subsequent CITs using the credential.
    - Future CITs using this this stored credential will use the POS entry mode 10 (no value "C")

2. Unscheduled Credential on File (UCOF) MITs to collect payments for a usage based subscription (a variable interval – as opposed to a fixed interval "recurring" type subscription)
    - The value "C" is needed in both the CIT setting up the MIT and in the subsequent UCOF MITs used to collect the payments

The use of indicators and the SCA requirements for these use cases is summarised in Table 18 below:

Table 18 Indicators and SCA requirements for Credential on File transactions

Use Case	Transaction Type	Visa MIT Framework		POS Entry Mode (F22)	SCA requirement
		POS Env (F126.13)	Original Tran ID (F125)[63]		
1a) Putting credential on file for use in future CITs	CIT	C	N/A	01 (Manual Key Entry)	Required if risk of fraud subject to each Issuer's risk policy[64]
1b) CIT Transaction using previously stored credential	CIT	N/A[65]	N/A	10	Required unless the transaction is out of scope or qualifies for an exemption
2a) Setting up an MIT UCOF	CIT	C	N/A	Any Valid[66]	Required when set up in a remote channel
2b) Subsequent MIT UCOF	MIT	C	Tran ID of initial CIT, or of previous MIT, or Interim Tran ID	10	Not required so long as SCA was applied at MIT set up[67]

[63] Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that elect to receive Field 125.
[64] It is legitimate to consider there is no risk of fraud when a card is added without a financial transaction (i.e. during an account verification/zero currency unit transaction), however some Issuers, especially in some markets, consider there is a risk even during a non financial transaction and therefore require SCA.
[65] The value "C" must not be present when the credential is already on file. It is the value 10 in F22 that indicates the credential used is stored.
[66] 10 if credential is already on file, 01 if was not and is entered by the cardholder during this transaction, or appropriate Face to Face POS entry mode if the CIT is a Face to Face transaction.
[67] See section 3.8.1.3 for details of limited exceptions to the requirement to apply SCA when setting up an MIT.

4.2.4 Reauthorizations

There are a number of payment scenarios where one or more authorizations take place when the cardholder is no longer present to complete a previously authenticated/exempted transaction, for example in the case of:

- A delayed authorization[68] that takes place some time after checkout/authentication when the customer is no longer available; or
- Multiple authorizations processed for a single checkout/order, one for each individual shipment or item of the order

These transactions must be processed as MITs in the Visa system as the cardholder is no longer present to be authenticated. The correct MIT type to use is "Reauthorization". These transactions processed via Reauthorization MITs are not MITs for regulatory purposes as they represent the completion of a CIT that could not be fully completed at time of checkout.

As such, exemptions can be used in the associated CIT if the CIT qualifies for the application of an exemption (see section 3.8.3.2 for more information). If an exemption is to be used, it can only be used via EMV 3DS as the Issuer must be made aware of the full amount of the transaction when deciding whether to agree to the exemption or not, which would not be possible in the initial authorization CIT as the full amount is not processed at that time. A CAVV must be submitted with either the initial CIT authorization and/or the subsequent MIT reauthorization(s). The merchant has options for when the CAVV is submitted depending on whether the initial transaction is just an account verification or is used to collect part payment and whether the merchant wishes to benefit from fraud liability protection.

If no exemption is used and the transaction is fully authenticated, liability protection applies but for that the CAVV must be submitted with the MIT.

The following three step process must be applied to process MIT Reauthorizations:

- The initial CIT must first be routed via EMV 3DS : The full purchase amount must first be routed via EMV 3DS for Issuers to either fully authenticate or agree/apply the exemption against the full amount.[69]
- An authorization must be processed as a CIT at checkout either to authorize a partial payment collected at checkout and/or to set up subsequent Reauthorization MIT(s) – this is referred to as authorization Step A
- At shipment, a Reauthorization MIT(s) must be processed to authorize the collection of payment(s) due. This is referred to as authorization Step B

Given all the above principles, the following applies to the CIT at authorization Step A:

---

[68] Does not include and should not be confused with i) a deferred authorization which cannot be submitted at the time of transaction processing due to a lack of connectivity, system failure or other technical issue (refer to section 3.2.5.3 for more details) or ii) delayed charges which are typically used in hotel, cruise lines and vehicle rental payment scenarios to collect a supplemental account charge after original services are rendered and correspond to a specific MIT type (see table 13).

[69] Except for token transactions with enhanced TAVV: Transactions do not need to be routed via EMV 3DS if an enhanced TAVV is available. If there is no enhanced TAVV and the transaction qualifies for an exemption, if or SCA is required, token transactions will need to be routed via EMV 3DS.

- If partial payment is due at check-out, an authorization must be submitted only for the amount due:
    - A CAVV is required in this CIT as even if exemptions are used, they can only be requested via EMV 3DS
    - If an exemption is used, the exemption indicator must be present in the CIT (but should not be used in the subsequent MIT)
- If no payment is due, the CIT must be processed as an account verification:
    - Submission of a CAVV with an account verification CIT authorization request is optional. The CAVV can either be submitted in the account verification or stored to provide liability protection for the MIT
    - If the CAVV is associated with an ECI 07, it is recommended that it is submitted with the CIT authorization, rather than with the Reauthorization MIT
- The merchant must store the Tran ID of the CIT to be submitted with future Reauthorization MITs
- The authentication data defined in Table 36 section 5.1.2 must be provided in the CIT authorization request

The following applies to the Reauthorisation MIT(s) at authorization step B

- The merchant must submit the delayed/multiple authorization(s) with Message Reason Code (MRC) 3903 and the Tran ID of the original CIT
- As it is indicated as an MIT and out of scope as authentication was applied to the initial CIT, Issuers cannot request SCA. Submission of the CAVV with the MIT authorization request is:
    - Optional if already submitted in the associated CIT
    - Required if not previously submitted in the associated CIT

  The submission of the CAVV in the MIT is to qualify the transaction for liability protection when applicable.

  If the CAVV has already been used in the CIT, or if more than one CAVV is needed due to multiple MITs, new CAVV(s) should be obtained as appropriate via the EMV 3DS 3RI functionality[70].
- The authentication data that may/must be submitted with the authorization request is summarised in Table 38

[70] If 3RI is not yet available, the original CAVV may be used as an interim up to a maximum of five times – note that liability protection is in this case limited to the 90 days validity of the CAVV. Also note that this interim arrangement can only be applied until 18 October 2024.

4.2.5 Principles for implementing SCA

Irrespective of the business processes that a merchant uses for e-commerce transactions, there are some fundamental principles that shape the approach a merchant takes to performing an authorization. These principles are summarized below and are the basis for the approach in handling each of the different scenarios in Section 5, and in the addendum to this guide *Implementing Strong Customer Authentication (SCA) for Travel and Hospitality*.

4.2.5.1 Out of Scope transactions

Where a merchant/Acquirer is able to identify a payment transaction as out of scope of SCA, then the merchant / Acquirer must submit an authorization ensuring that appropriate information is present that allows the Issuer to recognize that the transaction is out of scope of SCA. For example, by including relevant MIT indicators, or properly flagging as MOTO. For details of the correct indicators please see Section 3.2.9 and Table 40 in section 5.12.2.

4.2.5.2 Visa principles for implementing SCA

4.2.5.2.1 Implementing SCA in common payment use cases

The following Table 19 summarizes Visa's guiding principles for implementing SCA in common payment use cases for both CIT and MIT transaction.

Table 19: Summary of common CIT and MIT payment use cases

Transaction Type	Use Cases	Recommendation for SCA?
Cardholder Initiated	One-time purchase (with/without Credential-on-File)	Yes, but exemptions allowed
	Cardholder adds to an open/ uncompleted order	The card holder is initiating and available to authenticate the transaction, so SCA is required unless the transaction qualifies for an exemption. Refer to section 4.2.2.4.3 for more information.
	Establish agreement for ongoing (e.g. subscription) or one-off future payments (e.g. No Show)	SCA is required in most cases when the initial mandate is set up via a remote electronic channel[71]
Merchant Initiated	Executes payment (e.g. subscriptions, No Show, incremental)	Out of scope. SCA is required in most cases when the initial mandate is set up via a remote electronic channel but is not necessary for subsequent payments initiated by the merchant

[71] This does not apply in some specific cases outlined in Section 3.8 where the MIT field indicates transactions which are not out of scope but where SCA has already been performed or an exemption was applied before the transaction is executed – e.g. Reauthorization (used in delayed or split authorizations) and Resubmission (resubmitted transit transactions).

Transaction Type	Use Cases	Recommendation for SCA?
	Merchant updates payment terms (e.g. change payment date, price change)	Not required assuming this is addressed through T&Cs and other cardholder communications
	Original purchase delayed or split into subsequent events with or without price changes (e.g. basket updates)	Not required as long as the original transaction was an authenticated or exempted authorization
	Merchant initiated variation to an existing order when customer is not available. (e.g. substitution of unavailable items or change to shipping costs)	Options to enable merchants to process transactions for which the final amount is unknown without the need to authenticate are summarised for various payment use cases in section 4.2.2.4.

4.2.5.2.2 Implementing SCA in common non-payment scenarios

The following Table 20 summarizes Visa's guiding principles for implementing SCA in common non-payment use cases.

Table 20: Summary of common non-payment scenarios.

Action	Use Cases	Recommendation for SCA Requirement
Loading of Credentials	Adding a Credential-on-File	SCA required if there is a risk of fraud. • It is legitimate to consider there is no risk of fraud when added without a financial transaction but the risk assessment will depend on individual Issuer's inherent risk policies. Therefore, if SCA is not applied, merchants must be ready to receive an SCA decline requiring the transaction is resubmitted with SCA.
	Provisioning of a token	SCA Is required in the case when the token is issued in a remote scenario and bound to the device and the cardholder's identity with participation of the payer and PSP. Could be required when a token is being provisioned for other scenarios.

	Merchant received updated payment credentials from the Issuer (e.g. Visa Account Updater, Visa Token Service)	SCA not required, but under Visa Rules must be addressed through T&Cs and other cardholder communications.
	Cardholder provides a new expiry date without any change to the card number	Not required.
	Cardholder has a payment agreement with a merchant and adds a new card number to the payment instructions	SCA is required when the initial mandate is set up via a remote electronic channel.
Card Validity Check	Check validity of PAN and expiry date using an Account Verification transaction.	Not required when used only to check validity.
Trusted Beneficiary	A merchant will send in an enrollment request to the Issuer to be added to a cardholder's trusted beneficiaries list	SCA required on the enrollment.
Delegated Authentication	Carrying out initial cardholder verification used to enable subsequent delegated authentication	SCA required

4.2.5.3 Visa authentication, authorization and clearing principles for implementing SCA

Table 21 summarizes key principles that should be applied to the authentication and authorization and clearing processes.

Table 21: Fundamental Visa authentication, authorization and clearing principles for implementing SCA

Principle	Rationale
Visa Authentication Principles	
1. **CAVVs cannot be stored after usage.**	As per Visa Rules, the same CAVV can only be used for a maximum of two occasions[72]; however, PCI requirements dictate that it cannot be stored post authorization. This means that a merchant can only use the same CAVV for up to two authorizations, if they are in short succession (e.g. populating two authorization requests at the same time).
2. **CAVVs prove that the authentication process has taken place.**	If an Acquirer SCA exemption is being exercised, the merchant may still submit a CAVV to prove the authentication process has been performed to avoid receipt of an SCA decline code. The CAVV must always be submitted with the associated ECI value. Visa Rules determine that where no Acquirer SCA exemption has been applied, merchants only receive fraud liability protection for authorizations submitted with a CAVV and an ECI value 05 (indicating authentication performed) or 06 (indicating authentication was attempted but not performed). When an exemption has been applied, the ECI value is generally 07 (indicating SCA was not performed or attempted) and fraud liability protection under the Visa Rules is not applicable. For more information see Table 23 in section 4.4
3. **3RI (3DS Requestor Initiated Message) must be used by merchants wishing to have fraud liability protection when more than one transaction is required to complete a single purchase.**	Issuers will be enabling 3RI in EMV 3DS 2.1 and it will be an integral feature within EMV 3DS 2.2. This enables merchants to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions previously authenticated. The feature can be used to enable merchants to effectively manage some payment use cases by for example[73]:

[72] Visa has temporarily permitted, under waiver, the reuse of the CAVV up to five times for split shipment scenarios and scenarios where transactions are associated with indirect bookings via booking agents. The previous waiver expired on 1 September 2020 and Visa has now extended it to 18 October 2024 and to Merchant Servicers authenticating on behalf of other merchants. For more information please see VBN Article ID: AI12280 *New Rules and Updated Guidance to Support Transaction Processing in Line with SCA Requirements in the EEA and UK.*

[73] Until 18 October 2024, instead of using 3RI for these use cases, merchants can use the initial CAVV up to five times.

Principle	Rationale
	• Allowing an authorized entity in a Multi-Party Commerce scenario (for example in the Travel & Entertainment industry) to request a CAVV on behalf of a merchant. • Allowing merchant to obtain a new CAVV in case of split or delayed shipment when one or more item is not ready for shipment until a later date. • Requesting a new CAVV to maintain liability protection when authorization is sought more than 90 days after a transaction has been authenticated. The merchant needs to send prior authentication information and original ACS Transaction ID when submitting a 3RI transaction. A CAVV obtained under 3RI should be processed under the same rules as a CAVV obtained when the card holder was presented (e.g. cannot be stored after use, valid for fraud liability protection up to 90 days, etc.).
4. Token Transactions require a TAVV unless they are being submitted as MITs	Visa requires a TAVV to be present in all Token transactions unless the transaction is identified as a Merchant Initiated Transaction. Please refer to section 5.1.1 for more information.
Visa Authorization Principles	
5. SCA requirements apply to Tokens and PANs	Visa Tokens can be used in the place of PANs throughout the payments eco-system. Therefore, any merchant or Acquirer using Visa Tokens for financial transactions should use the same criteria for their SCA decisions as they use for PANs.
6. An MIT can only occur after an initial CIT has been performed to establish a customer agreement	SCA is not required for an MIT so long as SCA was applied during the initial mandate (CIT) set up when set up was taking place in a remote channel. In Visa's view SCA is not required for the CIT in the following cases when an exemption can be applied: • The CIT is split or delayed • The CIT is resubmitted in the case of contactless transit transactions • The CIT qualifies for the secure corporate payments exemption • The CIT is a proximity (face to face) contactless transaction and the total combined value of the CIT, and any associated incremental transaction is below the qualifying limit for application of the contactless exemption. If the combined value exceeds the contactless exemption limit, SCA is requiredSee section 3.8.1.3 for more information on why SCA is not required for incremental MITs set up via

Principle	Rationale
	contactless CITs that qualify for the contactless exemption.[74] In Visa's view, SCA is also not required when the mandate is set up via MOTO.
7. MITs must be properly indicated as MITs to ensure they are treated as out of scope of SCA	If a merchant initiates an MIT, the transaction is out of scope of SCA and Issuers must be able to recognize it as an MIT. In the Visa system, this is done by the merchant/Acquirer adding the MIT indicators to any MIT. When receiving transactions that are properly indicated as MITs using the MIT Framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02). This enables Issuers to recognize a transaction as an MIT (and therefore out of scope of SCA) by simply checking for the value of "1" in that tag. Issuers can also recognize transaction as MITs using the indicators from the Visa MIT Framework.
8. Merchants need to store the Transaction ID of the CIT (or of a previous MIT for 3 of the MIT types as defined in section 3.8.2.1) that established the agreement for future MITs.	An MIT must reference the transaction during which the MIT was set up by either including the Transaction ID of the original CIT (or the Transaction ID of a previous MIT - applicable only to certain types of MIT) in the authorization message. Therefore, merchants who might perform MITs need to store the Transaction ID of their associated CIT (or a previous MIT) until no further MITs are required and any agreement with the customer is complete.
9. Merchants should only request authorization when the goods are available and ready to be shipped	A merchant must not clear a transaction before goods have been shipped (as per Visa Rule # 0002981). In addition, merchants should only request authorization when they have confirmed that the goods are available and ready to be shipped. This minimizes the impact to the customer's open to buy and ensures that the CAVV is not used ineffectually.
10. Authorizations are valid for a maximum of up to 7 days	If an authorization cannot be fully cleared after 7 calendar days[75] have elapsed, the merchant must submit a reversal for the un-cleared amount. If the transaction can subsequently be fulfilled, the merchant must first perform a re-authorization (or several if shipment is split). In the PSD2 context, these re-authorizations must be performed with MIT re-authorization indicators to ensure authentication does not need to be performed again unnecessarily.

[74] This is for scenarios similar to the one described in section 5.8, but where the entry is facilitated via a card present tap/chip insert rather than app based.

[75] Different authorization validity periods may apply to some merchants and transaction types, particularly in the T & E sector. For example, mass transit transaction approvals are only valid for 3 calendar days. Refer to Visa rule ID #0029524 for more information.

Principle	Rationale
11. Merchants must perform an additional account verification and address CAVV expiry if a transaction is delayed by more than 90 days	Merchants should avoid being in the position of delaying authorization for more than 90 days. If a merchant cannot avoid being in a position of a greater than 90-day delay, it needs to obtain a new transaction ID for usage in a delayed authorization to ensure that the transaction meets Visa processing requirements, as if the transaction was done with a token, it will no longer be valid. As such, the merchant should perform a new account verification and the Transaction ID of this account verification must be stored for use in the delayed authorization. If a token is used, this new account verification will require a new TAVV. In addition, as per Visa Rules, the CAVV offers fraud liability protection for only the first 90 days after its creation. If needed, it can still be used past 90 days, albeit, without fraud liability protection[72]. For delays over 90 days: • A merchant wishing to receive fraud liability protection must first use 3RI (if available) to obtain a new CAVV (with ECI 05) for the relevant amount to include in the authorization. • If 3RI is not available or the merchant wishes to proceed without fraud liability protection, the merchant may submit a CAVV (and its associated value of 05) that is older than 90 days, but less than 6 months old, but Issuers will still have dispute rights. The benefit for the merchant is that including a valid CAVV should prevent the Issuer declining with an SCA decline code [76]. If the original CAVV was obtained using an Acquirer exemption (i.e. has an associated value of 07) – there is no need to use 3RI to obtain a new CAVV, as fraud liability protection does not apply.
12. When an authorization must be delayed until some time after checkout, at a point when the cardholder is no longer available, the merchant must always: **a. Perform an account verification and any required authentication at checkout** **b. Indicate the delayed authorization with appropriate indicators, such that the Issuer**	There are a number of payment scenarios where one or more authorizations take place when the cardholder is no longer present to complete a previously authenticated/exempted transaction, for example in the case of : • A delayed authorization that takes place some time after checkout/authentication when the customer is no longer available; or • Multiple authorizations processed for a single checkout/order, one for each individual shipment or item of the order These transactions must be processed as MITs in the Visa system as the cardholder is no longer present to be authenticated. The correct MIT type to use is "Reauthorization". These transactions must be processed

[76] A merchant should not submit a CAVV older than 6 months and should note that a CAVV older than one year will fail validation.

Principle	Rationale
knows that the cardholder is not available for authentication	according to the principles defined in section 4.2.4 and the practical guidance on the provision of authentication data and submission of CAVVs with the authorization requests given in section 5.1.3.
13. In the EEA, the amount authorized and cleared can be lower than the authenticated amount but not higher. In the UK, the final amount authorized may be higher than the amount authenticated subject to the "allowable increased final amount", however the amount cleared must be lower or equal to the amount authorized.	Dynamic Linking requires that the transaction amount and the identity of the payee at authentication must be included in the authentication code (CAVV). The EBA has stated that for EEA transactions, the final amount cannot increase above the authenticated amount without further authentication, although in the UK the FCA has determined that the final amount may increase within the customer's reasonable expectations up to a maximum of 20% so long as the customer has been advised that it may increase. The same does not apply where the final, authorized amount is lower than the authenticated amount. In these cases, no re-authentication is required. As a result, Visa eliminated the existing authorization tolerance limits that allow e-commerce and tipping merchants to clear an amount greater than the authorized amount for EEA acquired merchants (still allowed for UK acquired merchants). Under Visa rules, Issuers bear liability for any amount up to 15% above the authenticated amount. Liability protection is not available to merchants for the proportion of any additional amount that exceeds 15% of the authenticated amount in the case that the authorization amount is between 15% and 20% of the authenticated amount. Given this, it is down to the Issuer to decide whether to decline transactions where the final amount exceeds 15% of the authenticated amount. As a result, merchants may choose not to submit transactions to authorization without reauthentication where the final amount is greater than 15% above the originally authenticated amount. For guidance on options for dealing with variations in amount please see section 4.2.2.3
14. Issuers must not respond to the authorization request for out of scope transactions with an SCA decline code (1A)	An Issuer must not use an SCA decline code for transactions deemed out of scope from a regulatory perspective or ask for authentication in response to authorization requests for transactions legitimately identified as out of scope (MITs, MOTO One-Leg-Out or transactions performed with an anonymous payment instrument). In the case of MITs, the cardholder is not available for authentication, therefore it is essential that merchants use the MIT framework to enable Issuers to identify MITs where the cardholder is not available.

Principle	Rationale
15. Grandfathering can be applied to MITs performed based on agreements made prior to the regulatory enforcement date	A merchant with an existing agreement with a customer established prior to the regulatory enforcement date does not need to establish a new agreement with their customer with SCA. Instead, all MIT authorizations performed after the enforcement date can reference either the "initial" CIT, or the transaction ID of any previous related transaction processed before the enforcement date (CIT or MIT). The transaction ID of the selected transaction must be stored and always included in future related MITs as evidence of an existing agreement with the customer. The selected transaction does not need to meet SCA requirements (e.g. it does not need to have had a CAVV) given that it was performed prior to the enforcement date. For example: • In an established **subscription**, the transaction ID of any previous MIT of the series can be used. For transactions described under the MIT framework as Industry Specific Business Practices, the transaction ID of the previous CIT can be used, even if it wasn't authenticated, provided it was performed prior to the enforcement date.

16. When setting up an agreement to process future MITs (except for MIT reauthorizations), only authenticate and authorize for amount needed on the day of the agreement	When setting up an agreement (e.g. a magazine subscription), the merchant must clearly disclose the amounts that will be collected and when along with other associated terms (refer to section 5.12) but should only authenticate and authorize for the amount due immediately. For example:
	• For subscriptions (recurring and unscheduled credential on file (UCOF) transactions in the Visa system):
	  • If the first monthly payment is 5 Euros, authenticate and authorize for 5 Euros
	  • If a free trial period applies, authenticate and authorize for zero amount
	  • If the first payment is a reduced promotion amount of 2 Euros, rising to 5 Euros after 3 months, authenticate and authorize for 2 Euros.
	• For installment/prepayments:
	  • If the first installment/deposit is not due at the time of the agreement, authenticate and authorize for zero amount,
	  • If the first installment/deposit is due at the time of the agreement, authenticate and authorize for that amount.
	  • No amount should be authenticated or authorized in the case where an agreement includes an allowance for conditional future charges using other Industry Specific MITs such as "No Show", Incremental or Delayed Charges. For example, if booking a hotel with no deposit required, but with payment due in full in case of No Show,

Principle	Rationale
	authenticate and authorize for zero value at the time of booking. Reauthorizations MITs are exceptions to these principles: When processed for open orders and aggregated payments it is possible for the merchant to authenticate the transaction for a maximum estimated amount that the basket order can have. When processed for split/delayed shipment, the authentication must be done for the full amount of the order whereas the authorization must be done only for the amount due at time of the order (subsequent amounts to make up the full order will be processed with MIT reauthorizations)
17. If an exemption is indicated in EMV 3DS, the exemption indicator must also be present in the authorization request	If a merchant would like to indicate in EMV 3DS that an Acquirer exemption is to be applied, or that an Issuer exemption should be considered (for SCP and trusted beneficiaries), the appropriate exemption indicator should be set in the Transaction Challenge Exemption field of the Authentication Request. Merchants should note that when they indicate an exemption through EMV 3DS they must still include the corresponding exemption indicator in the subsequent authorization request.
Visa Clearing Principles	
18. Multiple clearing records can be submitted for a single authorization	This principle can be applied when an order cannot be fulfilled in a single shipment. It is Visa's recommended best practice to handle multiple shipments via multiple clearing records rather than via multiple authorizations. Because a CAVV is not included in clearing, submitting multiple clearing records to fulfil a single authorization does not impact merchant fraud liability.

4.2.6 Who can apply exemptions?

Under the regulation, the application of exemptions is restricted to regulated PSPs, however merchants may also play an active role. They may, for example, work with their Acquirer to apply the TRA exemption, indicate that they would like Issuers to apply the trusted beneficiaries exemption or may indicate to Issuers that a transaction qualifies for the secure corporate payments exemption.

Table 22 below summarizes which PSP is able to apply which relevant exemption for remote card transactions according to the regulation.

Table 22: Summary of who may apply an exemption[77]

Exemption	Issuer	Acquirer
Trusted beneficiaries	Yes	No[i]
Transaction Risk Analysis (TRA)	Yes	Yes[ii]
Low Value Transactions	Yes	Yes[ii], [iii]
Secure corporate payment processes & protocols	Yes[iv]	No[v]

Notes:

i. Under the regulation, an Acquirer may not apply the trusted beneficiaries exemption, however EMV 3DS 2.2 allows for:

   - A cardholder to add a merchant in their Trusted List while completing an SCA authenticated transaction; and
   - A merchant to be advised by the cardholder's Issuer as to whether it is on a cardholder's list and, if so, to indicate to the Issuer that it would like the exemption to be applied.

ii. The Issuer always makes the ultimate decision on whether or not to accept or apply an exemption and may wish to apply SCA or decline the transaction.

iii. While the regulation allows for the Acquirer to apply the exemption, this is not practically feasible as the Acquirer does not have visibility of the velocity limits that apply to the exemption.

iv. Issuers who have demonstrated to NCAs that applicable processes and protocols meet the requirements of the regulation should apply the exemption when a transaction is received with the secure corporate exemption indicator.

v. Merchants who process transactions originating from within secure corporate environments may be able to indicate to their Acquirer that the SCP exemption may apply. The Acquirer may indicate to the Issuer using the secure corporate exemption indicator, that they consider the transaction qualifies for the secure corporate payments exemption. Secure corporate environments could for example, and subject to the view of NCAs, include corporate purchasing or travel management systems. For more information refer to the *PSD2 SCA Secure Corporate Payment Exemption Guide*.

Note that Visa does not provide any indicator for the recurring transactions exemption as the exemption is not used in the Visa system; Visa transactions that would use the recurring payments exemption are MITs and as such are out of scope of the SCA requirements entirely. Visa provides a way to indicate recurring payments as MITs.

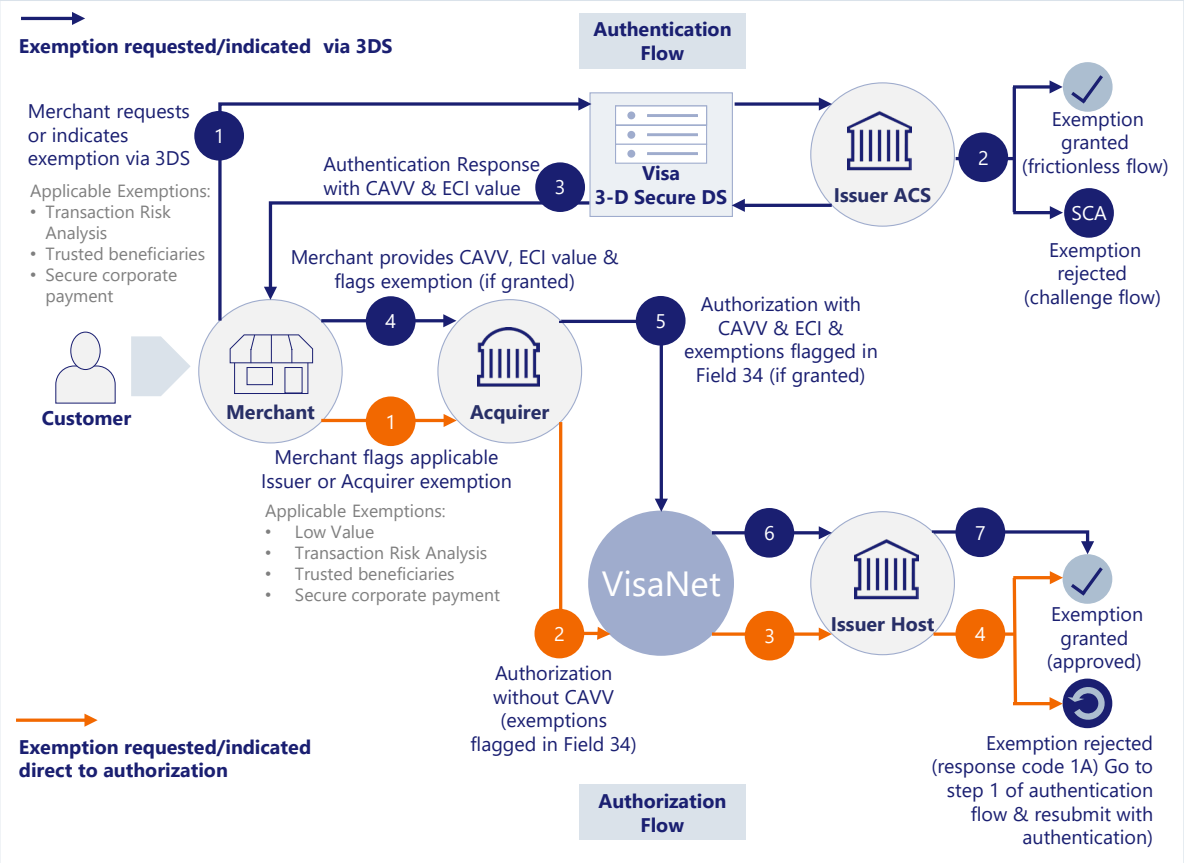
[77] Adapted from Table 2 in the EBA Opinion Paper on the Implementation of the RTS on SCA and CSC 13 June 2018.

4.2.7 Options for merchants & Acquirers regarding exemption application

If a payment transaction is in scope of SCA, then the merchant / Acquirer must determine whether an SCA exemption can be exercised or not.

A merchant / Acquirer can exercise an exemption via the EMV 3DS 2.2 authentication flow, or directly via a VisaNet Authorization, as shown in Figure 11 below:

Figure 11: Visa model to execute SCA exemptions



- **Exemption via EMV 3DS authentication:** The merchant can exercise an exemption via an EMV 3DS message first, before performing an authorization request. This is done by setting the relevant indicators in the EMV 3DS message and in the subsequent authorization. When merchants select EMV 3DS 2.2 to indicate Acquirer TRA (rather than submitting the transaction direct to authorization), data shows that this may facilitate a demonstrable increase in transaction success rate. For more information on the benefits of this approach refer to section 4.3.3.5. Merchants should be aware that if taking this approach, the exemption exercised during authentication, so long as it is accepted by the Issuer, must be re-stated in the authorization message along with the CAVV and ECI value received at the authentication step.
- **Exemption direct to authorization:** The merchant can go directly to authorization, flagging the exemption used in Field 34. The low value exemption can only be indicated by an Acquirer in the authorization flow as there is no associated EMV 3DS indicator. However, merchants considering this option should be aware that the Issuer can decline the exemption and request SCA. In the case where authorization is delayed

and the Issuer rejects the exemption, the cardholder will no longer be available to perform authentication. Acquirers/merchants should review market specific requirements before adopting this exemption option, since some markets may require exemptions to be raised via an authentication message first. For additional guidance, please refer to section 4.3

- **No exemption exercised:** The merchant can perform authentication and authorization without populating any exemption indicators in EMV 3DS and in authorization Field 34. If no exemption is indicated by the merchant or Acquirer, and the transaction is in scope of SCA, authentication must always be performed before submitting for authorization.

4.3 Step by step guide to SCA optimisation

4.3.1 Individual transaction decision flows

At the individual transaction level, merchants, Acquirers and Issuers move through a sequence of decision points to determine whether:

- The transaction is in or out of scope of SCA
- The transaction qualifies for an exemption
- Which qualifying exemption should be applied
- In the case of merchants/Acquirers, how the transaction should be routed, via EMV 3DS or direct to authorization

These decision points are summarized in Figures 12 and 13 below:

Figure 12: Key merchant/Acquirer decision points

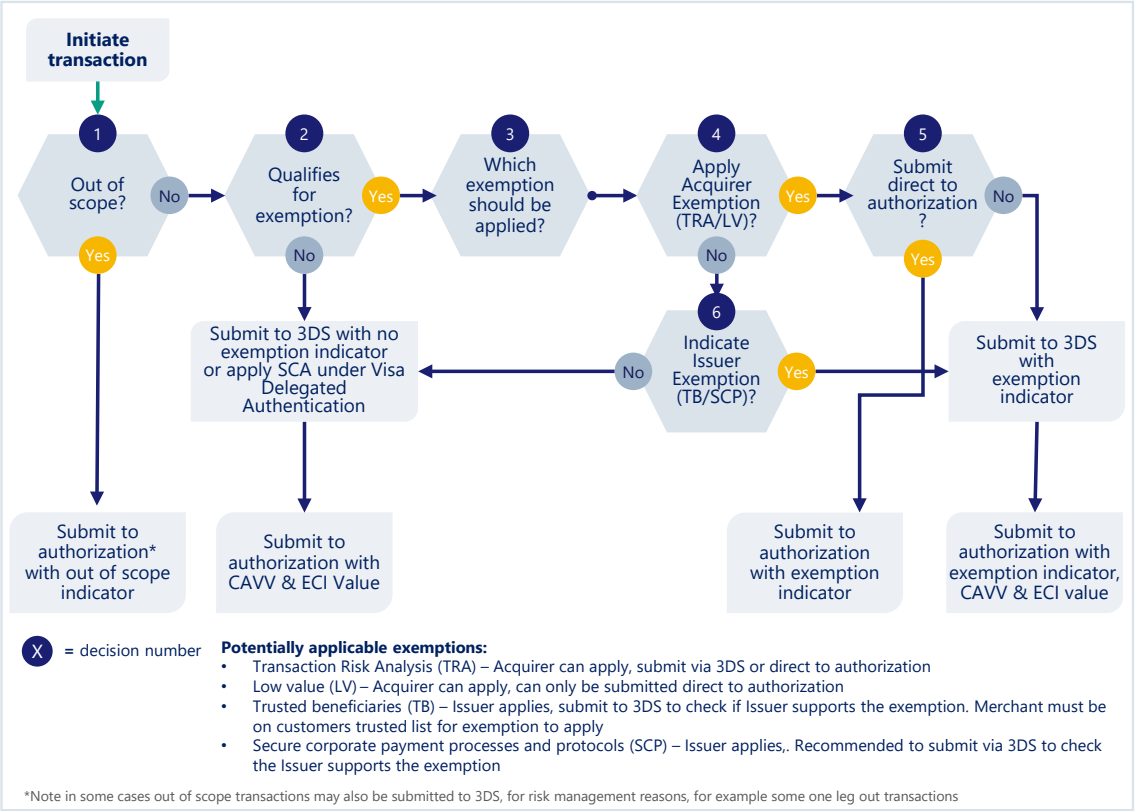
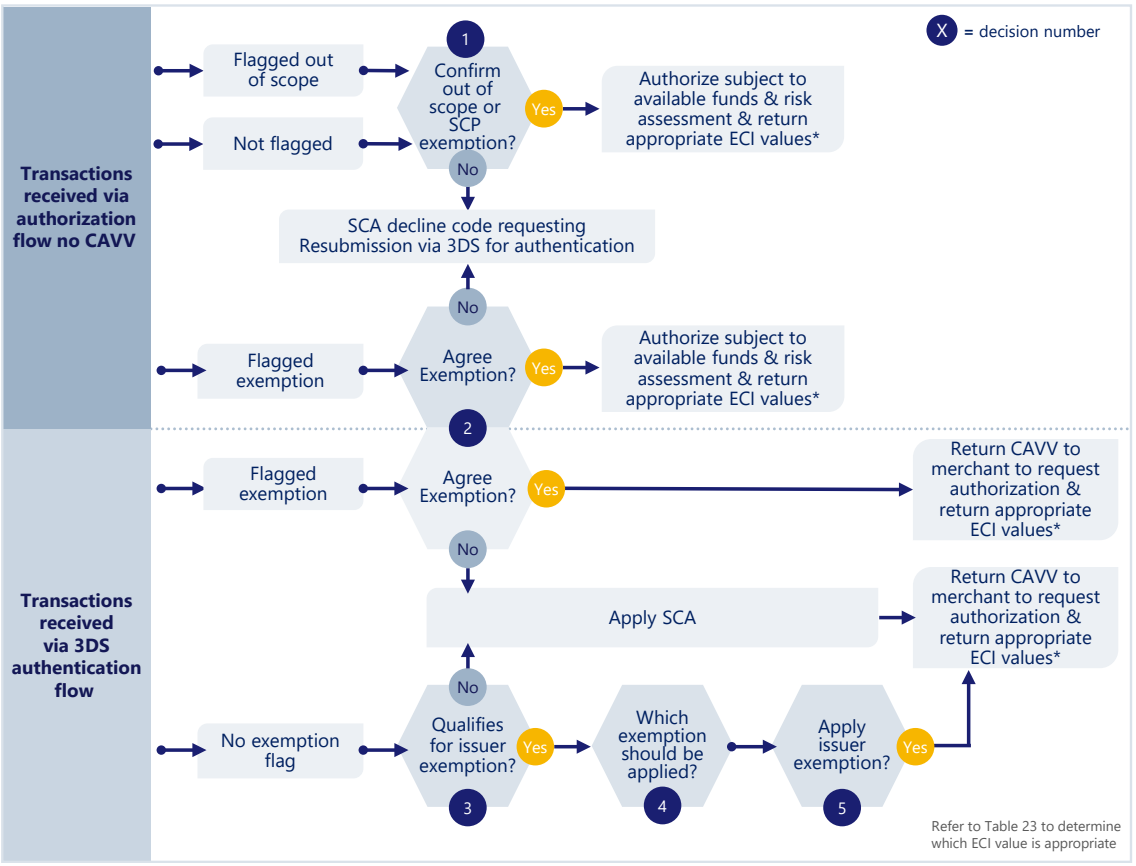


Figure 13: Key Issuer decision points



An overview of the considerations to take into account at each of these decision points is included in the following sections.

4.3.2 Key steps to minimising friction

There are a number of policy steps that merchants, Acquirers and Issuers can take to minimise any friction experienced by customers making remote electronic payments, while maintaining compliance with the SCA regulation. Reducing customer friction is essential to optimising customer experience and minimising transaction abandonment.

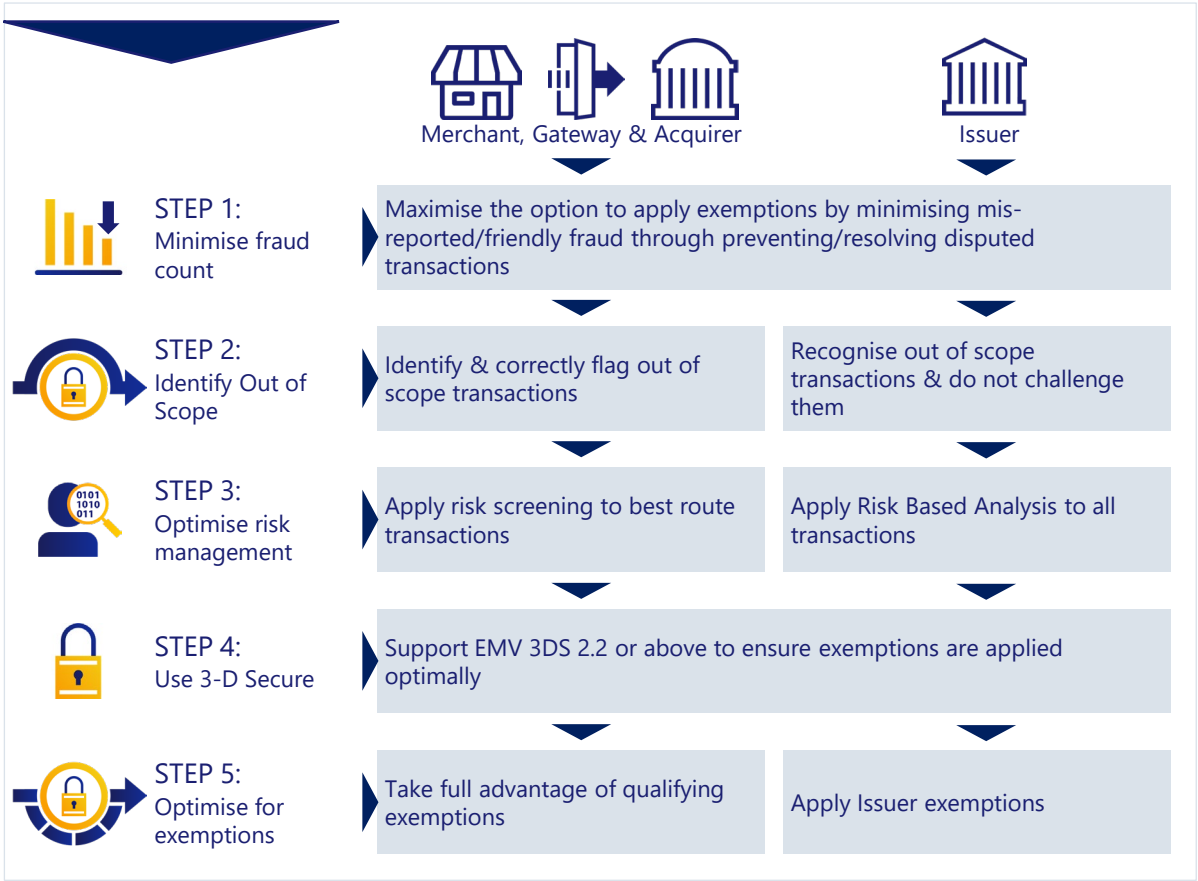
The steps that merchants, Acquirers and Issuers should take to minimise friction can be grouped into two clear stages:

- Stage 1: Minimising the need for SCA challenges
- Stage 2: Creating a challenge process offering minimal friction when SCA challenges are required

This section provides merchants, Acquirers and Issuers with guidance on Stage 1. See section 4.6 for guidance on Stage 2.

The key policy steps required to minimize the need for SCA challenges are summarised in Figure 14 below and the following sections. For more detail, please refer to the *PSD2 SCA Optimisation Best Practice Guide*:

Figure 14 Stage 1: Minimising the need for SCA challenges



4.3.3 Summary of the Steps

4.3.3.1 Step 1: Minimise fraud count

Disputes are often marked as fraud even when they are raised only because customers have trouble recognizing transactions and not because the transaction was unauthorised. Visa analysis indicates that fraud is reported 90% of the time a dispute is submitted[78].

Such disputes can artificially and unnecessarily inflate fraud counts, limiting the ability of Acquirers and Issuers to apply the TRA exemption and potentially limiting the ability of individual merchants to be considered for the application of certain exemptions[79].

Visa's experience has shown that a significant proportion of both disputes and transactions unnecessarily categorised as fraudulent can be avoided if customers and Issuers can be provided with additional information, such as the item purchased, to help customers validate transactions before they formally ask for a transaction to be disputed.

If merchants provide this information to Issuers it enables them to deal more effectively with customer queries, improving customer satisfaction and removing these transactions from the fraud count. This can potentially improve the risk score of every transaction a merchant processes, while increasing the ability of Acquirers and Issuers to apply the TRA exemption. Merchants can also benefit by reducing revenue losses from disputes, as well as increasing their ability to qualify for the application of key exemptions.

Verifi, a Visa company, offers a suite of related Pre-dispute Products to help both merchants and Issuers avoid and resolve such disputes. For more information see section 3.7.2.

4.3.3.2 Step 2: Identify and indicate out of scope transactions

Merchants who process out of scope transactions need to ensure that they can identify these transactions and populate the appropriate authorization indicators, as defined by their Acquirer. Note it is important that merchants check how their payment gateway/Acquirer would like them to identify MITs and other out of out of scope transactions. Some payment gateways/Acquirers use a proprietary standard for merchant indicators and then convert the indicators to the appropriate card scheme standard before submitting an authorization request.

Issuers must be able to recognise every type of out of scope transaction and must not decline or request authentication for transactions that have been indicated as out of scope by the Acquirer[80].

For more information on identifying out of scope transactions and other transactions that do not require SCA please refer to section 3.2.9.

4.3.3.3 Step 3: Optimise risk management

Visa recommends that merchants undertake risk screening on transactions before submitting them to authentication or authorization. Issuers are required to apply Risk Based Analysis (RBA)

---

[78] Source: Visa analysis from Visa Resolve Online statistics.

[79] Acquirers are more likely to consider applying exemptions to transactions from low fraud rate merchants.

[80] For more information please refer to *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom Visa Supplemental Requirements.*

to all transactions and will always take the final decision on whether to allow an exemption to be applied to a particular transaction when it is indicated by the merchant or Acquirer.

At its simplest level, RBA is based upon rules set by or in conjunction with the merchant to assess the risk of a transaction based upon simple characteristics of the transaction. More sophisticated solutions increasingly use machine learning based risk models and multiple datapoints to provide a much more accurate assessment of risk and minimise both fraud and false positives.

The approach taken by merchants will depend upon their size, resources and the risk profile of their business.

- Smaller merchants may choose by default to submit all of their transactions via EMV 3DS leaving the Issuer to risk assess them and decide which transactions qualify for exemptions. However, a merchant who applies no RBA or fraud screening risks a higher fraud rate, the application of fewer exemptions and higher customer friction. It is recommended that such merchants speak to their payment gateway, Acquirer or 3DS server provider to check what risk analysis and screening services they are able to offer.
- Larger and enterprise merchants should look to adopt more proactive strategies using more sophisticated risk tools to minimise fraud rates and take advantage of the ability to apply the Acquirer exemption and send transactions direct to authorization, to minimise the impact on customer experience and reduce authentication costs.

Merchants must align with their gateway/Acquirer to ensure that their SCA exemption strategy is supported.

Managing risk effectively will enable Issuers to maximise their ability to apply exemptions. Issuers should aim to implement risk strategies that balance the need to keep fraud low whilst at the same time avoiding the need to challenge every single transaction. In the case of the TRA exemption, keeping fraud rates within the reference fraud rate for the highest achievable transaction value band can be achieved by making full use of EMV 3DS data. For more information on Issuer application of RBA please refer to section 3.3.7.

4.3.3.4 Step 4: Use EMV 3DS

EMV 3DS is the leading industry standard solution being used across the card payments industry to apply SCA.

EMV 3DS 2.2, provides critical functionality that is fundamental to the optimisation of the application of SCA and all permitted exemptions. All Issuers are mandated to support EMV 3DS 2.2 and Acquirers are mandated to ensure their merchants are connected to vendors who support it.

Merchants must support EMV 3DS to facilitate the application of SCA and Visa strongly encourages merchants and Acquirers to support EMV 3DS 2.2 as early as possible.

For more information on EMV 3DS refer to section 3.3.

4.3.3.5 Step 5: Optimise use of exemptions

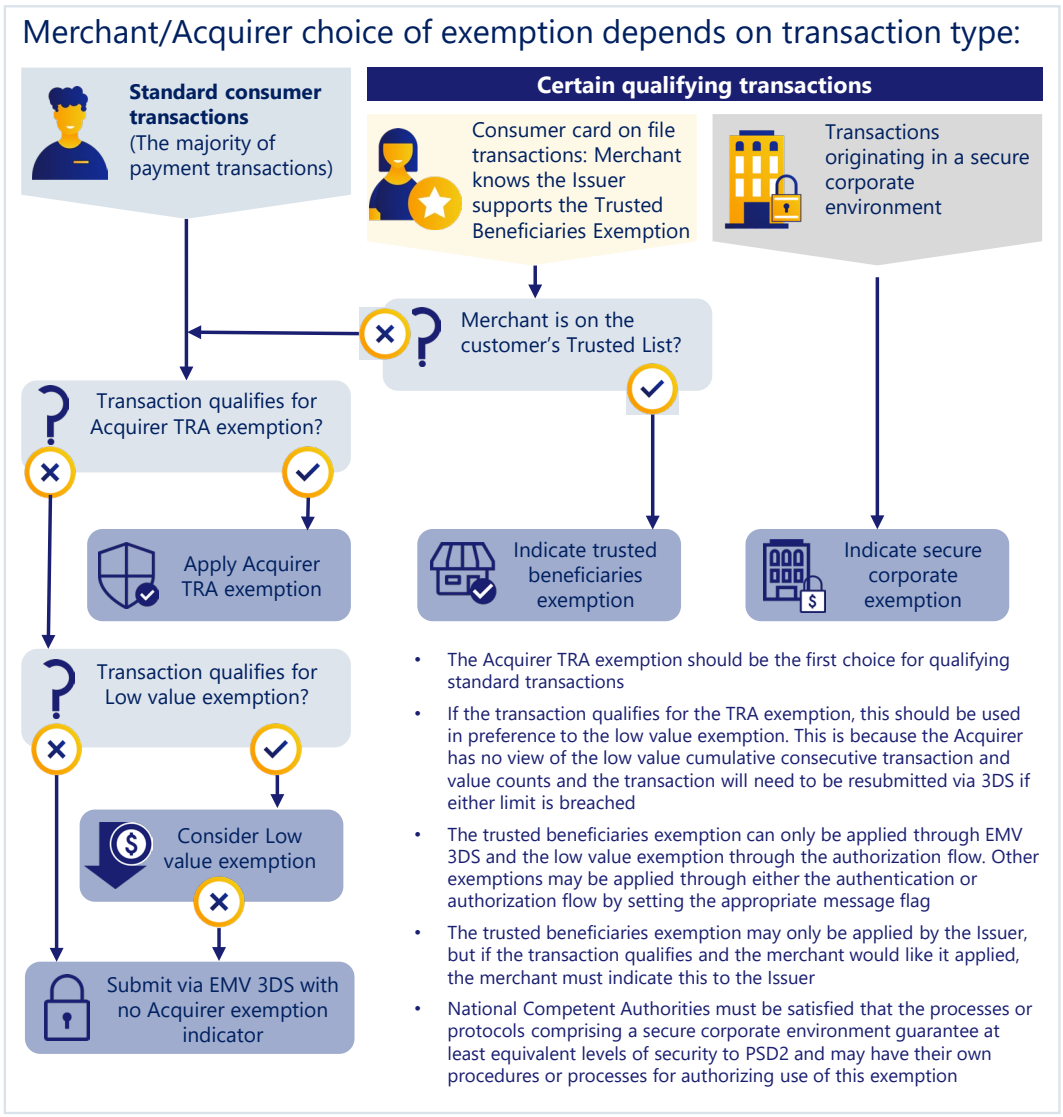
The logic shown in Figure 15 should help merchants and Acquirers to select which, if any, allowable exemption to apply or request.

Issuers may apply any of the exemptions.

Acquirers may, subject to transaction value and their fraud rate, apply either the TRA exemption or the low value transaction exemption. The EBA has confirmed that Issuers and Acquirers must take into account fraud on all transactions subject to SCA in the calculation of their fraud rate, regardless of which PSP took liability, for example by applying the TRA exemption. This may lead to Issuers being less likely to accept Acquirer TRA indicators as any fraud on these transactions will impact the Issuer's fraud rate. Fraud on transactions where the Issuer has applied a TRA exemption will also impact on the Acquirer's fraud rate. This reinforces the benefit for merchants to undertake risk screening of transactions before submitting them for authorization.

Merchants may indicate that they would like Issuers to apply the trusted beneficiaries exemption and may indicate to Issuers that a transaction qualifies for the secure corporate payments exemption. The order in which exemptions should be applied or requested by merchants and Acquirers depends upon the transaction type and whether the transaction qualifies.

Figure 15 Prioritisation of exemptions: merchant/Acquirer



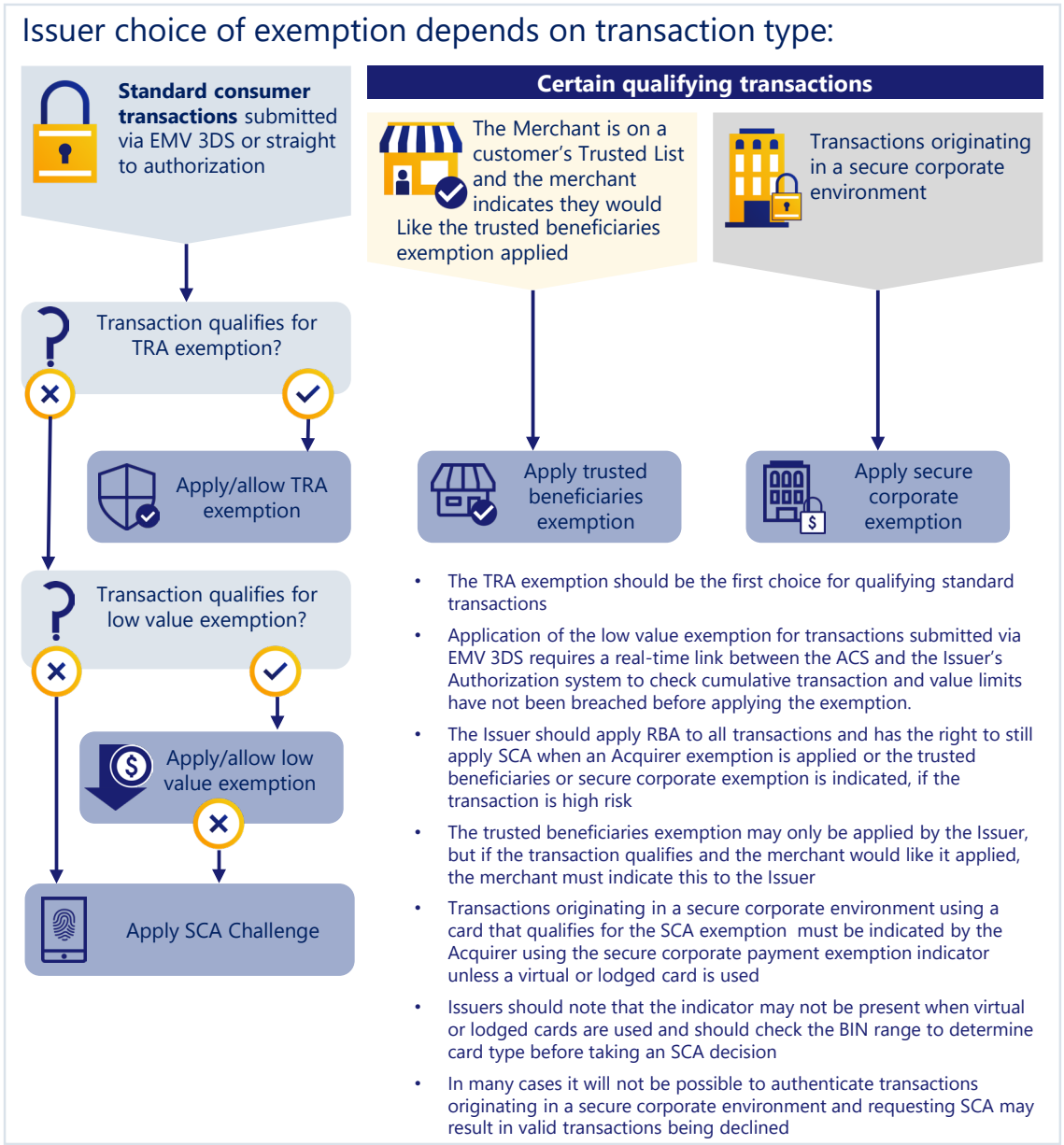
Merchants should note that only one exemption should be applied or indicated in a given transaction and that Issuers have the final say on whether an exemption can be applied and may choose to apply a challenge to a transaction indicated with an exemption indicator if they consider it to be high risk.

Issuers should apply risk analysis to all transactions and generally:

- When transactions are submitted by Acquirers with an exemption indicator (via EMV 3DS or direct to authorization), allow the exemption unless analysis indicates the risk is high
- When transactions are submitted by Acquirers via EMV 3DS without an exemption indicator, apply exemptions to all transactions that qualify

The most appropriate exemption will depend upon the transaction type and the qualifying criteria, as shown in Figure16:

Figure 16: Prioritisation of exemptions: Issuer



More information on the application of individual exemptions is included in Section 4.5 below.

Acquirer TRA-exempted transactions might be routed directly to authorization; however, Acquirer TRA via EMV 3DS usage is increasing and merchants can benefit from lower challenge rates, higher authorization and lower fraud rates by submitting Acquirer TRA exemption requests via EMV 3DS. At the time of publication of this guide, Visa has observed the following authentication, authorization and fraud performance trends at a macro level:

- The European challenge rate for Acquirer TRA exemption requests submitted via EMV 3DS is, at the time of publication of this guide, three times lower than the typical EMV 3DS observed challenge rate
- For the period from March 2022, Visa analysis indicated authorization approval rates between 1.5% and 3% higher for TRA-exempted transactions submitted via EMV 3DS vs. direct to authorization
- Fraud rates for EMV 3DS submitted TRA-exempted transactions have been at least half of those recorded for their direct to authorization equivalents

Merchants seeking to take advantage of the Acquirer TRA exemption are advised to consider submitting qualifying transactions via EMV 3DS and Acquirers are strongly advised to work with their low-risk merchants to review and adjust their management of Acquirer TRA-exempt transactions, to increase sales and reduce fraud through the use of EMV 3DS.

Merchants and Acquirers should also be aware that:

- Issuers may have less data on which to assess transactions sent directly to authorization than they would have for transactions submitted via EMV 3DS and they may therefore be more likely to request resubmission via EMV 3DS.
- The issuing of an SCA decline code and resubmission via EMV 3DS is likely to add latency to the processing of a transaction.
- If there is a delay between the cardholder initiating the transaction and authorization being requested and the Issuer requires resubmission via EMV 3DS, the cardholder may no longer be available to complete authentication resulting in a decline.

Acquirers must include an exemption indicator in the authorization request if they are submitting transactions under an Acquirer exemption or asking the Issuer to consider applying an Issuer exemption. In-scope transactions without exemption indicators or without having had SCA applied, should not be submitted direct to authorization [81] and are likely to receive an SCA decline code from the Issuer.

Acquirers should have policies in place on the risk profile of transactions that may be sent straight to authorization with exemption indicators set in order to provide merchants that qualify with the opportunity to take advantage of the facility while minimizing the risk of fraud and SCA decline code.

[81] Issuers are expected to decline transactions that are in scope of SCA but are submitted without SCA and without a correct indicator.

Merchants should consult their Acquirers to help determine under what circumstances it may be appropriate to submit transactions straight to authorization with an exemption indicator, in line with Acquirer policies.

Key Point

Acquirers must also ensure they pass any response code 1A (SCA required) on to their merchants rather than aggregating them with other generic decline codes such as "Do Not Honour" so merchants have visibility of the nature of decline and are able to respond to this particular message to re-submit the transaction

4.3.4 Guidance to Issuers on assessing transactions submitted direct to authorization

Issuers should have policies in place on risk assessing transactions that are sent straight to authorization with or without exemption indicators set. These should aim to minimize the unnecessary application of an SCA decline code while staying in line with the Issuers risk management policy and the requirement to decline or "soft decline" (by using an SCA decline code) transactions that are in scope of SCA but are submitted to authorization without SCA or without an exemption indicator

4.4 Liability for fraud-related chargeback

Tables 23, 24 and 25 below summarise how liabilities for fraud-related chargeback apply between the Issuer and the Acquirer under the Visa Rules for the application of exemptions, application of Delegated Authentication and resilience and for out of scope transactions. Exemptions applied or indicated by the Acquirer must have an exemption indicator in F34 in the authorization request to be considered valid by the Issuer.

Transactions for which SCA is applied are at Issuer liability ECI 05.

Please note that disputes liability under the Visa Rules may differ from "regulatory liability" under PSD2. For example, the payee's PSP cannot apply the trusted beneficiaries exemption, therefore, the Issuer is deemed to apply the exemption and is liable for fraud under PSD2 if an authorization was approved without appropriate authentication. If a merchant or Acquirer would like protection from fraud-related chargeback liability under the Visa Rules, they can choose to submit an EMV 3DS authentication request to the Issuer who can then decide to perform SCA or apply an exemption.

Please note that if the transaction qualifies for the Visa Digital Authentication Framework (DAF) and is approved, notwithstanding what is stated in the below table, the ECI value will always be 05 and the Acquirer will have Fraud liability protection, no matter what exemption or delegated authentication may have been indicated in the transaction

Table 23: Summary of EMV 3DS indicators and Field 34 indicators for exemptions and associated Fraud Liability

Exemption	Acquirer or Issuer applied	Authentication		Authorization	Fraud liability under Visa Rules[82]
		Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
Transaction Risk Analysis[83]	Submitted for authentication via EMV 3DS prior to authorization				
	Acquirer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	Issuer
	Submitted first to VTS[84] or straight to authorization				
	Acquirer	N/A	7	Yes	Acquirer
Low Value	Submitted for authentication via EMV 3DS prior to authorization				
	Issuer[85]	N/A	5	No	Issuer
	Submitted first to VTS[84] straight to authorization				
	Acquirer	N/A	7	Yes	Acquirer
	Issuer	N/A	7	No[86]	Acquirer
Secure Corporate Payment[87]	Submitted for authentication via EMV 3DS prior to authorization				
	Issuer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	Issuer
	Submitted first to VTS[84] straight to authorization				
	Issuer	N/A	7	Yes	Acquirer

[82] Regulatory liability may differ.
[83] The TRA exemption indicator is only available in EMV 3DS version 2.2 or higher (not in EMV 3DS 2.1).
[84] For token transactions not submitted via EMV 3DS, the exemption can only be indicated in the authorization request.
[85] There is no low value exemption indicator in EMV 3DS 2.1 or 2.2 for the Acquirer to request this exemption, however the Issuer can choose to apply this exemption in which case an ECI 05 is returned without a challenge.
[86] It is not recommended (yet allowed) for an Acquirer to submit this type of transaction without a value in Field 34. It is best practice for the Acquirer to populate an exemption indicator or other informational indicator (Visa Delegated Authentication, Resilience indicator) in F34 (or the Deferred authorization Indicator in Field 63.3) when no authentication data is sent to the Issuer in an authorization request.
[87] This exemption can only be applied by the Issuer – but the indicator can be set by the Acquirer to indicate this exemption may apply.

Exemption	Acquirer or Issuer applied	Authentication		Authorization	Fraud liability under Visa Rules[82]
		Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
	Issuer	N/A	7	No[86]	Acquirer
Trusted Beneficiaries [88]	Submitted for authentication via 3DS prior to authorization				
	Issuer	Yes	5	Yes[89]	Issuer

Table 24 Summary of EMV 3DS and Field 34 indicators for Visa Delegated Authentication Program and Resilience and associated fraud liability

Indicator	Authentication		Authorization	Fraud liability under Visa Rules[82]
	Merchant populated Delegated Authentication indicator in EMV 3DS or VTS Yes or No	ECI Value	Acquirer populated Delegated Authentication indicator in authorization F34 Yes or No	
Visa Delegated Authentication Program[90]	Issuer generated CAVV, or Visa generated CAVV or TAVV			
	Yes	7	Yes[91]	Acquirer
Acceptance environment outage Indicator	Submitted straight to authorization[92]			
	N/A	7	Yes	Acquirer

[88] The trusted beneficiaries exemption indicator in EMV 3DS is only supported in version 2.2 or higher.
[89] For the first transaction where a challenge is being applied to add a merchant to the Trusted Beneficiary list, it is not required to put the Trusted Beneficiary exemption indicator in F34. It is however required in the subsequent transactions
[90] The VDA programme is only available in EMV 3DS version 2.2 or higher (not supported EMV 3DS 2.1).
[91] The indicator must be populated when the CAVV was generated via EMV 3DS. When VDAP is applied by a digital wallet, this indicator is not populated by the Acquirer but by Visa upon receipt of the TAVV.
[92] Authentication via 3DS has been attempted but due to an outage in the acceptance domain (i.e. in the authentication flow between the merchant, gateway 3-D Secure (3DS) server, and Directory Server) an authentication request was not possible and/or an authentication response could not be received.

Table 25: Use of EMV 3DS and Application of Liabilities for out of scope transactions

Out of scope use case	Submitted Via EMV 3DS	Challenge Applied	Fraud Liability under Visa Rules
Merchant Initiated Transaction (MIT)[93]	No (subsequent transaction)	No	Acquirer ECI 07[94] [95]
	Yes (only for MITs using the Reauthorization indicator that carries a CAVV and associated ECI 05)	Yes	Issuer ECI 05
Anonymous cards	Yes	No	Acquirer ECI 07 or Issuer ECI 05[96]
	No	No	Acquirer ECI 07
MOTO	No	No	Acquirer ECI blank, 1, or 4
One-leg-out	Yes	Optional	Issuer ECI 05
	No	N/A	Acquirer ECI 07

[93] Note this use case refers only to subsequent MITs that occur after the MIT agreement is set up. The initial transaction required to set up the MIT agreement is a CIT.

[94] Note that in the Incremental authorization, the ECI value is 07 when performed in CNP mode please note however that when cleared, the applicable liability is that of the one in the associated CIT (initial estimate).

[95] Note that Visa does not currently support the use of 3RI to obtain a CAVV for uses cases other than split/delayed shipment and multi-party commerce – which both use the MIT reauthorization.

[96] An ECI 07 is for the scenario when the anonymous card is not enrolled in 3DS. If the Issuer chooses to support 3DS on Anonymous cards (which is the Visa recommendation as the Visa Attempts Server will not stand in for Anonymous Cards) then the Issuer may authenticate and provide an ECI 05.

4.5 Additional guidance on application of the exemptions

This section provides additional practical advice to Issuers, Acquirers and merchants on important considerations and factors to take into account when developing strategies to apply exemptions. For guidance on the order in which to consider applying the exemptions please refer to section 4.3.3.5.

4.5.1 The low value exemption

Remote transactions up to and including €30 (£25 in the UK) do not require SCA so long as the cumulative number of previous remote transactions using the exemption does not exceed five or the cumulative value of previous remote transactions using the exemption does not exceed €100 (£85 in the UK), since the last application of SCA. Issuers should select either the cumulative or consecutive limit. If Issuers do not select to apply one of the limits, they must apply both limits for each transaction.

However, in the majority of cases PSPs should consider applying the TRA exemption rather than the low value exemption:

- Acquirer application of the low value exemption should only be used when the transaction does not qualify for the TRA exemption, as the Acquirer has no view of the cumulative consecutive transaction and value counts and the transaction will need to be resubmitted via EMV 3DS if either limit is breached.
- Issuer application of the low value exemption for transactions submitted via EMV 3DS requires a real-time link between the ACS and the Issuer's Authorization system to check cumulative transaction and value limits have not been breached before applying the exemption.

Issuers also need to ensure:

- They have velocity checking against the cumulative low value transaction count or amount limits in place and that if they are applying the exemption to transactions submitted via EMV 3DS, the Issuer's ACS is linked in real time to the velocity checking in the Issuer's authorization system. If this is not done, there is a risk that the Issuer will apply the exemption at authentication, but when the transaction is submitted for authorization, if the count or value limit has been exceeded, an SCA decline code will be sent prompting the merchant to resubmit the transaction via EMV 3DS for a second time.
- The authorization system is able to increment and reset the velocity counters correctly based on when a Low Value exemption and/or RBA is applied.
- The low value exemption should not be applied to and the cumulative transaction count should not be incremented for account verification transactions that do not require SCA. See Section 4.8.3.2 for more information on these transactions. They are able to apply SCA to a low value transaction when the cumulative transaction count or amount limit is breached and when no other exemption is applicable.
- They are able to provide an SCA decline code should the maximum value or transaction count be exceeded.

- They still apply RBA to low value transactions as required by the PSD2 regulation and should apply SCA if the transaction is perceived to be at risk of fraud.
- The low value transaction limits can be applied separately to different devices/tokens linked to the same payment account[97].

Issuers should note that:

- Transactions should also not be considered low risk just because they are of low value. Any fraud that occurs will impact the ability of PSPs to apply the TRA exemption.
- The Issuer authorization system can keep track of transactions that have had authentication applied by checking the authentication method value in Field 126.20[98] of the authorization request message.
- However, if the Issuer decides to apply a low value exemption and not to apply SCA to a transaction, it will proceed as ECI 05 with Issuer liability. An Issuer using a supported version of the CAVV for EMV 3DS may choose to use one of five Issuer defined authentication method indicators in the CAVV. This could be used to notify the Issuer host environment that the low value exemption has already been applied in EMV 3DS. Please see *Visa Secure Cardholder Authentication Verification Value (CAVV)* Guide for details.

4.5.2 The TRA exemption

4.5.2.1 Introduction

TRA is key to delivering frictionless payment experiences for low-risk transactions.

The TRA exemption may be applied by the Issuer or the Acquirer. The process for applying the exemption is summarized in Section 4.3. This section provides some additional information to help Issuers, Acquirers and merchants to manage their strategies for the most effective application of the TRA exemption.

4.5.2.2 Requirements Regarding Risk and Transaction Monitoring

The PSD2 SCA RTS lay down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs[99]. However, to use the TRA exemption the PSP must take into account a number of additional risk-based factors set out in SCA RTS article 18 and determine, according to the rules in SCA RTS, that the transaction poses a low level of risk.

Visa requirements for the deployment of RBA and EMV 3DS specifications for the data elements that should be provided as the basis for RBA risk scoring are summarized in Section 3.3.8 and the *Visa Secure Program Guide*. Visa has also recommended standards for transaction monitoring and fraud detection and has best practice guides available on these subjects.

---

[97] SEE EBA Q&A 4036 & 4038 for more information.

[98] See Section 3.2.6 for more detail on Field 126.20 and the list of authentication method indicator values.

[99] See Recital 14 and article 2 of the Regulatory Technical Standards.

Issuers, merchants and Acquirers should ensure that their Risk monitoring and scoring systems used as the basis of for the application of transaction risk analysis meet these requirements.

4.5.2.3 Contracting out the application of TRA

Issuers will normally utilize risk engines provided by their ACS providers to apply TRA for the purposes of the TRA exemption.

Under the regulation, Acquirers may contract out the application of TRA to merchants however it is still the relevant PSP's fraud rate (and not the merchant's own fraud rate) which must be considered.[100]

4.5.2.4 Qualification to apply the TRA exemption

To qualify to apply the TRA exemption, a PSP must maintain its fraud rate within the following reference fraud rates:

Table 26: Reference fraud rates

Transaction value band EEA	Transaction value band UK	PSP Fraud Rate
≤€100	≤£85	13 bps / 0.13%
€100 ≤ €250	£85 ≤ £220	6 bps / 0.06%
€250 ≤ €500	£220 ≤ £440	1 bps / 0.01%

The reference fraud rate requirement only applies to the PSP applying the exemption, so for example an Issuer may apply the exemption to a transaction within a value band for which its fraud rate is below the reference fraud rate even if the Acquirer's fraud rate is above the reference fraud rate for that band.

Merchants, Acquirers and Issuers can all apply measures to ensure that they maximize their ability to benefit from the exemption. These include:

- **Merchants:** should ensure that they understand their Acquirer's fraud rate and should consider shopping around for Acquirers who are able to apply the exemption at the transaction value level they seek.
- **Acquirers:** have the flexibility to only allow certain low risk merchants to benefit from the exemption and may use this in order to minimize risk and fraud rates.
- **Issuers:** should carefully monitor fraud rates against the reference fraud rate thresholds to ensure they achieve a balanced application of SCA that enables them to maintain fraud rates within their target level for application of the exemptions while minimizing customer friction. While unnecessary application of SCA may decrease fraud rates, the inconvenience to consumers brings the risk of:

[100] (Reference: *EBA: Opinion Paper on the implementation of the RTS on SCA and CSC - June 2018, para 47*).

- Increased transaction abandonment, reducing e-commerce transaction rates and consumers switching to alternative, lower friction payment methods or Issuers.
- Breaching the Visa rule limiting transaction abandonment (see section 3.5 for more details).

4.5.2.5 Calculation of fraud rates

The PSD2 & UK regulation[101] requires that:

- The calculation of the fraud rate includes both unauthorized transactions and fraudulent transactions resulting from the manipulation of the payer.
- The calculation is defined as the total value of unauthorized or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under an exemption. This means that while transactions where an exemption applies should be included in the calculation, out of scope transactions, i.e. MITs, OLO and MOTO transactions (see section 2.3.1 for more information), should not be included in the calculation.
- The fraud rate is calculated on a rolling 90-day basis.
- In order to apply the exemption, an Issuer or Acquirer is required to provide the competent authorities, upon request, with the methodology, model and fraud rates it is using for the application of the TRA exemption. Issuers and Acquirers will be required to monitor their fraud rates to continue to apply the TRA exemption and notify their competent authority if they go over the reference fraud rates.

The EBA has confirmed[102] that PSPs should include all fraud, including transactions to which SCA has been applied and those where an exemption has been applied, irrespective of which PSP applied the exemption. Issuers should therefore include fraud on exempted transactions where both the Issuer and Acquirer have applied exemptions and vice versa. In the UK, the FCA has confirmed that the PSP should only include the fraudulent transactions for which it is solely liable (excluding the fraudulent transactions where another PSP was liable).[103]

4.5.3 Application of the trusted beneficiaries exemption

4.5.3.1 Introduction and principles

The trusted beneficiaries exemption allows for the cardholder to add a trusted merchant to a list of trusted beneficiaries held by their Issuer, completing an SCA challenge in the process. Further SCA application on subsequent transactions by that cardholder with the trusted merchant should generally not be required.

---

[101] Refer to the EBA Regulatory and Technical Standards for Strong Customer Authentication and the EBA Opinion Paper on the Implementation of the RTS on SCA and SCSC 13 June 2018. For the UK refer to FCA Policy Statement PS21/19

[102] Reference EBA Q&A 2019_4702 https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4702.

[103] FCA Policy Statement PS21/19 Article 20.68.

To be compliant with SCA provisions:

1. Only Issuers can create/maintain lists of trusted beneficiaries on behalf of cardholders and use the trusted beneficiaries exemption (which Issuers generally do via their ACS)
2. Only customers can add or remove a merchant to/from a Trusted List and this must be done through an Issuer controlled process
3. Additions to, and amendment of, the Trusted List requires SCA
4. Acquirers cannot apply this exemption and a merchant cannot set up the Trusted List for the purpose of the SCA exemption
5. A payment transaction can only use the trusted beneficiaries exemption if the intended recipient of funds for the transaction is a merchant who is on the customer's list of trusted beneficiaries.

Note the PSD2 regulation does not define a transaction value limit for the application of the trusted beneficiaries exemption so it can be applied to transactions of any value.

4.5.3.2 Benefits of applying the exemption

Conditional on the Issuer implementing a well designed user experience, the trusted beneficiaries exemption offers potential benefits to all parties:

Consumers may benefit from:

- A smoother payment experience, without the need to complete an SCA challenge when they purchase from a trusted merchant, regardless of the value of the transaction

Merchants who are nominated as trusted beneficiaries may benefit from:

- The ability to offer their regular customers a seamless purchasing experience without the need for SCA for a higher proportion of transactions
- The ability to use the trusted beneficiaries exemption for payment use cases where it may be difficult to apply SCA
- The possibility to maintain or improve sales conversions and authorization rates where the Issuer can apply the exemption

Issuers may benefit from:

- Providing their customers with a simple and secure way of ensuring that they are unlikely to be challenged when they shop at trusted merchants
- Putting their customers clearly in control of their Trusted Lists by providing a seamless way of adding and removing merchants from Trusted Lists and checking a merchant's status
- The possibility to maintain or improve sales conversions and authorization rates

4.5.3.3 Addition and removal of trusted beneficiaries to & from a Trusted List

Customers may be offered the option to add a merchant to their Trusted List:

In the purchase flow: Issuers can offer the ability for the customer to add an eligible merchant to their Trusted List during a purchase from the merchant where the transaction is submitted for authentication through EMV 3DS 2.2. In this case the Issuer will present the customer with an option to add the merchant to their Trusted List as part of the EMV 3DS user experience. Once SCA has been completed, the merchant will, subject to Issuer approval, be added to the customer's Trusted List.

Outside of the purchase flow: Issuers can offer the ability for the customer to add to and modify their Trusted List outside of the purchase transaction flow, for example in response to a request initiated elsewhere in a merchant's app or website or via an Issuer's online or mobile banking app or customer call/support center.

In either case, once the initial authenticated transaction to add the merchant to the Trusted List has taken place, subsequent transactions should not generally require SCA.

The following sections summarise the generic user experience associated with each of these options. The technical details of managing additions and removals to a Trusted List via EMV 3DS 2.2 are given in Appendix A.5

4.5.3.3.1 Adding a merchant to a Trusted List in the purchase flow

During a purchase, the merchant sends a request through EMV 3DS 2.2 for the Issuer to give the customer the option to add the merchant to their Trusted List. The Issuer or the Issuer's ACS provider will display the trusted beneficiaries option to the customer. This can be done by, for example, including a checkbox option to the EMV 3DS challenge screen to add the merchant to the customer's Trusted List. For technical and user experience guidance on implementing this option, please see: https://developer.visa.com/pages/visa-3d-secure/additional-use-cases-TrustedBeneficiary. If the customer agrees, the customer will be asked to authenticate both the purchase transaction and the addition of the merchant to their Trusted List through completion of a single SCA challenge. Once authentication is successful, the merchant will be added to the customer's Trusted List.

4.5.3.3.2 Adding a merchant to a Trusted List outside the purchase flow

A merchant may also be added to a customer's trusted list from one of the following:

Request initiated within a merchant website or app: The EMV 3DS 2.2 protocol allows for non-payment authentication requests sent from the merchant to request the Issuer allow the customer to add the merchant outside of the purchase transaction flow. The merchant will send a request through EMV 3DS 2.2 for the Issuer to give the customer the option to add that merchant to their Trusted List. The Issuer's ACS will respond by presenting an EMV 3DS challenge screen. This can be done by, for example, including a checkbox option to the EMV 3DS challenge screen to add the merchant to the customer's Trusted List. For more information please see https://developer.visa.com/pages/visa-3d-secure/additional-use-cases-TrustedBeneficiary. If the customer agrees to add the merchant to their Trusted List, the customer must complete SCA for the addition.

Via an Issuer's online or mobile banking services: An Issuer can configure their online or mobile banking services to enable functionality that allows their customers to manage their Trusted List. Issuers can develop features that enable customers to view their Trusted List and

add or delete trusted beneficiaries from their Trusted List. SCA is required when adding to or modifying a Trusted List through an online or mobile banking service. This also requires Issuers who use a solution provided by an ACS vendor to determine how to connect to the ACS's managed list service

Via the Issuer's Customer Service: The Issuer could provide customers with the ability to add/remove merchants from their Trusted List via their Customer Service Call Centre. This requires Issuers who use a solution provided by an ACS vendor to determine how to connect to the ACS's managed list service and provide their call centre staff with the ability to manage the ACS maintained list, without using EMV 3DS, noting that SCA must be applied when amending the list.

4.5.3.4 Applying the exemption or requesting challenges in subsequent transactions

A merchant that is on a customer's Trusted List, can indicate that it would like an Issuer to apply the trusted beneficiaries exemption to a transaction by using the trusted beneficiaries exemption indicator in EMV 3DS 2.2. Note that SCA must be applied when a merchant is added, or other changes are made to a customer's Trusted List.

4.5.3.5 Issuer options and obligations

Issuers are not under any obligation to provide their cardholders with a trusted beneficiary capability. However, having access to one more exemption to support smooth card transactions with identified trusted merchants provides clear benefits to both cardholders and merchants.

Issuers may still choose to apply SCA to a transaction with a listed merchant, if they consider that transaction at risk of fraud.

Issuers planning to support the use of the trusted beneficiaries exemption should consult their ACS service provider for access to an ACS-developed solution, or consider developing an in-house solution for the customers to add merchants to and subsequently manage their Trusted List.

Table 27 below summarises some additional minimal key considerations for Issuers when developing and/ or deploying trusted beneficiaries solutions. Issuers should however note that responsibility for designing and building a compliant solution that also offers a seamless customer experience while giving the customer a clear understanding of the Trusted List feature and how they can manage their trusted merchants, lies with them and/or their ACS service provider.

Table 27 Minimal key Issuer (or ACS) considerations for a trusted beneficiaries solution

Function	Considerations
Trusted list and List Management	• Issuers may want to consider managing a 'trusted listing' database which stores information about which merchants can be 'Trusted' by their cardholders • This database could also hold information about cardholders that have added merchants to their Trusted List either via the EMV 3DS flows or via the Issuer online, telephone or mobile banking services
Merchant identification	• Issuers need to consider how to identify the trusted merchant accurately across the authentication and/or authorization flows keeping in mind that different merchant ids/names may be used in both flows and that the merchant may not always use the same Acquirer
Merchant Selection	• Issuers may need to consider what the cardholder experience will be when selecting merchants they want to trust (e.g. which method(s) to support for enabling cardholders to add a merchant to or modify a Trusted List)
Authentication	• Issuers need to determine how SCA would be applied before a customer adds a merchant to or modifies their Trusted List
Implementation Considerations	• Issuers need to enable and test appropriate indicators in the EMV 3DS 2.2 flow during EMV certification to allow merchants to request application of the trusted beneficiaries exemption. Once certified, Issuers must activate the relevant account ranges in the Visa Directory Server as supporting the trusted beneficiaries exemption

4.5.3.6 Visa requirements on Issuers

Where an Issuer supports the trusted beneficiaries exemption, that Issuer must complete additional test cases during EMV 3DS 2.2 certification specific to the support of this exemption if not already done and once certified the relevant BIN or account ranges need to be activated in the Directory Server as supporting the trusted beneficiaries exemption.

For certification, standard processes, testing and project implementation fees will apply. To begin the process, visit https://technologypartner.visa.com/ for more information. Please also refer to *Issuer and Merchant/Acquirer Visa Secure –Implementation Guide for EMV 3DS* for more information.

4.5.3.7 Merchant options & requirements

A merchant can advise their customers of the benefits of using Trusted Lists and facilitate the addition process through:

- Promoting the benefits to regular customers and advising them of how they can add the merchant to their Trusted List
- Requesting that an Issuer serve the trusted beneficiaries enrolment option form through an SCA challenge when a customer who has not added the merchant to their list completes a transaction with them

A merchant that is on a customer's Trusted List, can indicate that it would like an Issuer to apply the trusted beneficiaries exemption to a transaction by using the trusted beneficiaries exemption indicator in EMV 3DS 2.2.

Ahead of submitting an authentication request with the trusted beneficiaries exemption indicator, the merchant should check to ensure the Issuer supports this feature. The 3DS Server provider should use the Preparation Request (PReq)/Preparation Response (PRes) message pair to obtain an updated list of Issuer support for the trusted beneficiaries exemption. Issuers supporting the exemption will have card ranges marked with an (ACS Information Indicator = 04). 3DS Servers should request updated data at least once every 24 hours and not more than once per hour. Merchants should work with their 3DS Server provider to confirm that an Issuer supports trusted beneficiaries for that specific range.

For more information, please refer to the *3-D Secure Implementation Guide*.

Merchants also have the ability to request that an Issuer does apply SCA to a transaction from a customer who has listed them. They should do this if they are concerned about the risk of the transaction by submitting that transaction via EMV 3DS using the 3DS Requestor Challenge Indicator = Challenge Requested: Mandate (04).

4.5.3.8 Technical dependencies

Visa supports authentication and authorization messages and fields to facilitate requests and communicate authentication and authorization status between the Issuer and the merchant relating to the usage of the trusted beneficiaries exemption. This section describes these messages and fields. Information on how these messages and fields are used in the process flows for adding merchants to a Trusted List and applying the exemption and authorizing subsequent qualifying transactions is provided in Appendix A.5.

4.5.3.8.1 Authentication fields, indicators & values

The trusted beneficiaries exemption is supported in all device channels (application, browser and 3RI) of the EMV 3DS 2.2 specifications.

Please note that the trusted beneficiaries exemption is referred to in the EMVCo 3DS 2.2 specification as "whitelisting" and was renamed to "Trusted Listing" with the release of the EMV 3DS 2.3 specification. The term "trusted beneficiaries" is used throughout this guide except where specific EMV 3DS fields, descriptors or values are named in which case the terminology used in the EMV 3DS specification is adopted.

Merchants and their 3DS Servers: need to be enabled for EMV 3DS 2.2 to use the indicators applicable to trusted beneficiaries. Merchants need to work with their 3DS Server provider to ensure logic is in place to know when to indicate a transaction using the trusted beneficiaries indicators.

Issuers and their ACS providers: need to be enabled for EMV 3DS 2.2 to use the indicators applicable to trusted beneficiaries. Issuers will be required to register their account ranges with Visa's Directory Server to indicate their support for the trusted beneficiaries indicators.

See Table 28 below for key EMV 3DS 2.2 fields for trusted beneficiaries. For more and the latest up to date information on the EMV 3DS 2.2 technical specifications with regards to trusted beneficiaries, refer to *EMVCo 3-D Secure Protocol and Core Functions Specifications Version 2.2.0*.

Table 28: EMV 3DS 2.2 message fields and values required for the trusted beneficiaries exemption

Field	Description	Accepted values
3DS Requestor Challenge Indicator	Indicates whether a challenge is requested for this transaction.	• 08 = No challenge requested (utilize whitelist exemption if no challenge required) • 09 = Challenge requested (whitelist option requested if challenge required)
whiteListStatus	Indicates the status of a particular whitelist.	• Y = 3DS Requestor is whitelisted by customer • N = 3DS Requestor is not whitelisted by customer • E = Not eligible as determined by Issuer • R = Customer rejected • U = Whitelist status unknown, unavailable, or does not apply
whiteListStatusSource	This data element will be populated by the system setting Whitelist Status.	• 01 = 3DS Server • 02 = DS • 03 = ACS
whitelistingDataEntry	Indicator to confirm whether whitelisting was opted for by the customer. whitelistingDataEntry is applicable only for the app device channel.	• Y = Whitelisting Confirmed • N = Whitelisting Not Confirmed
whitelistingInfoText	Text provided by the ACS/Issuer to customer during a Whitelisting transaction, applicable only for app device channel. If browser, the ACS will display text as part of the HTML.	

4.5.3.8.2 Authorization fields, indicators & values

To support Issuers that choose to implement their own trusted beneficiaries service, Visa supports authorization indicators to facilitate communication of the application of the exemption between Issuer, Acquirer and merchant during Authorization and to ensure that qualifying transactions are not declined or responded to with an SCA decline code (response code 1A).

If the merchant has requested application of the trusted beneficiaries exemption as part of the EMV 3DS 2.2 flow, the merchants (in agreement with its Acquirer) must specify the use of the exemption in the authorization message. A value of '1' must be passed in Field 34 Dataset ID 4A, Tag 84.

See Table 29 below for V.I.P. System fields for the trusted beneficiaries exemption. For more information on technical specifications, refer to *V.I.P System SMS POS Technical Specifications, Volume 1 & Volume 2*.

Table 29: V.I.P. System fields and values required for the Trusted Beneficiary exemption

Field	Description	Accepted Values in the Request Message	Accepted Values in the Response by Issuers
Field 34: Tag 84, Dataset ID 4A	The Acquirer indicates the Trusted Beneficiary exemption is being requested (with a value of '1') to the transaction.	• Trusted Beneficiary values • 0 = Trusted merchant exemption not claimed/requested • 1 = Trusted merchant exemption claimed/requested	• 2 = Trusted merchant exemption claimed/requested • 3 = Trusted merchant exemption claimed/requested
Field 34: Tag 8C, Dataset ID 4A	Tag to indicate 'Reasons for Not Honoring Exemptions' in the response message. Tag will contain Issuer-determined reason code values for not honouring the requested exemption. interpreted by the Acquirer in the response message.		• 8473 = Cardholder has not trusted merchant (issuer-determined) • 8474 = Did not meet the exemption (Issuer-determined)

4.5.4 Fraud Liability

As the trusted beneficiaries exemption is applied by the Issuer and initiated through EMV 3DS, the Issuer is liable for fraud resulting from lack of application of SCA due to use of the exemption. For more information please refer to Table 23 in section 4.4.

4.5.5 Interpreting the Secure Corporate Payment Processes and Protocols exemption:

4.5.5.1 Background:

Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are not consumers and are considered to be a "legal person". This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers. Subject to the view of NCAs, these payments may:

- Originate in a secure corporate environment, including for example, corporate purchasing or travel management systems
- Be initiated by a corporate customer considered a "legal person" using a virtual card or lodged account

In many cases it will not be possible to authenticate transactions originating in a secure corporate environment and requesting SCA may result in valid transactions being declined.

Issuers are therefore encouraged to support the exemption and merchants who process transactions originating from secure corporate purchasing systems or travel management systems should discuss with their Acquirer to determine whether any of their transactions should/could be indicated to their Acquirer with the secure corporate exemption indicator. This enables a transaction to be processed without authentication, so long as the Issuer supports the exemption, and the conditions for its application are present (among other, that the payer qualifies as a "legal person").

In order to apply the exemption, Issuers must ensure that, and NCAs must be satisfied that, the processes or protocols used guarantee at least equivalent levels of security to those provided for by PSD2. NCAs may have their own procedures or processes for assessing the use of this exemption.

Issuers are encouraged (and, for some NCAs, may be required to) to demonstrate to NCAs that applicable processes and protocols meet the requirements of the regulation and Visa recommends that Issuers liaise with NCAs over the procedure for this as required.

4.5.5.2 Interpreting the exemption

Subject to further regulatory guidance, Visa's view is as follows:

4.5.5.2.1 The exemption applies only to payers who are "legal persons" and not consumers

Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are not consumers and are considered to be a "legal person".

Issuers should liaise with NCAs to ensure they understand the interpretation of this exemption in each relevant jurisdiction.

4.5.5.2.2 Commercial card products to which the exemption may be applied

Visa considers that transactions made for business purchases using the following products used in the following ways could be within the scope of the exemption:

- Commercial virtual cards, Central Travel Accounts (CTAs) (also referred to as lodged accounts) that are embedded with B2B merchants[104]. These could include those used within an access-controlled corporate travel management or corporate purchasing system
- Physical Commercial cards that are issued for use by individual employees of a corporate entity and that originate within a secure corporate environment, may qualify for the exemption

4.5.5.2.3 Card Products and use cases to which the exemption may not be applied

Personal cards that have been issued to an employee or contractor as a consumer do not qualify for the exemption even if the transactions are for business purchases and the transactions with those cards are initiated from within a secure corporate environment.

The use of physical commercial cards issued to employees for business expenditure in circumstances where a secure dedicated payment process and protocol is not used (e.g. where online purchases are made via a public website) would not fall within the scope of this exemption, and SCA would need to be applied, unless the transaction qualifies for another exemption or is otherwise out of scope of the SCA requirement.

4.5.5.2.4 Examples of secure dedicated payment processes or protocols

Examples of secure corporate environments include:

- Corporate Travel Management Companies (TMCs) that store commercial card details of client employees within secure profiles that are only accessible by authorized employees through a secure log-in process
- Corporate travel booking tools (CBTs) that are only accessible by authorized employees through a secure log-in process[105]
- Corporate procurement systems that can accessed by authorized employees through a secure log-in process

Transactions initiated from within such environments with eligible cards should qualify for application of the exemption, subject to individual NCAs being satisfied that the security requirements of the regulation are met.

4.5.5.3 Application of the SCP exemption

The SCP exemption is an Issuer applied exemption. It may be applied to qualifying transactions that are submitted either:

- Via EMV 3DS (the EMV 3DS flow) or
- Straight to authorization (the authorization flow)

Issuers of virtual cards, CTAs and lodged accounts can use the BIN or account ranges to recognise transactions made using these types of card product.

---

[104] For the Visa definitions of Commercial Card products and their allowable usage under Visa rules please refer to the definition of "Commercial Cards" and individual card types in the Glossary.

[105] Note corporate booking tools may in some cases be provided by T&H suppliers acting as merchants as well as by specialist CBT providers.

They should apply the exemption to all qualifying transactions made using these types of card product, where the relevant NCA is satisfied that the requirements of the regulation are met.

However, where a physical Commercial Card is used, Issuers cannot differentiate between transactions that originate within a secure corporate environment that qualifies for the exemption and transactions that originate in a public environment where SCA is required. Furthermore, it is often not possible to apply SCA to a transaction originating in a secure corporate environment such as a TMC, CBT or procurement system. This means that unless the Issuer is told that a transaction using a physical card qualifies for the exemption, the Issuer is likely to request SCA and the transaction may fail.

For this reason, Visa has made available an SCP exemption indicator that can be used by a merchant or their Acquirer, and in some cases an intermediary, for example a Global Distribution System (GDS), to indicate to an Issuer that a transaction originates in a qualifying secure corporate environment and that it considers the SCP exemption may be applied. Visa has also put in place a framework of controls[106] and has updated Visa rules to support the use of the SCP exemption indicator and require that it is only used to indicate transactions that legitimately originated from environments that qualify for the application of the SCP exemption. Merchants/Acquirers may only submit transactions indicated with the SCP exemption indicator when they are satisfied that the requirements of the framework of controls have been met.

For more detailed guidance on applying the SCP exemption, use of the SCP exemption indicator and the framework of controls please see the *Secure Corporate Payments Exemption Implementation Guide*.

4.6 Challenge Design Best Practice

Reducing customer friction is essential to minimising customer dissatisfaction and transaction abandonment.

In those cases where it is necessary to apply an SCA challenge, the impact on customer experience will be minimised through:

- Careful selection and application of SCA factors and elements
- Optimised design of the challenge process and good communication – ensuring customers are clear on what steps they need to take
- Proper integration of the challenge screens into the checkout flow

The optimum SCA challenge solution(s) for an Issuer will depend upon the make-up of their customer base. Issuers, ACS and authentication providers should focus on the following SCA Challenge solution options, targeting them at the appropriate target customer segments:

- **Recommended solutions** – secure low friction solutions for the majority of customers in all markets:

[106] Note this framework of controls has been developed jointly by the major card schemes in consultation with Issuers, Acquirers and key stakeholders participating in a UK Finance working group dedicated to the application of the SCP exemption. The requirements apply to usage of the SCP exemption indicator across the EEA. Refer to *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements* for more details.

- Out of Band (OOB) app plus biometric
- OTP plus behavioural biometric

- **Tactical solutions** - Inclusive transitional are back up solutions for mainstream customers unable to immediately access recommended solutions:
  - OTP plus knowledge factor
- **Inclusivity solutions** – for niche segments unable to access recommended or tactical solutions:
  - Two factor card readers, OTP tokens, browser based solutions

Biometrics are the simplest and securest way to apply SCA. They minimise checkout friction and many customers are familiar with them and find them attractive. Both recommended SCA solutions use biometrics to provide an inherence factor.

For more information on the selection and implementation of these and the alternative tactical and inclusivity solutions please refer to the PSD2 SCA Challenge Design Best Practice Guide. This includes guidance on considerations including:

- The steps that Issuers need to take to optimise the onboarding and challenge user experience for the biometric solutions
- The user experience and security issues associated with use of knowledge factors and the selection of knowledge factors where these need to be used
- The steps that Issuers and merchants need to take to optimise the branding of the EMV 3DS challenge window and its integration into the overall user journey
- The requirement for merchant e-commerce websites to allow JavaScripts to run in the 3DS challenge window so as to enable collection of device data that is critical to ACS risk analysis and the operation of behavioural biometrics based challenge solutions

More detailed information on EMV 3DS UI challenge screen can also be found in section 4 of the EMVCo 3-D Secure Protocol and Core Functions Specification Version 2.2 and additional Visa guidelines for Issuers, ACSs and merchants, including detailed EMV 3DS challenge screen and OOB plus biometrics user experience design guidelines are available on the Visa Developer Center at https://developer.visa.com/pages/visa-3d-secure.

4.7 Use of EMV 3DS in storing credentials, setting up MITs & other key use cases: merchant & Issuer guidance

4.7.1 Introduction

This section provides additional guidance to merchants and Issuers on the use of EMV 3DS in specific transaction use cases to ensure that SCA is correctly applied and transactions are not unnecessarily declined. Experience has shown that these use cases can present challenges if merchants and Issuers are not clear on the intent of the transaction and/or how SCA should be applied.

It is particularly critical that Issuers are able to differentiate between use cases such as adding a stored credential for future customer-initiated transactions (CITs), which require SCA only if

there is a risk of fraud[107] and others, such as a CIT done to establish the agreement for future merchant-initiated transactions (MITs), which always require SCA when set up in a remote channel[108]. Currently, Issuers are unable to differentiate between these two use case in the Visa authorization system[109], resulting in unnecessary SCA declines when SCA is not provided.

To assist merchants and Issuers in indicating and identifying, respectively, the difference between these two scenarios and help minimize declines for transactions where Issuer authentication may not be required, merchants are recommended to use EMV 3DS and send the "3DS Add Card indicator" to correctly identify the intent of the transaction.

Other use cases require that the merchant requests that the Issuer applies SCA and that the Issuer responds accordingly.

Table 30 below summarises each of the relevant use cases, stating the SCA requirement and what the merchant wishes to achieve and to communicate to the Issuer through the use of EMV 3DS indicators. Table 31 summarises for each use case the correct use of the EMV 3DS indicators and population of the fields by the merchant and the correct response from the Issuer in terms of the application of SCA and generation of a CAVV. The Issuer can then use the CAVV during authorization to identify the type of transaction (and hence the SCA requirement) and whether or not SCA has already been applied in order to determine whether the authorization should be approved or declined. The population of the CAVV fields depending upon the use case, is summarised in Table 32.

Table 30 Use case overview

Use Case	SCA Requirement	Merchant Intent
1) Merchant adding credential on file for future CITs during a non-financial transaction (zero-value transaction)	Required if there is a risk of fraud Please note the following: • It is legitimate to consider there is no risk of fraud when the transaction is zero-value • The Issuer makes the final decision on whether SCA is required, i.e. some Issuers will require SCA, some will not, depending on their individual risk policy • To minimize potential declines with Issuers not requiring SCA, it is recommended to use EMV 3DS and send them the "3DS Add Card indicator" to correctly identify the transaction's intent	• Merchant wants a frictionless customer experience • Merchant wishes to advise the Issuer that the transaction may not require SCA

[107] Determination of fraud risk remains at the Issuer's discretion. Some Issuers may determine there is a risk and request SCA in add-card transactions, whether they are completed during a financial transaction or during an account verification, while others may not.

[108] Some exceptions apply where SCA may not be needed for CITs done to set up future agreements. For more information please refer to section 3.8.

[109] Refer to section 3.2.3.3and 4.2.3.1 for more details on how these use cases are indicated in authorization.

2) Merchant adding credential on file for future CITs during a financial transaction (> zero-value transaction)	• Exemptions may be used, but SCA is required if there is a risk of fraud • Visa recommends SCA is applied • The Issuer has final decision whether SCA is required or an exemption may be applied	Use case 2a): • Merchant would like a frictionless customer experience, and • Merchant wishes to advise the Issuer that the transaction may not require SCA OR Use case 2b): • Merchant requires SCA is applied prior to adding the credential on file to facilitate application of exemptions for future transactions
3) Merchant adding credential on file for future MITs during a non-financial transaction (zero-value transaction)	Required[110]	Merchant requires SCA to enable future MITs
4) Merchant adding credential on file for future MITs during a financial transaction (> zero-value transaction)	Required[110]	Merchant requires SCA to enable future MITs
5) Merchant receives SCA decline code (Response Code 1A) in authorization	Issuer has determined SCA is required	Merchant requires SCA is applied before resubmitting to authorization
6) Merchant considers transaction to be high risk based on their fraud assessment	Required	Merchant requires SCA due to assessed transaction risk
7) Merchant leaves it to the Issuer to decide whether to apply an SCA challenge or an Issuer exemption	Required unless the transaction qualifies for an Issuer exemption	Merchant would like to Issuer to decide

[110] See section 3.8.1.3 for details of limited exceptions to the requirement to apply SCA when setting up an MIT.

4.7.2 Merchant population of EMV 3DS Indicators and Issuer responses

4.7.2.1 Adding a Credential on File (use cases 1 & 2)

To minimize potential SCA declines with Issuers not requiring SCA on transactions processed to store a credential for use in future CITs, merchants are recommended to use EMV 3DS with the "3DS Add Card indicator" to correctly identify the transaction's intent.

- If this is done during a financial transaction, the "Message Category" in EMV 3DS must be "PA" for payment
- If this is done during an account verification transaction, the "Message Category" in EMV 3DS must be "NPA" for non payment
- The ability to use the 3DS Requestor Authentication Indicator = Add Card (04) for NPA transactions is being added to EMV 3DS only effective 15 October 2022.[111].

4.7.2.2 Setting up an MIT (use cases 3 & 4)

As SCA is required when setting up future MITs via a remote channel, merchants must use the 3DS Requestor Challenge Indicator = Challenge Requested: Mandate (04) for those cases as a challenge is required. Effective 15 October 2022, merchants have the option to send this indicator in a non-payment authentication (NPA) request when non-financial transactions are used to set up MITs, which was not the case before.

4.7.2.3 Merchant receives an SCA decline code (Response Code 1A) in authorization (use case 5)

An SCA decline code (Response Code 1A) received following submission of a transaction straight to authorization without SCA signifies the Issuer is requesting SCA.

When receiving this decline code, merchants must:

- Submit an authentication request via EMV 3DS requesting an SCA challenge by setting the 3DS Requestor Challenge Indicator to "04" – Challenge Requested (Mandate) before they re-attempt a new authorization request.
- Not re-submit the same transaction for authorization with an alternative exemption indicator.

If the merchant is unable to route the transaction through EMV 3DS then the authorization response must be interpreted as a decline and the transaction cannot be completed.

4.7.2.4 Merchant considers transaction to be high risk (use case 6)

A merchant that has undertaken risk analysis and considers a transaction to be high risk must submit an authentication request via EMV 3DS requesting an SCA challenge by setting the 3DS Requestor Challenge Indicator to "04" – Challenge Requested (Mandate).

[111] See VBN Article ID AI12300*Guidance for Merchants and Issuers on Use of EMV 3DSWhen Adding a Credential on File for Future Cardholder Initiated Transactions*, 1 September 2022.

4.7.2.5 Merchant leaves it to the Issuer to decide whether to apply an SCA challenge or an Issuer exemption (use case 7)

A merchant may decide to leave it to the Issuer to decide whether to apply SCA or an exemption. It may choose to do this if, for example, it does not have the capability to undertake risk analysis and or/or request the application of an Acquirer exemption, or if it wishes to benefit from liability protection. In this case, it should indicate this to the Issuer by setting the 3DS Requestor Challenge Indicator to "03" - 3DS Requestor Preference.

The Issuer chooses whether to apply SCA depending on its risk policy & must respond with a CAVV.

4.7.2.6 Summary of Indicators and Issuer responses by use case

The following table 31 summarises for each of the use cases:

- Key fields to use with the "Add Card" functionality where this is required
- The population of all relevant authentication request fields that indicate to the Issuer the type of transaction and authentication requirement
- The required Issuer response to these Indicators

Please note that a CAVV must always be generated for these transactions and if it is an NPA transaction it must be an NPA CAVV.

Table 31 Use of EMV 3DS Indicators, population of fields and Issuer response

Use Case	3DS Requester Challenge Indicator	3DS Requester Authentication Indicator	Message Category	Transaction Types	Issuer Response/ Considerations
1. Merchant adding credential on file for future CITs during a non-financial transaction (zero-value transaction)	Any applicable, as per transaction requirement	Add Card (04)	NPA (02)[112]	N/A	The Issuer chooses whether to apply SCA depending on its risk policy & must respond with an NPA CAVV. However the Issuer must consider the value of the 3DS Requestor Challenge Indicator when assessing these transactions, including honouring the challenge request when value is 04.

[112]Merchants should note that a CAVV generated when the message category is NPA can be submitted in authorization only in account verification transactions.

Use Case	3DS Requester Challenge Indicator	3DS Requester Authentication Indicator	Message Category	Transaction Types	Issuer Response/ Considerations
2. Merchant adding credential on file for future CITs during a financial transaction (> zero-value transaction)	Use Case 2a): Challenge requested: 3DS Requestor Preference (03)	Add Card (04) or Payment Transaction (01)	Payment Authentication (PA) (01)	Goods / Service Purchase (01)	Use case 2a): Issuer chooses whether to apply SCA or use an exemption depending on its risk policy & must respond with a CAVV
	Use Case 2b): Challenge requested: Mandate (04)				Use case 2b): Issuer must apply SCA & respond with a CAVV
3. Merchant adding credential on file for future MITs during a non-financial transaction (zero-value transaction)	Challenge Requested: Mandate (04)	Add Card (04)	NPA (02)[113]	N/A	Issuer must apply SCA & respond with an NPA CAVV
4. Merchant adding credential on file for future MITs during a financial transaction (> zero-value transaction)	Challenge Requested: Mandate (04)	Add Card (04) or Payment Transaction (01)	PA (01)	Goods / Service Purchase (01)	Issuer must apply SCA & respond with a CAVV
5. Merchant received an SCA decline code	Challenge Requested: Mandate (04)	Payment Transaction (01)	PA (01)	Goods / Service Purchase (01)	Issuer must apply SCA & respond with a CAVV

[113] Issuers should note that both PA and NPA categories are possible in this scenario. Merchants that wish to use message category PA (01) for cases where an MIT mandate is being set up using a non-financial transaction can continue to do so. In those cases, merchants must use the 3DS Requestor Authentication Indicator as Payment Transaction (01) and Transaction Type as Goods / Service Purchase (01). If NPA (02) is used, the CAVV generated can only be submitted to authorization in account verification transactions.

Use Case	3DS Requester Challenge Indicator	3DS Requester Authentication Indicator	Message Category	Transaction Types	Issuer Response/ Considerations
(Response Code 1A) at authorization and resubmitted the transaction to EMV 3DS					
6. Merchant considers transaction to be high risk based on their fraud assessment	Challenge Requested: Mandate (04)	Payment Transaction (01)	PA (01)	Goods / Service Purchase (01)	Issuer must apply SCA & respond with a CAVV
7. Merchant leaves it to the Issuer to decide whether to apply and SCA challenge or an Issuer exemption	Blank or Challenge Indicator = '01' (No preference) Challenge Indicator = "02" (no challenge requested). Challenge requested: 3DS Requestor Preference (03)	Payment Transaction (01)	PA (01)	Goods / Service Purchase (01)	Issuer chooses whether to apply SCA depending on its risk assessment & must respond with a CAVV

4.7.3 Additional Guidance for Issuers

The use of the 3DS Requestor Authentication Indicator = Add Card (04) in combination with the 3DS Requestor Challenge Indicator enables Issuers to identify the intent of a transaction during authentication and to apply SCA rules accordingly.

Through use of CAVV v7, Issuers are able to identify if a CAVV was generated as a result of the Add Card (04) function and an NPA. This allows Issuers to differentiate during authorization between credentials being stored for future CITs and transactions being used to set up MITs, and will help to minimize unnecessary declines. Table 32 below details the population of the CAVV fields to enable this. More information on CAVV v7 can be found in the *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

Issuers are reminded that during an Add Card (04) scenario where no financial transaction is being done at the time and the 3DS Challenge Requestor Indicator is not Challenge Requested: Mandate (04), SCA is only needed if there is a risk of fraud.

Issuers are required to challenge transactions in scenarios where the 3DS Requestor Challenge Indicator = Challenge Requested: Mandate (04). For scenarios where the 3DS Requestor Challenge Indicator is set to another value, Issuers need to assess the risk of the transaction and may choose to process the transaction as frictionless where appropriate.

Issuers are also reminded that when an EMV 3DS message is submitted with Message Category = NPA (02), a CAVV must be returned in the authentication response (even for frictionless transactions)[114].

Table 32 Population and use of the CAVV U3 V7 to differentiate use cases in authorization

Use Case	Issuer Response in EMV 3DS	CAVV U3 v7 – Field 126.9			126.20
		Position 1 (Authentication Results Code)	Position 2 (Authentication Method)	Position 6 (Supplementary Data)	
Merchant adding credential on file for future MITs during a non-financial transaction (zero-value transaction) (use case 3 from Table 31, performed with NPA category)	NPA Add Card CAVV generated - SCA Applied	Authentication Successful NPA transaction: '01'	'01'-'11', '92'-'96'	3DS Requestor Authentication Indicator value of '004': "Add Card"	Populated with value from CAVV Position 2 (Authentication Method)
Merchant adding credential on file for future CITs during a non-financial transaction (zero-value transaction) (Use case 1 or use case 3 with NPA category from Table 31)	NPA Add Card CAVV generated - SCA Applied	NPA: '01'	'01'-'11', '92'-'96'	3DS Requestor Authentication Indicator value of '004': "Add Card"	Populated with value from CAVV Position 2 (Authentication Method)
	NPA Add Card CAVV generated - Frictionless authentication		'97' or '99'		
Merchant requested SCA: • To add a credential on file and prefers a challenge to be applied	PA CAVV generated - SCA Applied	Authentication Successful: '00'	'01'-'11', '92'-'96'	All elements (Authentication Amount, Authentication Currency Code & Authentication	

[114] See the Visa Business News article *Visa Secure Non-Payment Authentication Rule Update* for details.

• To set up an MIT • In response to an SCA decline code • As it assessed transaction high risk (Use cases 2b, 3 with PA, 4, 5, 6 from Table 31)				Date) populated as normal for an approved PA transaction.	
Merchant leaves it to the Issuer to decide whether to apply an SCA challenge or an Issuer exemption (Use case 2a and 7 from Table 31)	PA CAVV generated - Frictionless authentication		'97' or '99'		

4.8 Additional guidelines for Issuers

4.8.1 Honoring step-up authentication requests

Issuers must always honor step-up cardholder authentication requests made by merchants to meet SCA requirements. Such requests are indicated by the use of a 3DS Requestor Challenge Indicator = "04" (Challenge requested (Mandate)). Merchants using this indicator may be doing so for one of three reasons:

- They view the transaction as risky and therefore want SCA to be applied
- They may be authenticating to set up an MIT mandate which requires SCA
- They may have received an SCA decline in authorization and are resubmitting requesting SCA.
- They may be adding a Credential on File and view this as risky and/or know the Issuer requires SCA for such transactions

4.8.2 3RI authentication requests

Issuers supporting EMV 3DS 2.1 and above may receive 3RI requests for a new CAVV for a transaction under some of the scenarios defined in Section 5 of this guide such as delayed or split shipments or under scenarios of multi-party travel bookings as described in *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality*. Each 3RI request for a CAVV should be assessed on its merits. Issuers must not blanket decline 3RI requests.

4.8.3 Issuer processing guidelines

This section summarizes the key points that Issuers need to be aware of when considering their role in the smooth implementation of SCA for e-commerce.

There are a number of important areas for Issuers to consider when processing e-commerce transactions.

4.8.3.1 BIN verification to identify transactions that are out of scope or qualify or an exemption.

Issuers are able to identify whether some transaction types are out of scope of SCA or qualify for an exemption by checking the BIN. This should be the case for:

- Anonymous prepaid cards (out of scope)
- Commercial virtual cards and lodged accounts issued to payers who are legal persons and not consumers (these transactions may qualify for the SCP exemption, subject to the opinion of NCAs).

When Issuers receive transactions that have been sent direct to authorization without the application of SCA and without an out of scope identifier or exemption indicator in Field 34, Issuers should check the BIN of the payment credential in the authorization request to identify whether the transaction is an out of scope anonymous transaction or a transaction to which the SCP exemption applies. If either of these is the case, the Issuer must not decline the transaction due to lack of SCA or issue an SCA decline code.

4.8.3.2 Account verification transactions

There are a number of reasons why a merchant may perform an account verification transaction as documented in Section 5 of this guide and summarized in Table 33 below. It is important that Issuers understand this is the case and adopt appropriate processing policies as several account verification transactions do not require SCA.

To help Issuers implement policies for these different scenarios, Table 33 below describes various types of use cases where account verification transactions are processed. It summarises how an Issuer can recognize them at a transaction field level and how Issuers should respond. In all scenarios except scenario 6 and scenario 5 when a CAVV with add card is present an Issuer will not be able to determine whether SCA is required or optional based on the data available to them. Visa recommends that Issuers consider relying on Acquirers / merchants to request and provide the CAVV when required and do not decline those transactions with an SCA decline code solely on the basis of the absence of a CAVV.

Note that token-based account verification authorizations that are not identified as MITs will continue to be submitted with a TAVV[115] even if the CAVV is not present.

Account verification transactions should not result in the cumulative transaction count that is used to determine whether the low value transaction exemption can be applied being incremented. See Section 4.5.1 for more information.

Best Practice

Some types of zero value transactions do not require SCA. Those types of zero-value transactions should not be declined because no SCA was performed.

[115] Token Authentication Verification Value (TAVV). Visa requires TAVV to be present in all token transactions unless the transaction is identified as Merchant Initiated Transaction.

Table 33 Account verification use cases, associated SCA requirements and expected Issuer processing policies

#	Merchant Use Case for Account Verification	SCA Required or Optional	Expected Authorization Fields	Expected Issuer Processing Policy
1	To check the validity and/or expiry date of a payment credential This is not a financial transaction (thus out of scope of PSD2), but a transaction processed purely to check the validity of a card. The merchant will check validity and will likely subsequently request a financial authorization including authentication data or suitable exemption indicators.	SCA not required.	Use cases 1, 2 and 3 can all be identified as follows: • Zero value • TAVV if token • Field 126.13 will be empty • Field 63.3 will be empty • No initial Transaction ID in Field 125 • No MIT indicator in Field 34, Tag 80 Dataset 02 • CAVV may or may not be present	An Issuer will not be able to determine which of these use cases the transaction was processed for; instead it must rely on the Acquirer to provide a CAVV if SCA is required and should not decline using an SCA decline code solely on the basis of no CAVV being present.
2	Setting up an agreement for No-Show, Delayed Charge or Incremental MIT when no initial charge is made at the time the agreement is made.[116]	SCA is required (CAVV must be present unless the Secure Corporate Payments (SCP) exemption applies, or the MIT agreement is set up via mail order / telephone order MOTO).		

[116] Note that any of these future MITs must refer to the initial CIT where authentication was performed except if the secure corporate payments exemption was used when setting up the No Show agreement.

#	Merchant Use Case for Account Verification	SCA Required or Optional	Expected Authorization Fields	Expected Issuer Processing Policy
3	Setting up an agreement for a delayed authorization or split shipment (MIT reauthorization) when no initial payment due at the time the agreement is made.	SCA may be performed but an exemption may also apply[117]. Even if SCA is performed, the CAVV may not be present as it may be kept by the merchant to populate in the MIT reauthorization later for fraud liability protection under the Visa Rules.		
4	Setting up an agreement for a future Unscheduled Credential-on-File (UCOF or usage based on recurring payment) when no initial charge is made at the time the agreement is made.[116]	SCA is required (CAVV must be present).	Use cases 4 and 5 cannot be distinguished, they will both look as follows: • Zero value • TAVV if token • "C" in Field 126.13 • Field 63.3 will be empty • No initial Tran. ID in Field 125 • No MIT indicator in Field 34, Tag 80 Dataset 02 • CAVV may or may not be present[118]	An Issuer will not be able to determine in authorization which of these use cases the transaction was processed for if it comes direct to authorization. Visa recommends Issuers to rely on Acquirer to provide a CAVV if SCA is required but understands if Issuers prefers more details. Refer to section 4.7 for further guidance on how to recognize those use cases via the CAVV and guidance on Issuer responses.
5	Storing credentials on file for the first time for future CITs when no payment is due at the same time. Note that future CITs performed with the credential will require SCA, or a suitable exemption.	SCA required if risk of fraud. It is legitimate to consider there is no risk of fraud when there is no financial transaction (account verification). but the Issuer makes the final decision on whether SCA is required based on its risk policy.		

[117] See section 3.8.1.3 for details. If an exemption is to be used, it can only be used via EMV 3DS – see section 4.2.4 for more details

[118] If present, refer to Table 32 to determine if a challenge took place or not

#	Merchant Use Case for Account Verification	SCA Required or Optional	Expected Authorization Fields	Expected Issuer Processing Policy
6	Setting up an agreement for a subscription (recurring payment) or installment / prepayment agreement) when no payment is due at the time of the agreement.	SCA is required (CAVV must be present).	• Zero value • TAVV if token • "R" or "I" in Field 126.13 • Field 63.3 will be empty • No initial Tran. ID in Field 125 • No MIT indicator in Field 34, Tag 80 Dataset 02 • CAVV must be present	In this Account Verification use-case an Issuer should request SCA if not present.. If the CAVV, or "enhanced TAVV[119] " is not present or valid, then the Issuer must decline with an SCA decline code.

4.8.3.3 Inclusion of CAVV and TAVV in MIT transactions

MIT transactions submitted after a previous CIT used to establish the agreement do not typically include CAVV or TAVV information, with the exception of Reauthorizations and card present incremental transactions. In the case of Reauthorization, the CAVV may be included by a merchant in order to claim fraud liability protection under Visa Rules (see Section 4.8.3.4).

Resubmissions as used in mass transit use cases where the initial contactless transactions was declined for lack of funds, will not be provided with a CAVV or TAVV as the original CIT to which they refer in the initial Transaction ID field is exempted from SCA (for more information refer to Section 5.10.

Note that it is also possible for an Incremental indicated with the MIT Framework to be a CIT (i.e. to be done in the presence of the cardholder), in which case the Incremental would have a card present POS entry mode and have associated chip data, including a cryptogram.[120]

4.8.3.4 Reauthorizations

A number of the scenarios in Section 5 of this guide use the Reauthorization message reason code 3903 with an initial Transaction ID in Field 125. These transactions represent payment scenarios where one or more authorizations take place when the cardholder is no longer present to complete a previously authenticated/exempted transaction, for example in the case of a:

- A delayed authorization[121] that takes place some time after checkout/authentication when the customer is no longer available; or
- Multiple authorizations processed for a single checkout/order, one for each individual shipment or item of the order

[119] Refer to section 4.8.3.8for a description of an "enhanced TAVV"

[120] This is for scenarios similar to the one described in section 5.8, but where the entry is facilitated via a card present tap/chip insert rather than app based.

[121] Refer to section 4.2.4 for a fuller definition of a delayed authorization.

These transactions must be processed as MITs in the Visa system as the cardholder is no longer present to be authenticated and so SCA should not be requested. The MIT type used is "Reauthorization". These transactions represent the completion of a CIT that could not be fully completed at time of checkout (i.e. are not MITs for regulatory purposes.

A number of principles apply to these transactions and these are summarized in section 4.2.5.3. Issuers should be familiar with these. Detailed guidance for merchants on submitting these transactions is included at section 5.1.3. Based on these principles, the following themes are notably important for Issuers to take into account when approving MIT reauthorizations:

- As the MIT Reauthorization used for split/delayed shipment is simply the completion of a CIT, MIT, exemptions can be used in the associated CIT so long as the CIT qualifies for the application of an exemption (see section 3.8.3.2 for more information). If an exemption is to be used, it can however only be used via EMV 3DS so the Issuer is made aware of the full amount of the transaction when deciding whether to agree to the exemption or not. This would not be possible in an initial authorization CIT that would be direct to authorization as the full amount is not processed at that time
    - Issuers should therefore not require that SCA has been completed in the associated CIT before approving an MIT reauthorization (i.e. should not decline an MIT reauthorization with an SCA decline code (response code 1A): if they had agreed to an exemption (Acquirer or Issuer applied) at time of the EMV 3DS request, they should honour their decision to accept an exemption.
- There are various options for the merchant in terms of where to submit the CAVV in the CIT /MIT reauthorization(s) combination depending on whether liability protection is being requested and the merchant is willing or not to get multiple copies of a CAVV. The merchant can populate the CAVV in the CIT and/or the MIT Reauthorization(s). Issuers should refer to Tables 37 and 38 in section 5.1.3 to be familiar with the acceptable options when deciding their authorization policies and honour each of these potential options. To summarize, in an CIT/MIT reauthorization combination:
    - A CAVV must be present in either the CIT or the MIT reauthorization; it can also be in both:
        - If the CAVV is present in the CIT, it will likely be for a higher authenticated amount than the one in the initial authorization as further authorization(s) will be completed later when processing the rest of the order
        - If it is not present in the CIT, it must be present in the MIT Reauthorization(s)
    - The CAVV may represent a fully authenticated transaction or contain an exemption
    - A CAVV may optionally be present in an MIT reauthorization
        - If there is no CAVV present in the MIT reauthorization, one must be present in the associated CIT, if not, the Issuer may decline the MIT reauthorization with an SCA decline code (response code 1A)

4.8.3.4.1 Expired CAVVs

It is important to note that merchants submitting Reauthorizations (MRC 3903) relating to delayed or split shipments may, on occasion include a CAVV that is over 90 days old. Visa Rules clearly state that fraud liability protection is limited to 90 days and therefore Issuers have dispute rights for any such transactions they receive. However, the CAVV if otherwise valid, can be resubmitted during the period up to 6 months[122] after it was generated to provided evidence that SCA was performed as part of the CIT. Issuers should not decline transactions based on the CAVV being more than 90 days old.

Key Point

Under Visa rules, merchants are liable for fraud on reauthorizations including a CAVV that is over 90 days old. However, the CAVV can still be used as evidence that SCA was performed and Issuers should not decline due to the age of the CAVV.

CAVVs over a year old will fail validation by Visa and will be indicated accordingly.

4.8.3.5 Transactions identified in accordance with the MIT framework

Issuers can identify MITs using one of the following methods:

- The existing Visa MIT Framework, or
- The initiating party indicator in Field 34[123]. The Acquirer must continue to use the existing Visa MIT Framework to indicate MITs. When receiving transactions that are indicated as MITs using the framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02). This enables Issuers to recognize a transaction as an MIT (and therefore out of scope of SCA) by simply checking for the value of "1" in that tag.

Transactions identified as MITs will have been performed at a time when the cardholder is not available. For this reason, Issuers must not decline a transaction indicated as an MIT solely on the basis that cardholder authentication was not performed (i.e. Issuers may not decline a transaction indicated according to the MIT framework based on the lack of authentication data).[124]

---

[122] A waiver is in place allowing, in Europe, the reuse of a CAVV up to 5 times for a period of 6 months rather than only 90 days, this until 18 October 2024, for split shipment scenarios and scenarios where transactions are associated with bookings via third parties, i.e. via Merchant Servicers or booking agents. For more information please see *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements*

[123] For more information please refer to *Article 9.1.4 of the October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019.*

[124] Unless there are reason to believe the MIT is not a legitimate one. Refer to *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements, version 3, section 3.4* for more details.

Best Practice

Issuers must not decline MITs on the basis that authentication is required (SCA decline code), as the cardholder is not present to authenticate.

For more information about how to recognize the different types of MIT, how they are indicated in authorization messages to distinguish them from CITs, Issuers should refer to Section 3.8.3.

Issuers are also reminded they must not decline a transaction based solely on a missing CVV2 for transactions where it is prohibited or not required to capture the CVV2: in Visa's view, all MITs fall in this category. For more details, including other transactions that cannot be declined solely on the basis of a missing CVV2, please refer to Visa Rule ID# 0029985 and 0029600.

4.8.3.6 Evaluate each transaction on its merits

Issuers are reminded that they are required, according to Visa rule # 0029326, to evaluate each transaction on its own merits. This means Issuers must not block, refuse, or decline Authorization Requests, payment token provisioning requests, or Transactions in a systematic or wholesale manner, unless there is an immediate fraud threat, or an exception is otherwise specified by applicable laws or regulations or in the Visa Rules.

4.8.3.7 Authentication provided by parties other than the merchant

In some cases, authentication may be requested by a party other than the merchant submitting authorization. Therefore, Issuers must be aware that the merchant name merchant ID and Acquirer ID used in authentication may legitimately be different to the merchant name, merchant ID and Acquirer ID in the authorization and process accordingly. In such instances it is best practice for the authenticating party to include the end merchant name in the authentication request. For example, an Online Travel Agent should authenticate on behalf of the merchants they represent citing the merchant name as "Online Travel Agent name * merchant name".

4.8.3.8 Using TAVVs to prove cardholder authentication

Visa requires a TAVV to be present in all token transactions unless the transaction is identified as an MIT.

Note that for a token transaction, an ECI is always supplied by the Visa Token Service with the TAVV and should always be used unless overridden by the use of EMV 3DS (for example, if VTS returns an ECI of 07 for a token transaction, but EMV 3DS is also successfully used, the merchant can change the ECI 07 to an ECI 05 or 06, as directed by the EMV 3DS transaction response).

A TAVV may be sufficient, without the presence of a CAVV, to indicate the cardholder has been authenticated in a transaction where the TAVV has been qualified under the following use cases:

- Under the Visa Delegated Authentication Program (VDAP)[125] where a VDAP indicator is present and the authentication factor indicators are present in the TAVV

Or

- Under an agreement in place between the Issuer and the Token Requestor for authentication and the authentication factor indicators are present in the TAVV.

This type of TAVV will be referred hereafter as an "enhanced TAVV". Where such a TAVV is used, a CAVV may not be required as proof of SCA.

4.8.3.9 Making allowances for legitimate data variations

Issuers need to be careful not to be overly prescriptive when matching data between authentications and authorizations, or CITs and the subsequent MITs. For example:

- The merchant name may be different between the authentication and corresponding authorization
- The merchant name may be different between a CIT and subsequent MITs (see Section 5.17.1 of this guide.
- The merchant name may differ for other reasons. For example, if the merchant uses multiple Acquirers, each of whom populate the merchant name slightly differently
- The Acquiring BIN and merchant ID may differ between the authentication and corresponding authorization as the merchant may use multiple Acquirers or in case of multi-party commerce (a third party handling the authentication on behalf of the merchant)
- The transaction amount may vary. For example:
    - A holiday booking fulfilled by more than one merchant may have been authenticated for the full amount of the booking, but each individual merchant may request a separate authorization for a lower amount corresponding to the value of their part of the booking.
    - In the case of a split shipment, the merchant may request separate authorizations for the value of each stage of the shipment. If 3RI is not yet available, the original CAVV may be used as an interim up to a maximum of five times and in each authorization request the amount will be lower than amount of the original CAVV.[126]

4.8.3.10 Handling transactions from merchants who are not yet fully ready for PSD2 or temporarily do not have a valid Tran ID

Issuers are reminded that to assist merchants who are not ready to send a valid Tran ID in MITs, Visa has assigned Tran IDs to Acquirers for use in the Original Tran ID Field (F125) as an interim solution that may be utilised until 31 October 2023. In those cases, where this interim Tran ID is used, Issuers will see a value of "0100000000000000" in Field 125 instead of the transaction ID of the original CIT or a transaction ID of a previous transaction in the agreed MITs. Beyond that date, Visa has identified a number of limited use cases where merchants

[125] For more information, please see the *Visa Delegated Authentication Implementation Guide*

[126] The interim arrangement only applies until18 October 2024.

may need as a "one off" to use an interim Tran ID to ensure continuity of pre-existing MITs (for example when switching acquirer and no longer having possession of the Tran ID they used to have for processing the MITs.) Visa has put in place another Interim Tran ID to use for those cases. Issuers are asked to therefore continue to accept the value "0100000000000000" even beyond 31st October 2023, but usage after that date should be limited. Refer to section 3.8.3 for more details.

All transactions from the travel and hospitality sector within scope of the SCA regulation must be compliant. Use of the MOTO indicator for some of these transactions[127] will be available as an interim solution to a technical issue preventing merchants from being able to provide all required proof of authentication / reference to MIT mandate setup authorization in their transaction flagging. No end date has yet been announced for this interim solution as it is not yet clear how quickly the industry can reasonably be expected to upgrade all relevant systems. Merchants are strongly encouraged to implement full solutions as early as possible to ensure they have sufficient time to complete the deployment once the end date for the interim arrangement is announced.

Issuers should continue to perform risk-based analysis on any MOTO transactions before making an authorization decision. It is possible that some of the transactions key-entered by merchants in a point of sale terminal without any MOTO indicator may not yet have been upgraded to include the MOTO indicator. These transactions may look in-scope and without any authentication; Issuers will need to consider which authorization decision to take in those circumstances.

4.9 EMV 3DS and authorization fall-back options

If for any reason an Acquirer is unable to authenticate a transaction using EMV 3DS due to an outage in the acceptance environment it may submit the transaction into authorization with the acceptance outage indicator in F34 to indicate that authentication was attempted for a transaction but there was an authentication outage in the authentication flow between the merchant, gateway 3DS server, and Directory Server, which means an authentication request was not possible. Please refer to section 3.2.5 for more details.

If for any reason an Issuer is unable to authenticate a transaction using EMV 3DS, or is unable to respond to an authorization request, Visa will step in, where applicable, through the application of the Visa Attempts Server or Stand-in Processing Service (STIP) respectively.

4.9.1 The Visa Attempts Server

The Visa attempts server will respond to an authentication request when a transaction is submitted using a version of 3DS that the Issuer supports but the Issuer's ACS is unavailable or does not respond in time[128]. In these cases, the Attempts Server will respond with a

[127] This is limited to out of scope MIT transactions in certain MCC codes, where authentication has been performed by a third party agent at the time of booking to set up the MIT mandate. Refer to *Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements, version 3, section 3.4* for more details

[128] Some card ranges, product types and message types are excluded from attempts processing. *See the Visa Secure Program Guide* for further information.

Transaction Status of 'A' (Attempts Processing Performed) and ECI 06[129] with the Issuer assuming liability. The Issuer may still authorize or decline the transaction at authorization.

Issuers should note that ECI 06 transactions have not been subjected to SCAAs all Issuers should support EMV 3DS, the only reason for generating ECI 06s should be because of ACS unavailability. Issuers will need to decide whether they can justify approving these transactions with their NCA (i.e. exceptional outage) or consider applying the low value exemption if the transaction qualifies.

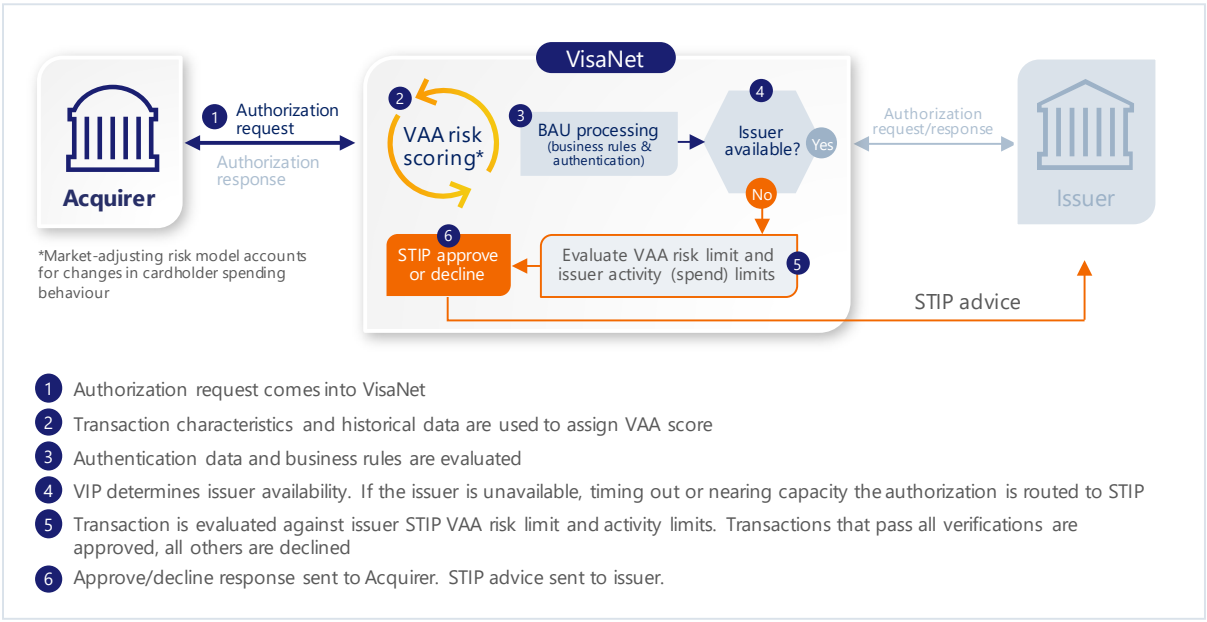
Issuers are advised to review their management of ECI 06 authorization responses should the Issuer's ACS be unavailable to respond to an authentication request once regulatory enforcement is in effect. Issuers may also want to consider their business continuity plans, in order to minimize the impact on consumers while ensuring that regulatory requirements are met.

The processing fee for each transaction processed by the Visa Attempts Server will be USD 0.075.

4.9.2 STIP

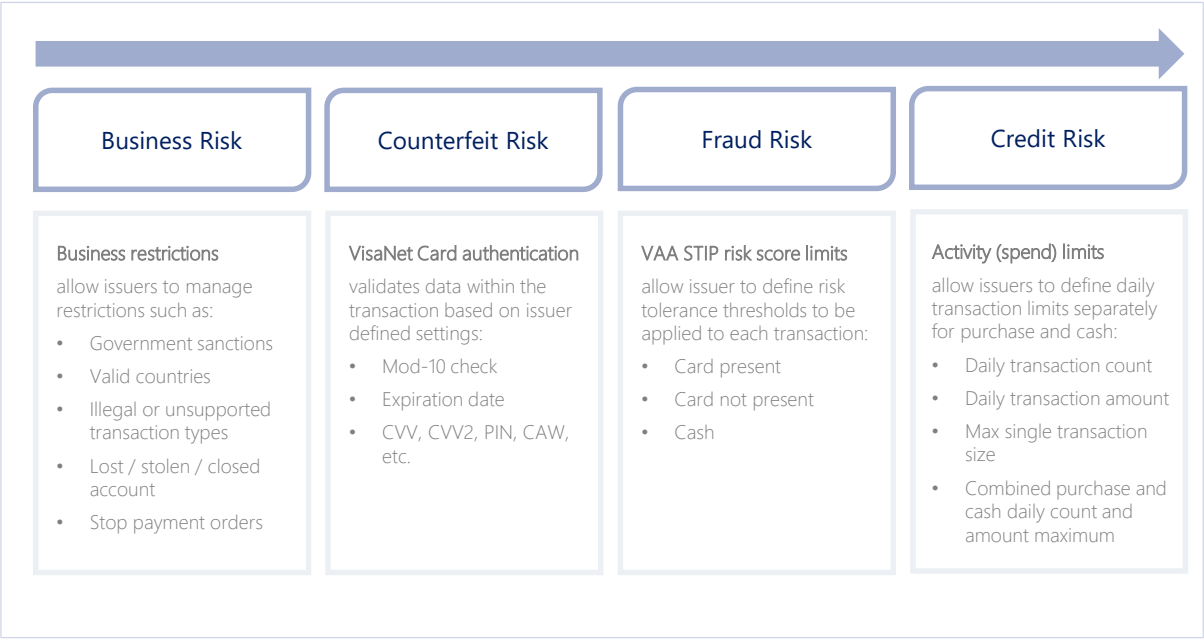
Stand-in processing (STIP) occurs when Visa acts as a backup processor that approves or declines authorizations on behalf of an Issuer. The VisaNet Integrated Payment (V.I.P.) System determines when a transaction is eligible for STIP based on Issuer availability or participation in various Visa on-behalf-of services. When a transaction is routed to STIP, a series of Issuer-defined parameters and activity limits are used to determine how the transaction should be processed.

Figure 17: Operation of the STIP approval service



[129] This response is mainly applicable to non-DAF and non-VDAP transactions. With DAF and VDAP the attempts server can provide different responses. See DAF and VDAP implementation guides for further details

Figure 18: The VisaNet STIP service offers a robust set of parameters to effectively manage STIP risk, including:



Please note: it is extremely important that Issuers provide Visa with their CAVV keys otherwise all e-commerce transactions will be declined in VisaNet STIP irrespective of what options have been set for SCA.

Activity limits determine the number of transactions and the amount that can be approved per day. The Visa Advanced Authorization (VAA) Score evaluates the fraud risk for each transaction.

Figure 19: An example set of STIP Limits for an Issuer's BIN

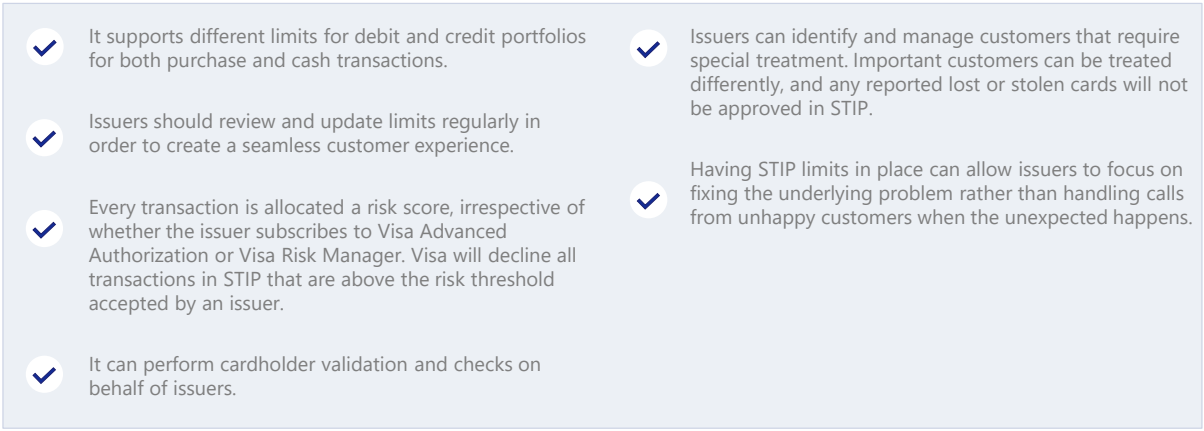
VAA Limits
- Card present, Card not present & Cash

Activity Limits
- Purchase & Cash
- Count & Amount
- Maximum single transaction amount

Combined Maximums (Purchase & Cash)
- Combined transaction count
- Combined transaction amount

Parameter	VAA Score Threshold	Total Count	Total Amount	Max Single Tran
Purchase-Card Present	30	10	$1,000	$500
Purchase-Card Not Present	30			
Cash	30	2	$500	$300
Max Combined		10	$1,000	N/A

Figure 20: VisaNet STIP protects an Issuer's business



4.9.2.1 Strong Customer Authentication Parameters for STIP[130]

To ensure that STIP transactions support the PSD2 requirement to enable SCA, SCA STIP parameters are available for Issuers in the EEA and the UK in the following scenarios:

- Does the Issuer want to decline all ECI 06 e-commerce transactions without a valid exemption or delegated authentication in STIP?
- Does the issuing BIN want to decline all ECI 07 e-commerce transactions without a CAVV and without a valid exemption in STIP?
- Does the issuing BIN want to decline all ECI 07 e-commerce transactions with a CAVV and without a valid exemption or delegated authentication in STIP?

The default value for all three questions listed above is 'No'. For example, an ECI 06 e-commerce transaction without a valid exemption will not be declined in STIP due to SCA. Issuers that choose to participate in these SCA STIP options must submit the SCA Client Implementation Questionnaire (CIQ) to specify their SCA parameters for STIP.

Note: Under the Visa Rules, the Issuer is responsible for a transaction authorized by STIP, including where the Issuer does not change the default values (via the CIQ) as listed above.

Issuers can define the response code to be used in SCA STIP for each of the three questions above:

- Declined with Response Code 05—Do Not Honor
- SCA decline code: Resubmit with SCA applied
- Approved with Response Code 00 (Note: This is the default if the Issuer does not use the STIP options as listed above.)

Issuers can define the exemptions to be used in SCA STIP; the valid exemptions from SCA for are below:

- Low value payment
- Transaction Risk Analysis (TRA)
- Trusted merchant / beneficiary

[130] These requirements are defined in VBN: *Changes to Stand-In Processing to Support Strong Customer Authentication Under PSD2* 18th April 2019.

- Secure corporate payment

Issuers may also define that delegated authentication is applied.

Additionally, Issuers can choose to select an exemption for transaction amounts less than the low value limit (EUR 30).

The default values for all six parameters listed above will be 'No'. For example, an Acquirer may have requested the Acquirer TRA exemption, but the transaction will be declined by default unless Issuers specify their SCA STIP parameters supporting TRA by submitting the SCA CIQ.

4.9.2.2 Scope of SCA / PSD2 for STIP Transactions

In addition to the exemptions and delegated authentication listed above, several types of transactions are out of scope for, or do not require SCA checks in STIP. These include:

- MITs
- MOTO transactions
- Original Credit Transactions (OCTs)
- One-leg-out transactions
- Merchandise returns

For STIP to recognize MITs as out of scope, a transaction needs to be indicated with the indicators from the existing MIT framework. For more details, refer to Section 3.8.

4.10 Visa Direct and SCA under PSD2

4.10.1 Background

Visa Direct is a real-time push payment platform designed to facilitate real-time payments to accounts globally. Visa Direct enables person to person (P2P) payments and can also be used by companies and public institutions for funds disbursements (e.g. insurance, salary, or benefit payments).

Visa direct can be used for a number of use cases including, for example:

Table 34 Visa Direct Use Cases

Money Transfer Use Cases	Funds Disbursement Use Cases
• P2P money transfer via bank or third-party apps • Loading money into another payment account, for example a prepaid card, e-money or stored value account • Withdrawal of money from another payment account, for example a prepaid card, e-money account	• General funds disbursements, for example, online gambling pay outs, lottery pay outs, shared economy • Merchant initiated disbursement, for example an insurance claim payout • Government initiated disbursement, for example VAT tax refunds

4.10.2 Visa Direct Transaction Types

Transactions associated with the Visa Direct service fall into two categories:

i. Original Credit Transactions (OCTs); used to "push" funds to a Visa cardholder's account

ii. Account Funding Transactions (AFTs); used to "pull" funds from a Visa cardholder's account

These transaction types are defined below:

4.10.2.1 Visa Direct Original Credit Transactions (OCTs)

Original Credit Transactions (OCTs) are push payments that allow a Visa cardholder to receive funds to their eligible Visa card account in near-real time.

Examples of OCTs are:

- A B2C payment such as the payout of an insurance claim to a customer's Visa card account or a salary payment made by a ride sharing platform to a driver.
- Small B2B supplier payment for business related supplies
- A gambling merchant paying winnings to a customer's Visa card

OCT may be initiated by a Visa member Acquirer on behalf of:

- A corporate entity who is paying a customer using a secure payment process or protocol (for example an insurance payout)
- A business with a need to pay a consumer on their Visa card

OCTs can be identified by Authorization Field 3, Field Value 26.

4.10.2.2 Account Funding Transactions (AFTs)

Account Funding Transactions (AFTs) are transactions used to pull funds from a Visa card account for the purpose of funding a different, non-merchant account; for example, loading or topping up prepaid card accounts, moving funds into another financial account such as a bank or E-money account, acting as a funding source for person-to-person (P2P) money transfers, or loading third-party staged digital wallets.

Examples of AFTs include:

- Consumer funding a P2P money transfer
- Consumer loading funds into an e-money or other stored value account
- Consumer loading funds onto, or topping up a prepaid payment card

AFTs are processed e-commerce transactions identified by Field Value 10 in Authorization Field 3.

Other purchase transactions are identified by Field Value 00 in Authorization Field 3.

4.10.2.3 AFT and OCT transactions

An AFT may precede an OCT transaction, for example when funds are pulled from a payer's Visa card account (an AFT) to fund a P2P money transfer destined to a recipients Visa card account (an OCT).

4.10.3 The Application of SCA and exemptions to Visa Direct Transactions

Visa Direct AFT transactions are in scope of SCA and SCA must be applied unless an exemption applies, or the transaction is out of scope. For example, this may be the case where the customer is loading funds into an account with a service provider they have added to a Trusted List and the trusted beneficiaries exemption may apply.

Examples include:

- Consumer funding a P2P money transfer
- Consumer loading funds into an e-money or wallet account
- Consumer loading funds onto, or topping up a prepaid payment card

The SCA requirement applies to payers, and therefore SCA does not need to be applied by the recipient when they receive an OCT transaction.

Examples include receipt of:

- Refunds
- Insurance claim Pay outs
- Other funds disbursements

Additional practical guidance on the application of SCA to Visa Direct transactions and the identification of Visa transactions that do not require SCA is given in Section 5.15.

4.11 Visa Secure Remote Commerce/Click to Pay

Click to Pay with Visa has launched as part of a wider industry initiative in accordance with the Secure Remote Commerce specifications published by EMVCo.

Merchants who use Click to Pay with Visa to provide a smoother checkout experience for their customers should be aware that using it alone does not fulfil their SCA obligations. Once the merchant has been provided with the payment credentials by Click to Pay, the merchant should check the Click to Pay payload to identify whether authentication has already been completed or must still be sought (e.g. using 3DS) or a suitable exemption exercised.

4.12 Visa Secure Authentication Technology and non-Visa Transactions

To maintain Visa Secure interoperability, any e-commerce transaction authenticated using the Visa Secure authentication technology must facilitate a Visa transaction. Entities that wish to use Visa Secure technology for non-Visa transactions, for example submitting a non-Visa transaction for 3DS authentication via the Visa Directory Server, must receive prior written permission from Visa. The Visa Rules have been updated to reflect these requirements. Clients that are currently using Visa Secure technologies to authenticate non-Visa transactions should contact their Visa Account Executive to discuss next steps[131].

[131] See *Visa Business News: Updated Rules for Visa Secure Authentication Technology 9 May 2019.*

5. Payment use cases and sector specific guidance for merchants and PSPs

The following subsections (starting at Section 5.2) provide merchants and Acquirers with best practice examples of how to ensure SCA is performed in compliance with PSD2 across common eCommerce payment scenarios, including MITs. The following information is provided for each payment scenario:

- A brief description introducing the payment scenario and when it is applicable, and
- When applicable, a step-by-step description of the actions that a merchant should take after each significant event (e.g. order is placed, shipment is made, etc.) occurs. The action taken by the merchant in each step is highlighted in bold and italics.

The approach for handling each of these scenarios serves only as a recommendation, therefore, merchants and Acquirers can choose alternative options that complement their business model, as long as they remain compliant with the key principles summarized in Section 4 and with any applicable laws, regulations and Visa Rules.

It is advisable that Issuers also familiarize themselves with the illustrated approach for handling each of the different eCommerce payment scenarios, so that they can adopt appropriate authorization policies to minimize unnecessary friction with their customers.

Before exploring individual payment scenarios, Section 5.1 explains the general approach across all scenarios for the inclusion of authentication-related data in the authorization message in order to achieve SCA compliance and meet Visa acceptance requirements.

5.1 Inclusion of authentication-related data

A merchant and/or Acquirer must populate authorization messages with the correct authentication-related data to indicate to the Issuer one of the following:

- SCA has been performed, or
- An SCA exemption is being exercised, or
- SCA has not been performed or attempted and an exemption is not being exercised, for example, because the transaction is out of scope of SCA.

If a merchant, or Acquirer, fails to include the correct authentication-related data in the authorization for a transaction that is in scope, then the Issuer might decline the transaction, creating unnecessary friction for the cardholder.

The following subsections help merchants understand which authentication-related data must be populated in the authorization messages and whether they qualify for fraud liability protection, depending on:

- Whether the transaction is in scope of PSD2 and SCA,
- The type of payment credential being used (i.e. PAN or Token),
- The authentication method being used (i.e. via 3DS or VTS), and/or
- How any exemption is being exercised (via 3DS or directly in authorization)

Based on the above, the merchant can then use the tables described in the following subsections to determine which of the authentication-related data listed below is applicable, and therefore, must be populated in the authorization message:

- Exemption indicator in Field 34
- CAVV (in case of EMV 3DS being used)
- TAVV (in case of token transactions)
- ECI value (can be either 05, 06 or 07)

5.1.1 Cardholder-Initiated Transaction (CITs)

Most CITs are in scope of SCA[132]. Therefore, depending on how SCA is being performed or exempted, the merchant must include the following in the authorization message for transactions of this type:

Table 35 Authentication-related data required for CIT authorization messages

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
SCA using EMV 3DS	PAN or Token	No	Yes	For token only (can be "enhanced TAVV"[133])	05 or 06	Yes
SCA exempted via EMV 3DS	PAN or Token	Yes	Yes	For token only (can be "enhanced TAVV")	05 or 07[134]	No
SCA exempted via authorization	PAN or Token	Yes	No	For token only (can be "enhanced TAVV")	07	No

[132] CITs that are out of scope of PSD2, do not require SCA. Examples of CITs that are out of scope of PSD2 are One-Leg-Out transactions (although SCA should be applied on a "best efforts" basis)

[133] See section 4.8.3.4for a description of an "enhanced" TAVV

[134] Refer to Table 23 Section 4.4 for further details on the ECI values associated with each exemption

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
SCA using VTS	Token	No	No	"Enhanced TAVV"	07	No

CAVV

- A CAVV can provide evidence of cardholder authentication or an applicable exemption to the Issuer.
- The merchant only receives fraud liability protection under the Visa Rules if the CAVV is provided with an ECI value of 05 or 06.
- If a CAVV was obtained, then the merchant should always include it in the authorization message, even if an exemption is being exercised or the transaction is out of scope of PSD2, to assist the Issuer in their authorization decision and prevent unnecessary declines.
- If an SCA exemption is exercised, then an applicable exemption indicator (in Field 34) along with the appropriate ECI value and the CAVV, if available, must be included in the authorization message.

TAVV

- All token transactions require the presence of a TAVV to support token domain controls, unless the transaction is a MIT, in which case a TAVV is not required.
- A TAVV may be sufficient, without the presence of a CAVV, to indicate the cardholder has been authenticated in a transaction where the TAVV has been qualified as described in section 4.8.3.8 and is considered "enhanced". Note that for a token transaction, an ECI value is always supplied by the Visa Token Service with the TAVV and should always be used unless overridden by the use of 3DS (for example, if VTS returns an ECI of 07 for a token transaction, but 3DS is also successfully used, the merchant can change the ECI 07 to an ECI 05 or 06, as directed by the 3DS transaction response).

5.1.2 Merchant Initiated Transactions

MITs are out of scope of SCA[135]. Therefore, authentication data is not required in authorization messages for transactions of this type. As such, Issuers may not decline MITs with an SCA decline code (Response Code 1A), as the cardholder is not available for authentication during these transactions. The merchant must include the following in the authorization message for transactions of this type (except for Reauthorization MITs in which case refer to section 5.1.3 below):

[135] SCA must be performed for the CIT used to set up the MIT agreement in most cases. Applicable SCA exemptions can be exercised in some cases such as Reauthorization or Resubmission MITs. See Section 3.8 for all exceptions.

Table 36 Authentication-related data required for MIT authorization messages

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
MIT out of scope	PAN or Token	Must not be present	No	No	07[136]	No

5.1.3 Reauthorization MIT (i.e. Delayed authorization with MRC 3903)

A Reauthorization MIT can *optionally* include a CAVV for the sole purpose of qualifying the merchant for fraud liability protection.

A number of the scenarios in Section 5 of this guide use the Reauthorization message reason code 3903 with an initial Transaction ID in Field 125. These transactions represent payment scenarios where one or more authorizations take place when the cardholder is no longer present to complete a previously authenticated/exempted transaction, for example in the case of:

- A delayed authorization; or
- Multiple authorizations processed for a single checkout/order, one for each individual shipment or item of the one check out order

The following three-step process must be applied to process MIT Reauthorizations:

- The initial CIT must first be routed via EMV 3DS: The full purchase amount must first be routed via EMV 3DS for Issuers to either fully authenticate or agree/apply the exemption against the full amount
- Authorization Step A: An authorization must be processed as a CIT at checkout either to authorize a part payment collected at checkout and/or to set up subsequent Reauthorization MIT(s)

  Authorization Step B: At shipment, Reauthorization MIT(s) must be processed to authorize the collection of payment(s) due.

The principles governing each step are summarised in section 4.2.5. This section provides the more detailed technical guidance for populating authorization request fields and providing authentication data at each step.

5.1.3.1 **Step A** - Perform an authorization CIT at checkout

The purpose of the CIT is to authorize any part payment that can be collected at time of checkout and/or set up subsequent reauthorization MIT(s) used for delayed authorization(s). If no payment is due at checkout, a zero value account verification transaction must be undertaken.

[136] Although MITs are out of scope of SCA, there is one special case where merchants can optionally include a CAVV in a Reauthorization MIT to qualify for fraud liability protection (ECI 05). More information on this is given in Section 5.1.3 below.

5.1.3.1.1 Use of exemptions when setting up the MIT Reauthorization

Exemptions can be used to process delayed/split shipments but they can only be used via EMV 3DS as the Issuer must be made aware of the full amount of the transaction when deciding whether to agree to the exemption or not. This would not otherwise be possible in the initial authorization CIT as the full amount is not processed at that time.

5.1.3.1.2 Provision of authentication data with the CIT authorization request:

The type of authorization request and the authentication data provided depends on the amount due at time of checkout:

- If no amount is due at checkout, an account verification must be submitted at checkout
- If only a partial amount is due at checkout, an authorization must be submitted only for the amount due

In each case the authorization request should contain the data outlined in Table 37.

Table 37: Step A - Authentication-related data in initial transaction

Transaction Type	CAVV required	TAVV required	ECI value	Exemption Indicator in Field 34[137]
Account verification	Optional	For token only ("enhanced TAVV")[138]	05 or 07 if CAVV present with exemption or 07 if no CAVV	Appropriate indicator must be present if exemption requested
Purchase transaction (partial amount)	Required for PAN Required for Token using exemptions (exemptions may be used only via EMV 3DS)	For token only (Must be "enhanced TAVV" if no CAVV)	05 or 07 depending on whether an exemption is used[139]	Appropriate indicator must be present if exemption requested

5.1.3.1.3 Submission of a CAVV with the CIT authorization request

As summarised in Table 37 above:

- A CAVV must be submitted if the CIT is being used to collect a partial payment at checkout (unless it is a token transaction, in which case an enhanced TAVV is sufficient as long as no exemption is requested).
- When no payment is collected at checkout and an account verification is used, merchants have the option to
  - Submit the CAVV with the account verification (Step A) and/or
  - The delayed (Step B) authorization,

[137] Exemptions can only be used when the transaction is first routed via EMV 3DS
[138] If this is not an enhanced TAVV, it means an exemption has been used so a CAVV is needed either in the CIT or the MIT reauthorization.
[139] Refer to Table 23 for details on liability when an exemption is used.

However merchants should note that

- In order to benefit from fraud liability protection where applicable, the CAVV must be submitted at Step B regardless of whether it is also submitted at Step A.
- If the CAVV was not submitted in Step A, it must be submitted in Step B

See Figure 21 below for a summary of these options. See also section 5.1.3.2.2 below for more detail on the implications of submitting the CAVV at Step A vs. Step B.

Issuers should not decline an account verification authorization request submitted without a CAVV with an SCA Decline Code (response code 1A), since this is not a financial transaction. The exceptions are:

- If the merchant is adding a new card on file at the same time (denoted by the value "C" in POS environment 126.13), in which case the Issuer may consider there is a risk of fraud and respond with an SCA decline code. Merchants may therefore prefer to include the CAVV in an account verification which contains a value "C" (adding a card on file) to avoid receiving an SCA decline
- If the merchant is setting up an MIT recurring or Installment transaction

Refer to section 4.8.3.2 for more Issuer guidance on authorization policies on MIT reauthorizations.

5.1.3.2 **Step B** – Submit delayed authorization with MRC 3903

At a later stage, when the shipment is ready, the merchant submits a delayed authorization(s) using Reauthorization MIT(s) with Message Reason Code (MRC) 3903.

5.1.3.2.1 Provision of authentication data with the delayed authorization request(s)

The delayed authorization should contain the data summarized in Table 38 depending on the authentication performed previously prior to the CIT

Table 38: Step B - Authentication-related data in Reauthorization MIT

Authentication scenario from CIT	Credential type	CAVV required	TAVV required	ECI value
SCA performed previously using EMV 3DS	PAN or Token	Required If was not in the CIT. Optional otherwise [140]	No	05 or 06, if CAVV present. 07 otherwise
Exemption was used via EMV 3DS at time of CIT	PAN or Token	No [141]	No	Refer to table 23 – varies depending on the exemption

[140] If the CAVV was submitted during the CIT, then the reauthorization can either be submitted with a new CAVV and associated ECI value (using 3RI, if available) or without a CAVV (in which case, without fraud liability protection).

[141] It is not worth submitting a CAVV if that CAVV has an associated value of ECI 07 as the only reason to submit a CAVV in an MIT is for liability protection.

Authentication scenario from CIT	Credential type	CAVV required	TAVV required	ECI value
Authentication submitted via VTS	PAN or Token	No	No	07

If an SCA exemption was exercised, then the applicable exemption indicator can be optionally included (in Field 34) in the authorization message, along with an ECI value of 07 and the CAVV, if available.

5.1.3.2.2 Submission of a CAVV with the delayed authorization request

If the merchant did not request an exemption/a challenge was applied, then the delayed authorization can optionally include a CAVV (with ECI 05 or 06) for the sole purpose of qualifying the merchant for fraud liability protection (see section 4.2.4 for more information).

The way the CAVV is submitted depends on the whether or not a CAVV was submitted with the initial CIT authorization request:

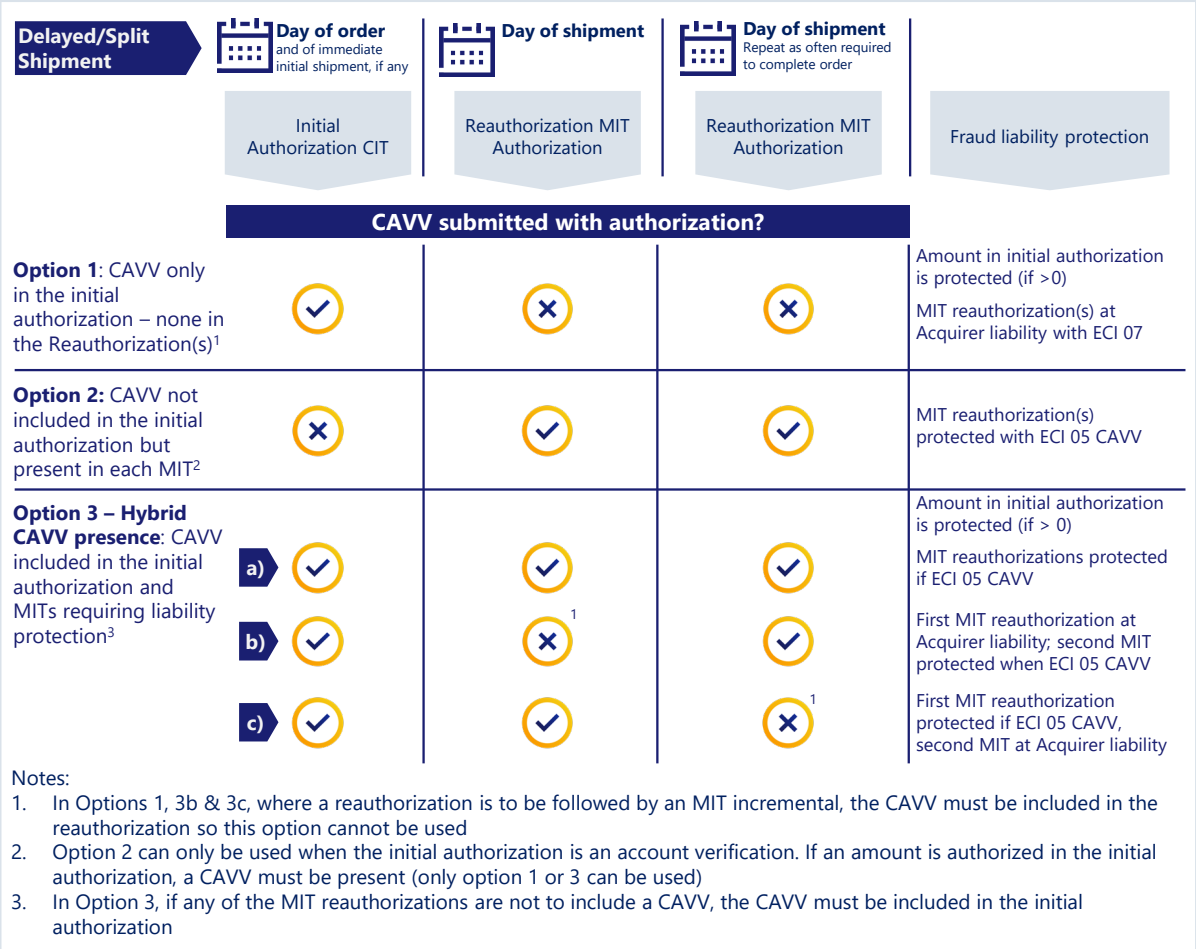
- **CAVV previously submitted at Step A:** If the CAVV was submitted during the account verification or partial payment (original CIT), then the delayed authorization can either be submitted with:
  - A new CAVV and associated ECI value (using 3RI to obtain a new CAVV, if available) or
  - The original CAVV (as an interim, if 3RI is not yet available, up to a maximum of five times – note that liability protection is in this case limited to the 90 days validity of the CAVV)[142] or
  - Without a CAVV (in which case, without fraud liability protection for this MIT reauthorization).

- **CAVV not submitted at Step A**: If the CAVV was not submitted during account verification or partial payment (initial CIT), then the CAVV must be stored for later submission in the delayed authorization(s). If multiple delayed authorizations are required to complete the purchase (e.g. due to split shipments), then the merchant and Issuer must be aware that each subsequent delayed authorization must have its own separate CAVV (e.g. using 3RI) for fraud liability protection, since the original CIT does not contain a CAVV that can be referenced. If 3RI is not yet available, the CAVV may be submitted as an interim approach up to a maximum of five times, but note that liability protection is in this case limited to the 90 days validity of the CAVV)[142]

A summary of the options for when the CAVV may be submitted when a reauthorization MIT is used for delayed and split shipment transactions, and how these impact liability protection is given in Figure 21 below.

[142] Until 18 October 2024, instead of using 3RI for these use cases, merchants can use the initial CAVV up to 5 times.

Figure 21 Summary of options for inclusion of CAVV in MIT Reauthorizations for Acquirer fraud liability protection



Notes:
1. In Options 1, 3b & 3c, where a reauthorization is to be followed by an MIT incremental, the CAVV must be included in the reauthorization so this option cannot be used
2. Option 2 can only be used when the initial authorization is an account verification. If an amount is authorized in the initial authorization, a CAVV must be present (only option 1 or 3 can be used)
3. In Option 3, if any of the MIT reauthorizations are not to include a CAVV, the CAVV must be included in the initial authorization

5.2 One-time purchase

A merchant receives an order from a customer for a known amount that it is able to fulfil in a single shipment within 7 days. For example a customer:

- checks out a basket of items online via a browser or mobile app
- purchases train tickets through an online booking service

Key Point

One-off transactions can be performed as a guest check out (POS entry mode = 01) or with a Credential-on-File (POS entry mode =10). For more detail see Appendix A1: Stored Credential Framework and section 4.2.3.1.

Processing a transaction with a stored credential does not qualify a transaction as out of scope or exempt of SCA. Many CITs use stored credentials and are in scope of SCA. Each transaction must be evaluated according to its own circumstances to determine if SCA is required. See section 3.2.9 for more information on out of scope transactions.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction* immediately *for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.2.
2. Authorize transaction • The merchant immediately ***authorizes*** *the transaction for the full amount*[144] and populates any applicable authentication-related data) in the authorization message as per Section 5.1.1 • If the transaction is out of scope of SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.
Shipment made (Customer no longer available)
3. Clear funds • The merchant ships the good(s) and **clears** the transaction for the full amount within 7 days.
Order Complete

5.3 Delayed Shipment

5.3.1 Delayed Shipment - expected delay

A merchant receives an order from a customer that it will fulfil in a single shipment, but it knows it will not be able to deliver within 7 days. The amount is known and not expected to change. Examples include:

- Item out of stock
- Pre-ordering upcoming goods or services such as new phone models or books / DVDs.

This approach is recommended so that the customer's open to buy is not impacted in the initial 7 days as the item will not be shipped within that period. If the authorization is to take place several months after initial order, it is best practice for the merchant to send a reminder to the cardholder a couple of days before authorization to maximize the opportunity for funds to be available.

Note: If the amount is not known at time of purchase, then the payment scenario described in Section 5.5 applies.

[143] If there is a possibility that the amount may change, the merchant should consider the options summarised in section 4.2.2.4 before deciding the amount to authenticate and whether to apply an exemption or request an SCA challenge.

[144] If the amount to be authorized exceeds the authenticated amount in the EEA or the allowable increased final amount in the UK, the merchant should refer to the options summarised in sections 4.2.2.4.1 or 4.2.2.4.2. depending on whether the change in amount is planned or unplanned.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization).
2. Perform a zero-value *account verification as an initial authorization* • The merchant must not authorize the transaction immediately as the authorization validity will expire before the shipment is ready and this would therefore impact the customer's open to buy for no valid reason. • Instead, the merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" transaction ID and store it for use in step 3.   • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3.
Merchant ready to make shipment (Customer no longer available)
3. Submit delayed authorization with MRC 3903 • When the order is ready for shipment, the merchant ***authorizes*** *for the full amount*[144]. The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework). • The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3. and the CAVV submission options summarised in Figure 21 If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3, table 21, Principle 11.
Shipment made
4. Clear funds • The merchant **clears** the transaction for the full amount.
Order Complete

5.3.2 Delayed Shipment - unexpected delay

Merchants should only perform authorization when they confirm that the goods are available and ready to be shipped (Section 4.2.5.3, Table 21, Principle 9). However, if a merchant does authorize before confirming goods are available, Visa recommends it proceeds as follows.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.2.

2. Authorize transaction
• The merchant immediately ***authorizes*** *the transaction for the full amount*[144] and populates any applicable authentication-related data in the authorization message as per Section 5.1.1:
  • The merchant must also store the Transaction ID for this step in case it is required later.
  • If the transaction is out of scope of SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.

End of 7 days Authorization validity period (Customer no longer available)
3. Submit reversal • After 7 days the merchant has been unable to ship the goods. The merchant must submit a ***reversal*** for the full transaction amount. • **Note**: The merchant could submit the reversal earlier as soon as they are aware that the shipment will be delayed beyond 7 days.
Merchant ready to make shipment (Customer no longer available)
4. Submit delayed authorization with MRC 3903 • When the order is ready for shipment, the merchant **authorizes** for the full amount [145] • The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework) • The merchant must populate any applicable authentication related data in the authorization message as per the Step B in Section 5.1.3 and the CAVV submission options summarised in Figure 21 • In the unlikely event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3, Principle 11.
Shipment Made
5. Clear funds • The merchant **clears** the transaction for the full amount.
Order Complete

[145] If the amount to be authorized exceeds the authenticated amount in the EEA or the allowable increased final amount in the UK, the merchant should refer to the options for unplanned amount variations summarised in section 4.2.2.4.2.

5.4 Split Shipment

5.4.1 Split Shipment - all fulfilled within 7 days

A merchant receives an online order from a customer for multiple items that it is able to fulfil within 7 days, but the goods are delivered in multiple shipments.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.2.
2. Authorize transaction • The merchant immediately ***authorizes*** *the transaction for the full amount*[144] and populates any applicable authentication-related data in the authorization message as p er Section 5.1.1 If the transaction is out of scope of SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.
Shipment Made (Customer no longer available)
3. Clear funds for each shipment separately • The merchant ***clears*** *for the amount of each shipment separately* as and when they happen over the next 7 days using multiple clearing sequence numbers[146].
Order Complete

Visa best practice is to use a single authorization with multiple clearing records for split shipment scenarios as defined in Section 4.2.5.3, Table 21, Principle 9.

There is an alternative approach available for merchants who, due to their business processes, would prefer to submit multiple authorizations. For more information, refer to Section 5.4.3.

5.4.2 Split Shipment - partially fulfilled within 7 days (unexpected delay)

A merchant receives an order from a customer that it fulfils across multiple shipments, but some of those shipments unexpectedly take place more than 7 days after the initial order.

Note: Merchants who follow best practice and only perform authorization when they confirm that the goods are available and ready to be shipped (Section 4.2.5.3, Table 21, Principle 9), will not find themselves in this position. Instead, they will either be able to confirm shipment straight away (refer to Section 5.4.1) or they will identify a delay and therefore the need to perform multiple authorizations (refer to Section 5.4.3).

However, if a merchant does authorize before confirming goods available for shipping and then finds itself in this situation, Visa recommends it proceeds as follows.

[146] For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028915

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization).

2. Authorize transaction
• The merchant immediately ***authorizes*** *the transaction for the full amount*[144] and populates any applicable authentication-related data in the authorization message as per Section 5.1.1
  • The merchant must also store the Transaction ID for this step in case it is required later.
  • If the transaction is out of scope of SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.

Merchant ready to make partial shipment (Customer no longer available)
3. Clear funds for the amount of each shipment separately • The merchant ***clears*** *for the amount of each shipment separately* using multiple clearing sequence numbers as and when each shipment occurs over the next 7 days[147].
End of 7 days Authorization validity period (Customer no longer available)
4. Submit reversal • At the end of 7 days, the order has only been partially fulfilled. The merchant submits a reversal for the amount of the original authorization that remains unfulfilled. **Note:** The merchant could submit the reversal earlier as soon as they are aware that the shipment will be delayed.
Merchant ready to make partial shipment (Customer no longer available)
5. Submit delayed authorization with MRC 3903 • When each subsequent partial order is ready for shipment, the merchant authorizes for the amount relating to the goods included in the shipment[148]. • The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework). • The merchant must populate any applicable authentication related data in the authorization message as per the Step B in Section 5.1.3 In the unlikely event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3 Principle 11 and the CAVV submission options summarised in Figure 21.

[147] For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

[148] If any of the amounts to be authorized for individual shipments varies such that the total value of all shipments will exceed the authenticated amount in the EEA, or the allowable increased final amount in the UK, the merchant should refer to and adopt an appropriate option as summarised in sections 4.2.2.4.1 or 4.2.2.4.2, depending on whether the change in amount is planned or unplanned.

6. Clear funds for the amount of each shipment separately The merchant ***clears*** for the amount of each re-authorization as the related shipments are made.
Order Complete

5.4.3 Split Shipment - Multiple Authorizations

A merchant receives an order from a customer that they will fulfil across multiple shipments. Visa's best practice is to handle with one single authorization and multiple clearing as in scenario 5.3.1 and 5.3.2 above. If the order can be fulfilled in 7 days, the benefit of this approach is to avoid matching between a single authentication and multiple authorizations and minimize the need for the use of the MIT Framework. However, merchants whose business processes are such that they must request a new authorization for every shipment can do so as per the example below.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the full amount*[143], obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization).
2. Either authorize transaction or perform a zero-value account verification • Depending on whether the goods for inclusion in the first shipment are immediately available, the merchant must *choose one of the following options*: a. Immediately ***authorize*** *the transaction for the value of the goods to be shipped*, if goods are available and store the "initial" transaction ID for later use in step 3 if further shipment(s) will be needed, or b. Perform a zero-value account verification, if none of the goods to be shipped are available. • In case of **option (a)**: • The merchant must **authorize** immediately for the value of the goods to be shipped[144]. • The merchant must populate any applicable authentication-related data in the authorization message as per Step A (purchase) in Section 5.1.3. and the CAVV submission option in Table 37 • If the transaction is out of scope of SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope. • In case of **option (b)**: • The merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" transaction ID and store it for later use in step 3. • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.13 and the CAVV submission options from table 37 summarised in Figure 21.
Merchant ready to make shipments (Customer no longer available)
3. Submit delayed authorization with MRC 3903 • When each of the remaining shipments is ready, the merchant ***authorizes*** *for the value of goods to be shipped*.

- The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework).
  - The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3 and the CAVV submission options from Table 38 summarised in Figure 21
- In the event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3 Principle 11.

4. Clear funds

- The merchant **clears** the amount authorized as the related shipment is made.

Order Complete

5.5 Open orders - Unknown final amount

The merchant receives an initial order from a customer. The value of the order may subsequently change prior to shipping for reasons including:

- The customer adding or removing items to or from the order
- Product substitutions
- The inclusion of products whose exact cost is unknown at time of order placement

This may result in the final amount increasing above:

- The amount authenticated at the time of the initial order for an EEA transaction
- The allowable increased final amount for a UK transaction[149] .

For example, online grocery shopping where the delivery date can be booked by the customer placing an initial order in excess of a defined minimum value several days, weeks or even months in advance. The customer can come back and update the order as often as they like until the pre-agreed cut-off time. In addition, even after the order is complete, further variance may occur, due to item substitutions, inclusion of items priced by weight etc.

In this scenario, there are different options for the merchant to consider. The best option for a particular merchant will depend upon:

- The merchant's preferred business processes
- Whether the final amount can be changed by the merchant after the customer has finalised the order (for example as result of product substitution by the merchant)

In all cases, if the final authorization is to take place several weeks/months after the initial order, it is best practice for the merchant to send a reminder to the cardholder a couple of days before authorization to maximize chances of funds being available.

5.5.1 Customer adding to basket - final amount does not change after the customer has finalised the order

These options are available to the merchant in cases where once the customer has finalised the order:

[149] Refer to section 4.2.2.3 for the definition of the allowable increased final amount.

- For an EEA transaction there will be no further increase in value for an EEA transaction
- For a UK transaction any subsequent increase will not exceed the allowable increased final amount

If there is a possibility that the final amount will increase above these levels after the customer has finalised the order, for example due to a product substitution, please refer to section 5.5.2.

5.5.1.1 Option 1:, Re-authenticate every time the customer adds to the basket, then process a delayed authorization

With this option, authentication is performed for the new total amount every time the customer edits the order.

As the amount will not vary after the customer initiated changes, if the transaction qualifies for an exemption, SCA challenges do not need to be applied, and the customer experience may be frictionless. In this case authentication should be requested through EMV 3DS with an appropriate exemption indicator.

This first option may be appropriate in cases where there is a high likelihood of qualification for an exemption, for example if the merchant knows the customer has added the merchant to their Trusted List supported by their Issuer or when the expected final value of the basket is such that the transaction should qualify for the Acquirer TRA exemption. Merchants should however be aware that an Issuer may choose to apply an SCA challenge, e.g. if it considers the transaction to be high risk.

Scenario Steps
Customer places an Order
1. Authenticate customer • The merchant ***authenticates*** *the transaction immediately for the initial order amount*, obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization).
2. Perform a zero-value *account verification* • The merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3. • (Only possible if the transaction is submitted via EMV 3DS - not direct to authorization)
Customer updates Order[150]
3. Re-authenticate customer • Each time the customer comes back to adjust the order, the merchant performs another ***authentication*** *for the new total cumulative amount*, obtaining a new CAVV or "enhanced TAVV" (and associated ECI value), discarding the initial one and keeping the latest one. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization). **4. Perform an additional zero-value *account verification* (optional)**

[150] Use and repeat steps 3 and optionally step 4 as often as the customer updated the order, If/when the customer does not update the order, skip to step 5 .

- The merchant may also optionally perform an additional zero-value *account verification* each time to check that the card is valid.
  - The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3.

Merchant ready to make shipment (Customer no longer available)

5. Submit delayed authorization with MRC 3903

- At time of shipping, the order is closed. The merchant ***authorizes*** *for the final amount*[151].
- The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework)
  - The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3 and the CAVV submission options summarised in Figure 21
    - If the customer has not updated the order, use the authentication data from Step 1. If the customer has updated the order, use the authentication data from Step 3
- If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3, Table 21, Principle 11.

6. Clear funds

- The merchant **clears** the transaction for the final amount.

Order Complete

5.5.1.2 Option 2: Authenticate at checkout for a highest estimated amount, then process a delayed authorization

The merchant can authenticate at initial checkout for a maximum estimated amount that would cover potential additions to the basket made by the customer at a later time. Whenever the customer edits the basket, no further authentication is required as long as the new total amount is below or equal to the authenticated amount in the EEA or the allowable increased final amount in the UK. If a change increases the total amount above the authenticated amount in the EEA or the allowable increased amount in the UK, a new authentication must be performed for the new total amount. Qualifying exemptions may be applied as described in the previous option.

This second option may be appropriate in cases where a transaction is less likely to qualify for an exemption. However, it may cause customer confusion/cart abandonment at authentication if the cardholder is unclear as to why they are being asked to authenticate for a higher amount than the checkout value of the goods or services ordered. If this option is selected it is essential to clearly communicate to the customer prior to authentication (i.e. prior to the presentation of the 3DS challenge window) that:

- They are being authenticated for an estimated maximum amount
- They will only be charged for what they purchase (which may be lower than the authenticated amount)
- No charges will appear on their card statement until the order is finalised

[151] The amount cannot be higher than the allowed variation above the authenticated amount. If there is any chance it could be, the merchant must select one of the options in section 5.5.2.

Scenario Steps
Customer places an Order

1. Authenticate customer
• The merchant ***authenticates*** *the transaction immediately for an estimated maximum amount* that the basket can have, obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization).
• The merchant must inform the customer that:
  • this is an estimated amount,
  • they will only be charged for what they purchase when the order is finalized
• Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization).

2. Perform a zero-value *account verification* • The merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" Transaction ID and store it for later use.   • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3.
Customer increases order value
Use and repeat step 3, and optionally step 4, each time the customer updates the order, If the customer does not update the order, skip to step 5. **3. Re-authenticate customer only if updated amount near or above original amount** • Each time the customer comes back to adjust the order, no further authentication is required unless the adjustment causes the order value to increase to near or above the originally authenticated amount. • In which case, a new ***authentication*** *must be performed for the new cumulative amount*, obtaining a new CAVV or "enhanced TAVV" (and associated ECI value), discarding the initial one and keeping this latest one. • Applicable exemptions can be exercised (only possible if the transaction is submitted via EMV 3DS - not direct to authorization). **4. Perform an additional zero-value *account verification* (optional)** • The merchant may also optionally perform an additional zero-value *account verification* each time to check that the card is valid.   • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3.
Merchant ready to make shipment (Customer no longer available)
5. Submit delayed authorization with MRC 3903 • At time of shipping, the order is closed. The merchant authorizes for the final amount[151]. • The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework)   • The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3 and the CAVV submission options summarised in Figure 21 • If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3 Principle 11.
6. Clear funds • The merchant **clears** the transaction for the final amount.
Order Complete

5.5.2 Customer adding to basket - final amount may change after the customer has finalised the order

This scenario covers the case when the amount could still vary after the customer has finalized the order:

- For an EEA transaction there may be a further increase in the amount over an above the amount of the final authentication
- For a UK transaction there may be an increase over and above the amount of the final authentication that exceeds the allowable increased final amount

These increases may be as a result of for example, product substitutions by the merchant or inclusion of in the order of weighed goods whose cost is not known until the goods have been picked.

For this scenario exemptions cannot be applied and SCA is required as d the merchant can use an MIT incremental as defined in option 1 in section 4.2.2.4.1 to process any additional amount beyond the one authenticated by the customer.

Scenario Steps
Customer places an Order
1. Authenticate customer The merchant **authenticates** the transaction immediately for • the initial order amount if option 1 (section 5.5.1.1) above was selected or • *an estimated maximum amount* that the basket can have if option 2 above (section 5.5.1.2) was selected, obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization. **With either option, the merchant must inform the customer that:** • this is an estimated amount, • they will only be charged for what they purchase when the order is finalized and must inform the customer **and get their consent that** • the final amount may be higher than estimated, either because cardholder may make addition to the basket and/or due to allowable variations within reasonable expectations (e.g. brand substitution, item not available etc.) • It is not permissible to use an exemption under this option, as authentication is necessary in order for the merchant to have the option of initiating an Incremental MIT at the time of shipping (see below). SCA must be requested by setting the 3DS Requestor Challenge Indicator to "Challenge Requested: Mandate (04)".
2. Perform a zero-value *account verification* • The merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. • The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3. • The Transaction ID for this authorization is stored for later use.
Customer updates Order
Follow step 3 and 4 from option 1 (5.5.1.1) or 2 (5.5.1.2) above depending on which was selected • Note that for both options, even if option 1 was selected, the merchant must inform the customer that: • this is an estimated amount, • they will only be charged for what they purchase when the order is finalized and must inform the customer and get their consent that

- the final amount may be higher than estimated, either because cardholder may make addition to the basket and/or due to allowable variations within reasonable expectations (e.g. brand substitution, item not available etc.)
- It is not permissible to use an exemption in order to skip authentication under this option, as authentication is necessary in order for the merchant to have the option of initiating an Incremental MIT at the time of shipping (see below).

Use and repeat steps 3 and optionally step 4 as each time the customer updates the order, setting the 3DS Requestor Challenge Indicator to "Challenge Requested: Mandate (04)" (exemptions cannot be used). If/when the customer does not update the order, skip to the appropriate step 5 .

Merchant ready to make shipment (Customer no longer available) - amount lower than the authenticated amount (or lower than the allowable increased final amount in the UK)

5. Submit delayed authorization with MRC 3903

- At time of shipping, the order is closed. The merchant ***authorizes*** *for the final amount*.
- The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework)
  - The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3 and the CAVV submission options summarised in Figure 21
    - If the customer did not update the order, use the authentication data from step 1
  - If the customer updated the order, use the authentication data from step 3.
- If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3, Table 21, Principle 11.

6. Clear funds

- The merchant **clears** the transaction for the final amount.

Merchant ready to make shipment (Customer no longer available)- amount greater than the authenticated amount (or greater than the allowable increased final amount in the UK)

5. Submit two authorizations

- At time of shipping, the order is closed. The merchant authorizes for the latest amount authenticated.
- The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework)
  - The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3. In this case, the CAVV must be present in the transaction to enable the processing of the MIT Incremental as Issuers may check that the transaction with the initial estimate was authenticated.
  - This transaction must include an "estimated indicator" as it will be followed by an Incremental transaction.[152]
  - If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.5.3 Principle 11.
- The merchant must **also submit a second authorization** for the additional amount not authenticated, but using the **message reason code 3900- MIT Incremental.**
  - The original transaction ID in this Incremental must refer to the delayed authorization that was just processed with the initial estimated indicator.[152]
  - The merchant must populate any applicable authentication-related data in the authorization message as per section 5.1.2.

6. Clear funds

The merchant **clears** the transaction for the final amount.

Order Complete

[152] Merchants should check with their Acquirers regarding the rules and technical requirements associated with the use of estimated/incremental transactions.

5.6 Aggregated payments

Visa rules define an aggregated payment as a single transaction that combines multiple purchases made by the same cardholder on the same payment credential (which may be updated from time to time) at the same merchant during a defined time period and up to a defined amount (refer to Visa rule ID # 0024270).

Visa allows aggregation of payments for ecommerce merchants, typically capped at 15USD (or local currency equivalent) or 7 days whichever comes first. However, these terms vary for some MCCs and some disclosure requirements and receipt requirements apply (refer to Visa Rule ID # 0002906 and # 0028052).

In this scenario, a merchant handles micro-payments and only charges the customer when reaching a pre-agreed total or at a specific time. The charge occurs when the cardholder is not available. The exact time and amount can vary based on market and MCC, but for the purposes of these examples a time limit of 7 days is used.

When considering how best to handle aggregated payments for their business model, the merchant can choose from the following options.

5.6.1 Option 1: Merchant sets up customer agreement to enable payments under MIT Unscheduled Subscription type (UCOF)

A merchant storing a Credential-on-File for aggregated payments could process orders as Unscheduled Credential-on-File (UCOF) MITs by setting up an agreement with the cardholder. This approach is suitable for use cases such as bike or car sharing, where the customer is not directly engaging with the merchant in a manner which allows authentication to take place. For further details see Section 5.14.3.

5.6.2 Option 2: Authentication for fraud liability protection

Scenario Steps
Customer makes purchase that triggers a new aggregation series
1. **Notify customer of payment levy conditions** • The merchant ***informs*** the cardholder that payment will be levied either when transactions cumulate to 15 USD (or local currency equivalent) or at 7 days, whichever comes first.
2. **Authenticate customer** • Merchant ***authenticates*** *for 15 USD (or local currency equivalent)* obtaining a CAVV or "enhanced TAVV" (and associated ECI value). • Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.2.
3. **Perform a zero-value *account verification*** • The merchant must perform a zero-value ***account verification*** to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. ○ The merchant must populate any applicable authentication-related data in the account verification as per Step A (account verification) in Section 5.1.3. ○
Aggregated value or time threshold reached (Customer no longer available)
4. **Submit delayed authorization with MRC 3903** • When either threshold is reached (15USD, or local currency equivalent – or 7 days, whichever comes first), the merchant ***authorizes*** *for the final amount*. • The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 3 (as per MIT Framework) ○ The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3 and the CAVV submission options summarised in Figure 21. • If the authorization is declined, as the goods and services have already been provided to the customer, the merchant may *resubmit* the transaction indicated with MRC 3903 to recuperate the funds, providing that the original decline response code indicates that the Issuer may approve a future transaction.
5. **Clear funds** • The merchant ***clears*** the transaction for the full cumulative amount.
Customer makes purchase that triggers a new aggregation series
6. **Restart from step 1**

5.6.3 Option 3: Authorize for the maximum amount upfront, authenticate only if required by the Issuer

Whilst it is possible for a merchant to immediately authorize for the full amount upfront, requesting a suitable SCA exemption and then only authenticating if required by the Issuer, and clearing the transaction when the 15USD total is reached or at 7 calendar days, this is not Visa's recommended approach, since it:

- Immediately impacts the customer's open to buy, in particular if the customer has limited cash flow
- Does not provide a convenient user experience when authentication is required
- Increases the chance that an Issuer will decline the transaction

Therefore, this approach should only be used if the merchant has no other option.

5.7 Real-time service via mobile app with payment after service /completion

In these scenarios, the customer is initiating a service via an app and paying for it once the service has been delivered without further interaction being needed with the app. Examples include:

- Ordering a car sharing ride via a mobile app
- Opening a fuel pump and buying fuel via a mobile app
- Electrical vehicle charging
- Parking app

In such cases, the amount can be estimated at the start, but the final amount is not known at the time of order. Payment is not made on booking, but at service completion.

The same applies to app based store entry and unattended service delivery scenarios which are summarized in section 5.8.

Note: The rest of this section is written keeping in mind that Unscheduled Credential-on-File (UCOF) MITs are not suitable for this type of scenario, since it involves a merchant/cardholder interaction via a mobile app where authentication is possible.

5.7.1 Option 1: Using exemptions

If the transaction qualifies for an SCA exemption an SCA challenge may not be required, and a frictionless experience may be offered. However, the final transaction amount cannot exceed the amount disclosed to the Issuer when the exemption is requested. This restriction applies in both the EEA and the UK. If the final amount is any higher, a new authorization, and possibly an associated authentication, will be needed.

Scenario Steps
Customer books/initiates service via use of an app
1. Terms and conditions must be clearly displayed [153] Customer must be notified - in the app - that upon initiating the service: • An amount of €x will be held/blocked (this amount must represent a genuine estimation of what the cardholder will spend) • This is only an estimate and if the final amount is less than €x, unused funds will be unblocked by the cardholder's bank once the transaction is processed. If the final amount is higher, there may be subsequent authorization requests - the cardholder agrees to pay the final amount as long as it is within the cardholder's reasonable expectation. Note: If this is the first time the credential is stored – also follow disclosure requirements for storing credentials
2. Authentication (optional as exemption may be requested direct to authorization, in which case skip to step 3) The merchant ***authenticates*** *the transaction for the highest estimated amount of the service at booking*, indicating the appropriate exemption and obtaining a CAVV or "enhanced TAVV" (and associated ECI value) for later submission in the authorization request.
3. Authorize transaction • Merchant ***authorizes*** *for the highest estimated amount of the service at booking*, claiming appropriate exemption and using the estimated amount indicator (refer to Base I Technical Specification Volume 1 for further details). o The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. (Refer to the authentication scenario "SCA exempted via authorization" in Table 35).
If the transaction is approved, skip to step 5 or 6, as applicable. If the Issuer responds with an SCA decline code (Response Code 1A), either follow step 4 here or step 1 from Option 2 (section 5.7.2) [154] **4. Authenticate customer in response to SCA decline code** (this may occur if exemption was requested direct to authorization and step 1 was skipped**)** • If the Issuer responds with an SCA decline code (Response Code 1A), the merchant must perform authentication for the highest estimated amount, obtaining the CAVV or "enhanced TAVV" and associated ECI value, and then request authorization again. The estimated indicator must again be populated in the authorization request.
Final value of service exceeds the estimated amount in Step 2, 3 or 4 [155]

[153] Refer to Visa Rule ID # 0025596 for requirements associated with the use of estimated/incremental

[154] Option 2 may be appropriate if there is a possibility that the final amount could exceed the estimated amount as it allows use of an MIT incremental to collect the additional amount

[155] In the UK only, if an SCA challenge has been applied and the final amount is within the allowable increased final amount as defined in section 4.2.2.3, skip this step and move to Step 6.

5. Submit reversal, authorize and clear final amount

- If the final amount is above the initially authenticated/authorized amount (Step 3 and/or 4), the merchant must ***Reverse*** the authorization from step 3 or 4[156]
- ***Authorize*** *for the final amount* using applicable exemption flags in Field 34.
  - The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1(refer to the authentication scenario "SCA exempted via authorization" in Table 35).
  - If no exemptions can be exercised or the Issuer responds with an SCA decline code (Response Code 1A), then the merchant must contact the cardholder (either sending a message or waiting for next usage of the app as most appropriate with business model) to authenticate prior to attempting another authorization. (If a CAVV was obtained in step 2 or 4 it is no longer valid as not covering the final amount and should not be used in this authorization).
  - If a decline is received for a reason other than an SCA decline code (Response Code 1A), the merchant may retry this CIT later in accordance with Visa's rule on merchant reattempt limits (up to 15 attempts in 30 days. Refer to Visa Rule ID # 0030640 for more details)

6. Clear funds

- The merchant ***clears*** *the transaction for the final amount*

An alternative to step 5 and 6 above is for the merchant to:

- Clear the initial authorization approved in step 3 or 4
- Authorize for the additional amount not yet authorized using an exemption as applicable
  - If no exemptions can be exercised or the Issuer responds with an SCA decline code (Response Code 1A), then the merchant must contact the cardholder (either sending a message or waiting for next usage of the app as most appropriate with business model) to authenticate prior to attempting another authorization.
  - If a decline is received for a reason other than an SCA decline code (Response Code 1A), the merchant may retry this CIT later in accordance with Visa's rule on merchant reattempt limits (up to 15 attempts in 30 days. Refer to Visa Rule ID # 0030640 for more details)

    while this alternative is possible. It is not the recommended one as in such case the cardholder will see two separate transactions on their account which may raise questions/potential chargeback requests

Final value of service lower than or equal to authorized amount[157]

7. Clear funds

- The merchant ***clears*** *the transaction for the final amount* -Note that if the initial authorization from step 3 was for a higher amount than the amount cleared, the merchant must also ***submit a partial reversal for the difference***. Please refer to Visa rule ID #0025597 for more information.

Order Complete

[156] An MIT incremental cannot be processed as an exemption was used. SCA is required in the initial estimated transaction if an Incremental is to be processed.

[157] In the UK only this may be within the allowable increased final amount as defined in section 4.2.2.3.

5.7.2 Option 2: Always authenticate at the start and use Incremental MIT to authorize an increase[158] above initial amount

Scenario Steps
Customer books/initiates service via the use of an app
1. Terms and conditions must be clearly displayed[159] Customer must be notified - in the app - that upon initiating the service: • An amount of €x will be held/blocked (this amount must represent a genuine estimation of what the cardholder will spend) • If final amount is less than €x, unused funds will be unblocked by cardholder's bank once transaction is processed If the final amount is higher than estimated, there may be subsequent authorization requests: the cardholder agrees to pay for the final amount as long as it is within the cardholder's reasonable expectation. Note: If this is the first time the credential is stored the merchant must also follow disclosure requirements for storing credentials.
2. Authenticate customer • Merchant ***authenticates*** *for initial or estimated amount at ordering*, obtaining a CAVV or "enhanced TAVV" (and associated ECI value) – an SCA challenge is required (i.e. the 3DS Requestor Challenge Indicator must be set to "Challenge Requested: Mandate (04)". Exemptions cannot be used if the merchant wishes the ability to process any incremental transaction later.

3. Authorize transaction with estimated indicator
• The merchant immediately ***authorizes*** *the transaction for the initial or estimated amount at ordering*, ***using the estimated indicator*** (no incremental transaction can be processed later unless preceded by an estimated authorization).
  • The merchant should check with their Acquirers to ensure they understand the rules associated with the use of Incremental transactions for their MCC.
  • The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1.
  • If this is the first transaction, the appropriate indicator ("C") must also be populated to indicate that credentials are being stored. For more information about the Stored Credential Framework and the requirements a merchant must meet, see Table 19 in Section 4.2.3 and Appendix A.1
• The Transaction ID for this authorization is stored for later use.

Final value of service is higher than amount of initial authentication/authorization[157] from steps 2 and 3
4. Perform an incremental authorization using the MIT Framework • If the final amount on service completion is higher than the amount initially authenticated and authorized but within the terms disclosed to the customer, , the merchant must perform an ***incremental authorization using the MIT Framework*** *for the additional amount not yet authorized in step 3.* • The authorization must include a message reason code of 3900 to indicate that the customer is no longer present and the Transaction ID from step 3 (as per MIT Framework).   • The merchant must populate any applicable data in the authorization message as per Section 5.1.2.

[158] Any increase above the initial authenticated amount in the EEA and any increase above the allowable increased final amount in the UK

[159] Refer to Visa Rule ID # 0025596 for requirements associated with the use of estimated/incremental

- Note that if a decline is received, the merchant may retry this MIT later in accordance with Visa's rule on merchant reattempt limits (up to 15 attempts in 30 days). Refer to Visa Rule ID # 0030640 for more details.

5. Clear funds

The merchant ***clears*** *the transaction for the final amount.*

Final value of service lower or equal to authorized amount[157] from step 3

6. Clear funds

- The merchant **clears** the transaction for the final amount.

Note that if the initial authorization from step 3 was for a higher amount than the amount cleared, the merchant must also submit a partial reversal for the difference. Please refer to Visa rule ID #0025597 for more information.

Order Complete

5.7.3 Option 3 – Only authorize upon service completion)

This option involves sending an authorization request for the final amount after the service has been rendered, similar to any ecom one time purchase. The difference is that as the cardholder is generally not readily available/involved at completion, this relies on the use of an exemption and if the Issuer declines the application of the exemption, it may not be possible to authenticate the customer and therefore may not be possible to collect any payment.

In this option,

1) The Customer must be notified at start that they agree to pay, with the card that is on file, for all items they purchase/service they use
2) At service completion, the transaction is sent as an unauthenticated e-com CIT, requesting an applicable exemption
   - Cannot be processed as an MIT as the cardholder is the one that initiated the use of the service and was available to authenticate then – this action thus generates a Cardholder Initiated Transaction (CIT) - albeit delayed until completion
   - If the exemption is accepted, the transaction will likely be approved (unless other reasons than SCA to decline)
   - If the Issuer does not agree with the exemption and sends an SCA decline, SCA will be required before the authorization can be retried/completed, this means trying to recontact the customer before proceeding with payment collection
   - If the transaction is declined for other reasons, the merchant may subsequently resubmit the transaction in accordance with Visa's rule on merchant reattempt limits (up to 15 attempts in 30 days). Refer to Visa Rule ID # 0030640 for more details.

5.8 App based store entry/unattended service delivery & purchase

This scenario covers retail and service delivery models when a merchant enables an "automated entry/no checkout experience". The customer's credentials are presented and the customer is authenticated (as appropriate) upon entry to the store or accessing an automated/unattended facility such as a smart fridge or self service car wash. The final amount that will be collected from the customer is not known at the time of entry/start. Various technologies including cameras, sensors and barcodes are used to detect the items the customer is purchasing and/or the services they are consuming. Once the customer has finished collecting their purchases or service delivery is complete, the customer can exit the store or leave the facility without having to visit a checkout. The access/authentication and payment experience is facilitated end to end through an App and is presented as a Card Not Present transaction.

When this experience is facilitated by credentials being captured at entry and payment is taken using a previously stored credential, the three options presented in section 5.7 can be used.

In evaluating which of the three options to adopt, merchants need to consider that physical goods or services may have already been provided to the customer who has left the store or facility when the transaction is finalized. If the final amount due cannot be authorized because SCA is required, the merchant may suffer a real monetary loss.

Note that just as in the scenarios described in section 5.7, the use of Unscheduled Credential-on-File (UCOF) MITs are not suitable since the scenario involves a merchant/cardholder interaction via a mobile app where the customer is initiating purchase/usage and is available to be authenticated.

Also note that it is possible for this shopping experience to be initiated through a card present experience (i.e. not app based) facilitated through a contactless or chip/dip transaction. Requirements in these cases differ slightly but are outside of the scope of this guide which focuses on remote transactions. Separate guidance will be provided by Visa on those use cases.

5.9 Omni-channel purchases

There are certain scenarios where a merchant chooses to deliver goods or services via a mixture of remote and face-to-face experiences. Such omni-channel use cases are becoming more and more common, and also need to be SCA compliant.

Key Point

The authentication for a delivery does not have to be performed online but can be delayed until later face-to-face interaction. Equally an authentication performed on-line can be leveraged to enhance later face-to-face delivery or in store pick-up of goods and services.

5.9.1 Reserve on-line, pay in store

A customer places an order via a website or mobile app but does not perform any authentication or authorization online. In this case, all authentication and authorization would be performed in store, as part of a face-to-face transaction. For example, a customer could reserve stock for collection within 24 hours at a general-purpose store, performing a Chip and PIN or contactless transaction at time of collection to meet SCA requirements.

5.9.2 Buy online, pick up in store (BOPIS)

A customer places an order via a website and complete authentication and authorization online (as per the one-time purchase scenario defined in Section 5.2).

The merchant would then need to have in place a mechanism to tie up the order with the customer at time of collection, for example:

- Purchase clothes online for collection in store, with customer presenting an order reference number or proof of ID to enable collection
- Buying cinema tickets online for collection from automated machines that use the card used to pay online to identify the customer and deliver the tickets

In this case, it is the online experience that manages authentication and authorization, therefore the transaction is treated as eCommerce, not face-to-face.

5.9.3 Pay in-app when in store

A customer uses a mobile app check-out experience to pay for goods in store. From a transaction authentication point of view, this should be considered the same as BOPIS. The in-app transaction is the environment where authentication and authorization are performed, and therefore the transaction is treated as eCommerce, not face-to-face.

5.9.4 Pay in store for home delivery

A customer purchases goods in store for home delivery, completing the authentication and authorization face-to-face, but with the order being fulfilled through the merchant's eCommerce home delivery processes. For example, a customer wishing to buy a pair of shoes goes into a store, but their size is out of stock. The merchant guides them through a process using a tablet-based POS to purchase the desired size for home delivery. Payment is completed with the merchant face-to-face as a Chip and PIN transaction or contactless as appropriate, meeting SCA requirements.

5.10 Resubmission of declined authorization on contactless transit transactions

Resubmissions are a type of MIT whereby the merchant can re-submit a previously declined authorization due to lack of funds in the case **of contactless transactions performed in the transit environment where a service has already been delivered**. For example, if a cardholder taps into a mass transit gate with their Visa card or token on a mobile device, but at the end of day authorization is declined by the Issuer due to lack of funds. In these circumstances, the Mass Transit merchant is allowed to resubmit the authorization after an agreed period of time to attempt to collect the funds owed. In this case, the original CIT is exempt from SCA under the unattended terminals for transport fares and parking fees exemption and the Resubmission (which can only be performed as card not present since the contactless authentication data has already been used once) is simply an attempt to complete that already exempted transaction. Therefore, no SCA data needs to be included in the resubmission.

The merchant must identify the Resubmissions using the Transaction ID from the declined contactless authorization for the original Transaction ID.

Table 39: Resubmission

Description	Transaction Type	POS Entry Mode (PEM) (F22)	POS Environment (F126.13)	Message Reason Code (F126.13)	Original Transaction ID (F125[160])
Resubmission	First Transaction (CIT)	07[161]	--	--	--
	Subsequent Transactions (MIT)	01[162]	--	3901	Tran ID of First transaction

[160] Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that participate to receive Field 125.

[161] Associated chip data must be present in the transaction.

[162] Chip data must not be present in this transaction.

Key Point

Resubmissions **must not** be used for declined authorizations *where the services (or goods) have not yet been delivered*. For example, a customer attempts to purchase goods online at a merchant; however, the authorization is declined due to lack of funds. At this point, the goods have not yet been shipped. In this case, for the transaction to complete, the customer must either provide a different payment credential or replenish funds prior to the merchant submitting a new authorization request.

In the case of an MIT other than Resubmission being declined, a Resubmission must never be used. For example, if a merchant charges in advance for a service subscription using a recurring MIT. If the recurring transaction MIT is declined, depending on the decline response code, the merchant may later attempt a new authorization request as a recurring MIT for that subscription charge, until it is either approved or a maximum retry limit is reached. Refer to Visa's rule on merchant reattempt limits (Visa Rule ID # 0030640) for more details.

5.11 Accessing stored credentials using QR codes

Some merchants provide proprietary closed-loop payment solutions through their mobile app by enabling the customer to initiate a transaction using a QR code[163]. Examples include apps that generate a QR code which can be presented to the merchant in-store, or apps that read a QR code printed on a utility bill or similar payment request. The QR code subsequently enables the merchant back-end systems to identify a stored credential. Such an approach enables the merchant to enrich the customer experience by providing mobile app features such as loyalty.

Merchants using this kind of solution must be aware that as with CITs using stored credentials, such transactions still require SCA, or an applicable exemption. The precise means by which a merchant achieves this will be implementation specific, but Visa provides a number of tools that could help:

- **3D Secure:** Integration with 3DS can meet SCA requirements and EMV 3DS 2.1.0 and above is optimized for mobile-based solutions.
- **Delegated Authentication:** Both 3DS and the Visa Token Service can be used to enable participation in the Delegated Authentication Program, giving merchants the opportunity to control the SCA experience for their customers. For more information on Visa Delegated Authentication, please see section 3.6.
- **Use of the Trusted Beneficiaries Exemption:** Encouraging customers to register the merchant as a trusted beneficiary with their Issuer, where the Issuer supports the exemption, to maximize the possibility of being able to exercise the trusted beneficiary exemption[164]

[163] There is an EMVCo Specification for supporting open-loop in-store payments using QR codes, but it is only supported in a limited number of global markets, none of which are in the European region.

[164] Note that Issuers are not obliged to provide a trusted beneficiary capability and those that do may still choose not to apply it for every transaction where it is requested

5.12 Establishing a new agreement for future MITs

Upon establishing an agreement to process future MITs, a merchant must authenticate and authorize for the amount being collected at the time of the agreement and disclose appropriate T&Cs related to the agreement as described below. In a few select cases, SCA may not be required if an exemption can be applied. Please refer to Section 3.8 for information on those specific cases.

5.12.1 SCA is required by merchant to set up new agreement via a remote channel

Scenario Steps
Customer Signs up to a new agreement for future merchant-initiated payments
1. **Cardholder accepts T&Cs for MIT agreement** • The merchant discloses to the cardholder appropriate T&Cs and follows other requirements associated with the future MIT type it will process. • The customer must explicitly accept the T&Cs for the agreement to proceed.   • Merchants should discuss with their Acquirers and be familiar with the rules, including all disclosure requirements, associated with their MIT types. For more information, see Appendix A.1, Appendix A.3 and Section 5.14.

2. **Authenticate customer**
• When setting up an agreement to process future MITs, the merchant **authenticates** for the amount due immediately only (if no amount is due, authentication must be performed with "zero" as the amount) as per Section 4.2.5.3, Principle 16, applying SCA.
• **Note**: An SCA challenge must be requested by setting the 3DS Requestor Challenge Indicator to "Challenge Requested: Mandate (04)" SCA exemptions cannot be exercised when setting up a new MIT agreement via a remote channel except:
  • For Reauthorization and Resubmission MITs, where applicable exemptions can be exercised in the original CIT used to set up future MITs of these types.
  • During a booking made via a secure corporate payment process that qualifies for application of the secure corporate payments processes and protocols exemption.
Refer to Section 3.8 for details on the use cases where exemptions can be used.

3. **Authorize transaction**
• The merchant ***authorizes*** *for the amount due immediately (which, as noted above, must be zero if no amount is due)* and populates any applicable authentication-related data in the authorization message as per Section 5.1.1 or 5.1.3 in the case of reauthorization MITs, taking into account the fact that SCA exemptions cannot be exercised when setting up a new agreement (except in the cases stated in Section 3.8).
  • The merchant must store the Transaction ID of this authorization for later use as the Initial Tran ID in future MITs [165].
  • If zero, or a discounted, amount is due immediately (e.g. as part of an introductory/promotional offer), then authorize only for the amount due immediately (i.e. for zero or discounted amount) as per Section 4.2.5.3, Principle 16.
  • This first authorization is the CIT used to establish the agreement for future MITs and should be indicated as per the key data fields detailed in Section 3.8.3.2 Table 15

[165] If the agreement was established prior to 14 September 2019, then Grandfathering applies. See Section 4.2.5.3, Principle 16

- If the authorization is approved, the payment credentials can be stored for future use according to the Stored Credential Framework if appropriate (see AppendixA.1) 166.
- If the transaction is declined, the credentials cannot be stored and the agreement is not considered to be in place.
- If the credential is not stored under the Stored Credential Framework, the details can be kept but only as long as required in order to complete the current transaction agreement (e.g. to process any Industry Specific MITs such as No Shows, Incremental Authorizations or Resubmissions).

Customer uses service leading to additional payments

4. **Authorize using MIT Framework**
   - Depending on the MIT type, the merchant must communicate with the cardholder, if required for the MIT type, prior to processing an MIT (see Section 5.14 for examples).
   - Merchant ***authorizes*** MITs, identified as shown in Section 3.8.3.2 Table 15 . The initial Tran ID to use is the one generated in step 3 or the Tran ID of a previously approved MIT can be populated instead, or until 31 October 2023 if the merchant does not have any previous Tran ID available, a Visa Acquirer-assigned interim Tran ID can be used if supported by the Acquirer[167].
   - *The amount in future MITs may vary from the original amount as long as the amount calculation method is disclosed to the customer in the T&Cs of the established agreement and the amount authorized is within reasonable customer expectation.*
   - It is important for merchants to be aware, however, that MITs do not generally have fraud liability protection under the Visa Rules[168]. No CAVV or TAVV is required to be included in the authorization, as the MIT is out of scope of SCA. Refer to Section 5.1.2 for more information.

5. **Clear funds**
   - Merchant **clears** the transaction for the final amount in the MIT.

5.12.2 MIT agreements established by mail order or telephone order (MOTO)

Sometimes a cardholder establishes an agreement with a merchant over the phone, by mail or email. In those cases, setting up the agreement is recorded as a MOTO type transaction. When this is the case, it is important for merchants to remember that the subsequent payments made under that agreement must be indicated as MITs. They can also be indicated as MOTO but this alone is not sufficient. The following also applies:

- When an agreement is initiated via MOTO, this initial CIT is to be indicated as MOTO and is out of scope of SCA. The subsequent ongoing transactions must be indicated with the appropriate MIT type using the Visa MIT framework (see Section 3.8 for more details). MITs are considered by Visa out of scope of PSD2, so SCA is not required.

[166] The credential must be stored according to the Stored Credential Framework for Standing Instruction MITs. For industry best practice, use of stored credential depends on the situation.
[167] For any usage between August 2022 and 31 October 2023, non-compliance assessment fees (NCAs) may apply to Acquirers. Refer to section 3.8.2.3 for more details.
[168] With the exception of MIT reauthorizations where a CAVV or TAVV is included in the transaction and MIT Incremental which, if approved, will have the same protection granted to the initial estimated transaction. Refer to section 5.1.2 for more details.

Key Point

When setting up an MIT agreement via the MOTO channel, MOTO is only valid for the initial transaction when the agreement is established. Afterwards, the ongoing payment must be identified as an MIT. This transaction can be indicated as MOTO but this is not sufficient – the MIT indicators from the Visa MIT Framework must be present in the transaction

Table 40 below summarises the differences between how merchants should treat and indicate MOTO, MIT setup and ongoing MIT transactions.

Table 40 MOTO vs MIT transactions

	Transaction Type			
	MOTO Single Purchase Transaction	MOTO transaction to set up an MIT	Ecomm transaction to set up an MIT	Subsequent MIT transaction
SCA requirements	SCA not required as MOTO is out of scope	SCA not required as MOTO is out of scope	SCA is required when setting up and MIT via a remote channel	SCA not required as MITs are out of scope if SCA was applied at mandate set up
Required indicators[169]	• POS Condition Code (F25) = 08 and/or ECommerce Indicator (F60.8) = 01 or 04. • No value required in POS Environment (F126.13) except if a credential is being stored at same time as the transaction, in which case a	• POS Condition Code (F25) = 08 and/or ECommerce Indicator (F 60.8) = 01 or 04. • If mandate setup is for Recurring, Installment or UCOF – appropriate value (R, I or C) must be present in POS	• POS Condition Code (F25) = 59 (ecom) or 51 (account verification[170]) • If mandate setup is for a standing instruction MIT, i.e. Recurring, Installment or UCOF, appropriate value (R, I or C) must be present in POS Environment (F126.13)	• MIT Framework indicators •Value must be present in Field 126.13 (R, I or C) or Field 63.3 (3900 – 3904) •Transaction ID must be present in F62.2 (for Acquirers) or F125. • Applicable values in POS

[169] Refer to *VisaNet Authorization-Only Online Messages – Technical Specifications* for a full definition of the fields and values that need to be populated for these transaction types. This table only defines the indicators required to identify and differentiate between MOTO, MIT set up and subsequent MIT transaction types.

[170] To be used when no payment is due at time the MIT is being set up.

	Transaction Type			
	MOTO Single Purchase Transaction	MOTO transaction to set up an MIT	Ecomm transaction to set up an MIT	Subsequent MIT transaction
	value of C is required	Environment (F126.13)		Condition Code (F25), i.e. : •08 is one of those possible value if the initial CIT was MOTO •Values 02 (Recurring) or 03 (Installment) may be used in F60.8 but are not required outside of the USA. In Europe if 02 or 03 are used – they are not sufficient and the MIT Framework must also be used
Best practices/requirements in an SCA context	Merchants must clearly indicate MOTO Transactions and not include any indicators that can result in Issuers confusing the intent of the transaction. •MOTO indicators must be used as specified in "Required Indicators" above •F60.8 **must not be** 02 (Recurring) or 03 (Installment) as these values are to be used only with transactions that are MITs – use of these values here may confuse the Issuer and result in a decline •VisaNet authorization specifications do state that value 01 or 04 are optional for MOTO transactions[169], however for clearer intent to the Issuer,		Merchants must clearly indicate when an MIT Mandate is setup via ecomm or Account verification (0$ Authorization) using the "Required Indicators" specified above	MIT indicators defined in the Visa MIT Framework must always be used when the MIT is submitted, even if the MIT was set up via MOTO (in which case MOTO indicators may also be used)

	Transaction Type			
	MOTO Single Purchase Transaction	MOTO transaction to set up an MIT	Ecomm transaction to set up an MIT	Subsequent MIT transaction
	Acquirers that populate an "08" in F25 are recommended to also populate value 01 or 04 in F60.8			
		Merchants must indicate the transaction is for an MIT set up using the Required Indicators specified above		

Merchants should work with their Acquirers to ensure that transaction types are correctly used and indicated as per the Visa specification.

5.12.3 Using a stored credential established by MOTO

A merchant may obtain via the MOTO channel a cardholder's credential for storage and future use. It is important for merchants to understand that any subsequent CITs using a stored credential established over MOTO must be indicated according to the circumstances of the current transaction. For example:

- When a stored credential is established via MOTO, this initial CIT is to be indicated as a MOTO and as MOTO transactions are out of scope of PSD2, SCA is not required.
- Any future CITs initiated using that stored credential must be indicated according to the channel over which that transaction is being performed. For example, if over the phone, the transaction can be indicated as MOTO and is out of scope; if initiated via the merchant website, it must be indicated as eCommerce with stored credential and SCA is required unless the transaction qualifies for a suitable exemption.
- If the credential is obtained for use in future MITs, refer to Section 5.12.2 above

The fact that a transaction uses a stored credential previously obtained via MOTO does not mean it can be considered a MOTO transaction for the purposes of SCA. Each transaction which uses stored credentials must be evaluated according to the circumstances of that transaction whether the card details were stored or are entered only for the completion of that transaction is irrelevant to the SCA or no SCA decision.

Key Point

Each transaction must be evaluated for its own circumstances. A transaction using credentials previously obtained via MOTO is not necessarily a MOTO transaction.

5.12.4 Agreements established prior to PSD2 RTS for SCA coming into effect

If a merchant has an agreement in place prior to the regulatory enforcement date for any kind of MIT (standing instructions or industry specific) then the merchant does not need to establish a new agreement with the customer. However, the merchant is required to ensure ongoing payments are submitted in accordance with the MIT Framework for Issuers to recognize those transactions as being out of scope. To do this, the merchant must store the Transaction ID of the payment processed to set up the agreement or one of the payments processed under the agreement and dated prior to the regulatory enforcement date so that it can be used as the "initial Tran ID" for all future transactions using the MIT Framework. This process is known as "grandfathering". If the merchant does not have any previous Transaction ID available, until 31 October 2023, a Visa Acquirer-assigned interim Transaction ID can be used if supported by the Acquirer. Refer to Section 3.8.2.3 for more details.

Best Practice

Merchants using an interim Tran ID (or their gateway provider or Acquirer) must, prior to 31 October 2023, be in a position to store a valid Tran ID of an MIT that was populated with the interim identifier and successfully approved. This will enable the merchant to start using a valid Tran ID instead of the interim one for MITs initiated after the final date of usage of the interim Tran ID. Note that usage of the Interim Tran ID beyond 1st August 2022 is considered non-compliant and may attract non-compliance assessment fee.

5.13 Changing agreement payment terms

A change to the payment terms of the ongoing agreement sometimes may need to be instigated by either the merchant or the customer. SCA is always recommended in those situations but the merchant may opt not to authenticate if certain conditions apply as described in each scenario.

5.13.1 Merchant driven agreement changes

For merchant driven changes to payment terms, authentication is not required provided that the original agreement T&Cs and other cardholder communications clearly cover the eventuality of such changes. If not, SCA is required.

Example changes include:

- The price changes (e.g. due to inflation or other changes for example in the calculation method of the amount)

- The date or frequency of payment changes (e.g. moving from a monthly to yearly billing model)

When a change is made, existing requirements for disclosure and cardholder consent apply, as applicable to the type of agreement.

Note that whether authentication is required or not, the merchant must notify cardholders 7 days before any changes to the agreement, including date of payment or how the amount is calculated. For more information, see Visa Rule ID # 0029267.

5.13.2 Customer driven agreement changes

Examples of customer driven changes to payment terms include:

- Changes to pricing or terms, such as
  - Package (e.g. switch from premium to standard or vice versa)
  - Change of billing cycle (e.g. from monthly to yearly)
- Pausing or stopping and then restarting a subscription, such as
  - A subscription is paused by a customer to be restarted at an unknown later date
  - Customer agrees to pause a subscription and resume at a certain date (e.g. "I'm going away for 3 months, please pause my service contract until I return".)
  - Customer explicitly cancelled a subscription, but later returns as a customer

Whether the customer requests a change to pricing and terms or pauses or stops and then restarts an agreement, authentication is not required provided that the agreement T&Cs clearly cover the eventuality of such changes and the merchant has appropriate risk management in place. If there is any doubt that the T&Cs cover the change or if there is a risk of fraud, then the change should be treated in the same way as setting up a new agreement. As there is an existing relationship between the merchant and the customer, merchants with appropriate risk management in place may decide to use the approach to establish a new agreement as described in Section 5.12.

Key Point

If a customer with an existing agreement requests to change the card used to pay for the agreement, or takes any other remote action with a risk of payment fraud, then this is considered the same as setting up a new agreement.

5.14 Executing payments based on established agreements

Once an agreement has been established then the merchant can use that agreement to execute payments, within the T&Cs of that agreement. The following sections give examples of the different types of MIT that a merchant could use, depending on the use case they are looking to deliver.

Key Point

MITs are out of scope of PSD2 SCA, therefore no SCA is required provided the initial CIT used to set up the agreement has been performed in accordance with Section 5.11. This remains the case for as long as the agreement is in force. There is no time limit after which SCA must be reapplied. If the agreement changes, then in some cases SCA may be required, as outlined in Section 5.13.

5.14.1 Installments and prepayments

Installments are payments made in the case where the customer establishes an agreement to pay for goods received in one or more installments over an agreed period. In Visa systems these are known as "Installment/Prepayment". For example:

- A cardholder places an order with an electrical retailer for a TV costing €600. The consumer agrees to a consumer credit agreement requiring them to make an initial payment of €100 on placing the order followed by a series of 5 monthly installment payments of €100.
- Prepayments are payment(s) made towards a future purchase of goods/services. For example:
  - A cardholder orders a piece of furniture and agrees to pay a deposit at the time of ordering, with the balance due when the sofa is delivered.

Scenario
Customer agrees Installment plan or prepayment
1. **Set up new MIT agreement** • The merchant ***sets up a new agreement*** in accordance with Section 5.12 and using the Installment/Prepayment MIT type "I" in the authorization request. Note that this could include the taking of an initial payment or deposit.
Date of next payment arrives
2. **Authorize using MIT Framework** • The merchant[171] ***authorizes*** at the time interval and for *the amount defined in the Installment/prepayment agreement*. The transaction must be identified as an Installment/prepayment MIT subsequent transaction (see Table 14) ○ The merchant must populate any applicable data in the authorization message as per Table 15 and 16 and Section 5.1.2. 3. **Clear funds** • The merchant ***clears*** *the transaction for the amount based on the Installment/prepayment agreement.*
Payment schedule complete

[171] It is possible that the merchant processing the Installments with which the customer has an agreement and the retailer providing the goods could be different.

For more information on rules applicable to Installments and Prepayments, see Visa Rule ID # 0029267. Key highlights as of October 2022 are as follows:

If the cardholder cancels within the terms of the cancellation policy, the merchant or its agent must provide to the cardholder both of the following within 3 business days[172]:

- Cancellation or refund confirmation in writing
- Credit Transaction Receipt for the amount specified in the cancellation policy

If an Authorization Request for a subsequent payment is declined, the merchant or its agent:

- Must notify the Cardholder in writing and allow the Cardholder at least 7 days to pay by other means.

A merchant or its agent must **not**:

- Process an initial Installment Transaction until the merchandise or services have been provided to the Cardholder
- Process individual Installment Transactions at intervals less than 7 calendar days

5.14.2 Subscriptions at fixed interval

These are payments for the delivery of ongoing goods or services. They have a **fixed interval** for each payment, but the amount can be fixed or variable, as established in the merchant customer agreement. In Visa systems these are known as "Recurring" payments Examples include:

- Regular payments for a magazine subscription
- Regular payments for an on-demand digital entertainment service
- Monthly mobile phone or utility bill payments
- Quarterly payment for a gym membership

When setting up an agreement that also includes an initial charge (e.g. a magazine subscription), the merchant should only authenticate and authorize for the amount due immediately, as explained in Section 5.12. However the amounts to be paid later on a recurring basis must be clearly disclosed to the cardholder at the time the credentials are requested/entered.

Several rules apply to recurring payments. For more information see Visa Rule ID # 0029267. Key highlights as of October 2022 are as follows:

Using the method of communication agreed with the cardholder, the merchant must inform the cardholder of the following:

- Provide the cardholder with confirmation that a Recurring Transaction agreement has been established within 2 business days.

[172] For prepayments, if the Cardholder does not cancel (or pay the remaining balance, if applicable) within the terms of the cancellation policy, the Merchant may retain the prepayment(s) only if the Merchant has disclosed on the Transaction Receipt that the prepayment is non-refundable.

- Provide the fixed dates or regular intervals on which the transactions will be processed (not to exceed one year between transactions)
- Provide notification to the cardholder at least 7 working days before taking payment:
    - In the event of a trial period, introductory offer, or any promotional activity has expired, or
    - If more than six months have elapsed since the previous transaction in the series

At the same time as providing these notifications, the merchant must advise the cardholder how to cancel the agreement with the merchant. A simple cancellation procedure, and, if the cardholder's order was initially accepted online, at least an online cancellation procedure must be available.

A merchant must not complete a recurring MIT:

- Beyond the duration expressly agreed by the cardholder
- If the cardholder requests that the merchant or its agent change the payment method
- If the cardholder cancels according to the agreed cancellation policy
- If the merchant receives a Decline Response

Finally, the following are best practices a merchant should consider implementing:

- Remind the cardholder of the upcoming payment one or two days ahead of the payment even if payment is on a regular or fixed date. This is not only a positive experience for the cardholder but maximize chances of funds being available
- Check the Visa Account Updater (where available) before submitting the transactions. The service provides payment card updates, which means that merchants can avoid declines due to expired cards and other costs and inconveniences associated with re-issued cards
- Take care to ensure that the correct expiry date is included with each transaction. Issuers may choose to decline transactions if this is incorrect or missing.
- Should not submit a recurring transaction through more than one Acquirer unless the names used (line 1 & 2 of the statement narrative and/or MID) are identical
- Should not submit incorrect or misleading authorization data in an attempt to avoid a stop instruction placed against a card

Scenario
Customer signs up for ongoing service or subscription
1. Set up new MIT agreement • The merchant ***sets up a new agreement*** in accordance with Section 5.12 and using the Recurring MIT type. • For recurring payment there is a requirement to ensure the amounts to be paid both at time of set up and later on a recurring basis are clearly disclosed to the customer on the page or screen where the credential is requested/entered.
Customer receives regular goods or service
2. Customer receives regular goods (e.g. monthly magazine), or service (e.g. access to on demand video content, mobile phone connectivity).
Agreed payment interval reached
3. Authorize using MIT Framework • The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029267) • The merchant ***authorizes*** *the amount based on the recurring payment agreement* at the pre-agreed interval as a Recurring MIT subsequent transaction (see Table 14) . o The merchant must populate any applicable data in the authorization message as per Table 15 and 16 and Section 5.1.2. **4. Clear funds** • The merchant ***clears*** *the transaction for the amount based on the recurring payment agreement.*
Customer ends agreement

5.14.3 Signing up for services charged at irregular intervals (usage based)

This is the type of agreement where the amount and/or the time period between payments is variable and cannot be defined at the time of agreement. Payment is usually triggered based on usage. In the Visa systems these are known as "Unscheduled Credential on File" payments (Refer to Table 14 for further details). For example, a customer might sign up for:

- Top-up for a prepaid account when balance reaches a pre-agreed level (e.g. mobile phone or Mass Transit).
- An ongoing delivery agreement for a service such as groceries (e.g. reserving a weekly time slot for delivery of groceries with the facility that the time slot may be changed or cancelled, and items can be added to basket until a pre-agreed cut off time).
- A bike or car share scheme where payment is made based on usage.
- Transport services such as usage of a transponder or other device for road tolling or unattended parking where payment is made based on usage.
- Receipt of a "basket of goods" on a regular basis from which the customer decides which items to keep and returns unwanted goods. The merchant charges upon

receipt of unwanted items or after an agreed time period, whichever comes first, for the items not returned.

- A snow clearance service where the driveway of a customer is cleared by the merchant after each snowstorm in the winter months.
- Aggregated payments using a stored payment credential (e.g. purchases from a mobile app store)

This can only be treated as an MIT where the cardholder is not directly engaging with the merchant, in a manner which allows authentication to take place.

Several rules apply to Unscheduled Credential on File payments. For more information see Visa Rule ID # 0029267. Key highlights as of August 2022 are as follows:

- Using the method of communication agreed with the cardholder, a merchant must provide notification to the Cardholder of any change in the agreement, including, but not limited to, any change in the way the amount of the transaction may be calculated, at least 2 working days before the change.
- A simple cancellation procedure, and, if the cardholder's order was initially accepted online, at least an online cancellation procedure must be available.

A merchant must not complete a recurring MIT:

- Beyond the duration expressly agreed by the Cardholder
- If the Cardholder requests that the merchant or its agent change the payment method
- If the Cardholder cancels according to the agreed cancellation policy
- If the merchant receives a Decline Response

Finally, the following are best practices a merchant should consider implementing:

- Check the Visa Account Updater (where available) on a regular basis. The service provides payment card updates, which means that merchants can avoid declines due to expired cards and other costs and inconveniences associated with re-issued cards
- Take care to ensure that the correct expiry date is included with each transaction Issuers may choose to decline transactions if it is incorrect or missing
- Should not submit a recurring transaction through more than one Acquirer unless the name used (line 1 & 2 of the statement narrative and/or MID) are identical
- Should not submit incorrect or misleading authorization data in an attempt to avoid a stop instruction placed against a card

Scenario
Customer and merchant establish agreement
1. Set up new MIT agreement • The merchant ***sets up a new agreement*** in accordance with the options in Section 5.12 and using the Unscheduled Credential on File (UCOF) MIT type.
Customer consumes goods or service
2. The customer receives goods or consumes service at any time. No further authentication or authorization is required.
Merchant ready to request payment
3. Authorize using MIT Framework • The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029267) • The merchant ***authorizes*** *an amount based on the agreed method of calculation in the agreement* as a UCOF MIT subsequent transaction (see Table 14).   • The merchant must populate any applicable data in the authorization message as per Table 15 and 16 and Section 5.1.2. **4. Clear funds** • The merchant **clears** the transaction for the amount based on the agreed method of calculation in the agreement.

5.14.4 Processing a purchase at the same time as establishing a new agreement

In this scenario, a merchant may give a customer the option to sign up for a Standing Instruction (recurring, installment or UCOF) at the same time as making another purchase. For example, a customer could:

- Purchase a phone and at the same time sign up for a monthly data plan
- Purchase a DVD and also sign up for ongoing streaming payable monthly
- Buy a book and sign up for weekly paper or digital magazine at the same time
- Purchase a mobile phone and a care agreement for that phone
- Booking a holiday trip and subscribing to a travel membership scheme paid on a monthly basis[173]

[173] For all travel-related scenarios, please also refer to the Visa Guide: *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality*

Scenario
Customer checks out and agrees to ongoing payments
The merchant must ensure to clearly disclose all terms and conditions including the following on the page/screen where the credential is requested/entered • The amount (and currency) due that day for the purchase and • The amount due as per the recurring payment agreement (amount and when). **1. Authenticate customer** • The merchant ***authenticates*** *the transaction immediately for the amount due that day* (total for purchase and agreement), obtaining a CAVV for later submission in the authorization (unless a reauthorization MIT is being set up in which case refer to section 4.2.4) • As the establishment of an agreement requires explicit cardholder authentication, exemptions cannot be exercised in most cases (refer to Section 3.8 for the cases where exemptions can be applied).
2. The merchant can choose one of the following options: **(a)** Perform a single ***authorization*** *for the full amount due that day* **(b)** Perform two separate ***authorizations*** *for purchase amount* and *agreement amount* respectively • In case of **option (a)**, the merchant performs a single ***authorization*** *for the full amount due that day*, and populates any applicable authentication-related data in the authorization message as per Section 5.1.1. • This authorization must be indicated as the initial CIT for enabling subsequent MITs (see Table 15). • The Transaction ID of this authorization must be stored for usage in the future MITs. • The receipt for this transaction must fulfil all obligations for both the agreement and the purchase. • It is recommended that the transaction be cleared as a single amount but with the receipt clearly breaking down into the amount charged for the purchase and the amount for the agreement to avoid customer confusion. • In case of **option (b)**, the merchant performs two separate ***authorizations*** *in succession* and ***clears*** two transactions as below: • ***An authorization for the purchase***. The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. ▪ As this transaction is not being used to establish the agreement, any applicable exemptions can be exercised. • ***An authorization for the amount due today related to the agreement***. The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. ▪ As the establishment of an agreement requires explicit cardholder authentication, exemptions cannot be exercised in most cases. ▪ This authorization must be indicated as the initial CIT for enabling subsequent MITs of the appropriate type (see Table 15). ▪ The Transaction ID of this authorization must be stored for usage in the future MITs. ▪ The CAVV and associated ECI value must also be submitted with this transaction as proof of authentication if required for the agreement.
Customer uses service
3. Authorize using MIT Framework • The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029267) • The merchant ***authorizes*** future MITs • The merchant must populate any applicable data in the authorization message as per Table 15, 16 and Section 5.1.2.

- The amount in future MITs may vary from the original amount as long as the amount calculation method is disclosed to the customer in the T&Cs of the established agreement.
- The merchant performing the MIT could be different to the merchant that performed the CIT, provided the conditions outlined in Section 5.17.1 are met.

4. **Clear funds**
   - The merchant **clears** the transaction for the amount in the MIT.

5.15 Visa Direct payment

Visa Direct is a real-time push payment platform designed to facilitate real-time payments to accounts globally. Visa Direct enables person to person (P2P) payments and can also be used by companies and public institutions for funds disbursements.

Transactions associated with the Visa Direct service fall into two categories:

i. Original Credit Transactions OCTs; used to "push" funds to a Visa cardholder's account

ii. Account Funding Transactions (AFTs); used to "pull" funds from a Visa cardholder's account

Refer to Section 4.10 for definitions of these transaction types and guidance on when SCA is and is not required.

5.15.1 Example Visa Direct use cases and use of OCTs and AFTs

Table 41 summarizes examples of push payment services that are supported by Visa Direct, indicating whether an AFT and/or OCT is used:

Table 41: Example use cases showing usage of AFT and OCT

Example	Description	AFT	OCT
Peer-to-Peer (P2P) money transfer	Customer (A) sends money from their payment card to be credited to the payment card of customer (B), via a payment service.	Yes	Yes
Prepaid load	Customer (A) loads money into a prepaid card, e-money or stored value account held by a third-party financial institution using their Visa payment card as a funding source	Yes	No
Funds disbursement	General, business and government-initiated funds disbursements including for example: • Reimbursements • Refunds • Rebates • Pay-outs • Loan distributions • Government disbursements	No	Yes

5.15.2 OCTs and SCA

OCTs are identified by Field Value 26 in Authorization Field 3.

OCTs do not require SCA to be performed on the recipient of the funds. Therefore, an Issuer may not use SCA decline code (Response Code 1A) in response to authorization requests properly identified as OCTs.

These transactions should be indicated by transaction originators using code value 26 in Field 3.

Issuers can identify an OCT by checking for the processing code value of 26 in Field 3.

5.15.3 AFTs and SCA

AFTs are identified by Field Value 10 in Authorization Field 3.

AFTs are processed as e-commerce transactions and therefore the 3DS and Authorization flags and flows, as well as the tools and services (such as the Visa MIT Framework) described in Section 3 apply to AFT transactions in the same way as other remote electronic transactions. This is true whether the transactions originated through ISO messages or via the Visa Direct AFT API.

As per Section 4.10.3, AFT transactions are in scope of SCA and therefore authentication must be performed, or a suitable exemption exercised. For example, if the AFT is a single transaction of a known amount to fund a one-time payment, the process described for a one-time purchase in Section 5.2 should be followed, but with the additional inclusion of the value 10 in Field 3.

5.16 B2B payments

Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are not consumers. This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers. This is referred to as the Secure Corporate Payment (SCP) exemption.

More detailed guidelines for merchants, intermediaries, Acquirers and Issuers on the interpretation and application of the SCP exemption is given in in the Visa *PSD2 SCA Secure Corporate Payment Exemption Guide*.

Detailed guidance for Issuers of Commercial Cards on the application of SCA and the other exemptions defined in the PSD2 SCA RTS to remote electronic transactions performed with Commercial Cards is given in the *PSD2 SCA Commercial Cards Guide*. This guide also summarises guidance that Issuers may wish to give to their commercial card customers to ensure that transactions are not unnecessarily declined due to the inability to apply SCA.

More detailed guidelines for merchants, intermediaries, Acquirers and Issuers on the interpretation and application of the SCP exemption is given in in the Visa *PSD2 SCA Secure Corporate Payment Exemption Guide*.

Detailed guidance for Issuers of Commercial Cards on the application of SCA and the other exemptions defined in the PSD2 SCA RTS to remote electronic transactions performed with Commercial Cards is given in the *PSD2 SCA Commercial Cards Guide*. This guide also

summarises guidance that Issuers may wish to give to their commercial card customers to ensure that transactions are not unnecessarily declined due to the inability to apply SCA.

5.17 Multi-party commerce

Depending on the scenario, customer interactions could have one or more than one merchant.

5.17.1 Multiple merchants

A merchant setting up an agreement may not be the same as the merchant processing subsequent MITs. For example, a customer could:

- Buy a fridge from a white goods supplier, but the installments could be collected by a third party credit provider.
- Purchase both a mobile phone and a care contract for the phone in-store. The care contract is fulfilled by a third party provider.
- Purchase furniture in-store and pay for delivery and installation by a third party contractor

Key Point

The merchant performing the initial CIT and the merchant collecting subsequent MITs can be different, as long as the customer is clearly informed. This means that the Initial Tran ID in an MIT transaction may be related to a CIT transaction that was performed by a different merchant and a different Acquirer.

Therefore, the Visa authorization system allows the CIT and MIT to originate from different merchants (i.e. merchant descriptor, merchant ID and Acquirer ID can be different), and different Acquirers as long as:

- The customer has been clearly informed who he or she is transacting with at the time of CIT and which merchant he or she is authorizing to perform MITs in the future. (e.g. T&Cs and other clear communication inform the customer that the merchant name will differ from the initial transaction to the subsequent transactions);
- There is a way to prove the relationship between the two merchants (e.g. T&Cs presented to the cardholder show who is taking payment today and who is taking payment in the future etc.)

It is important for merchants working together to be aware that whilst it is acceptable for merchants to set up agreements for each other (provided it is clear covered in T&Cs) it is not acceptable for any merchant to collect funds on behalf of other merchants for their goods and services unless they do so under a Visa recognized payment model such as Payment Facilitator or Marketplace as defined below.

5.17.2 Marketplaces (single merchant)

As per Visa rule ID# 0030069, Visa defines online marketplaces to be environments where a single entity brings together buyers & sellers on a branded platform and collects payments on behalf of the other parties who provide goods or services to the customer under the marketplace brand. The marketplace owns the overall customer relationship, is responsible for the transactions and often sets T&Cs for the sale. Examples could include:

- An online marketplace for goods where the payment is always taken by the marketplace operator.
- A take-away food delivery company, where the payment is always taken by the delivery company, and not the establishment providing the food.

A Marketplace must:

- Ensure that its name or brand is:
  - Displayed prominently on the website or mobile application
  - Displayed more prominently than the name and brands of retailers using the Marketplace
  - Part of the mobile application name or URL
- Handle payments for sales and refunds on behalf of the retailers that sell goods and services through the Marketplace, and receive settlement for transactions on their behalf
- Be financially liable for disputes and resolve disputes between cardholders and retailers

In these cases, the merchant will be the same across all aspects of service delivery (i.e. the Marketplace brand), even if different parties are involved in aspects of the fulfilment.

From an SCA perspective, it is the Marketplace brand that will be responsible for authentication and authorization. The name of the merchant providing the goods or services is not seen anywhere in the Visa system, neither in the authentication nor authorization.

IMPORTANT: An entity that brings customers and merchants together but does not handle payments on behalf of the merchant is not considered a Marketplace under Visa Rules but a referral service. For more information see Section 5.17.4.

5.17.3 Payment Facilitators

Payment Facilitators are parties that authorize and settle on behalf of a merchant, but it is the merchant that provides the goods and services and has the relationship with the cardholder.

From an SCA perspective, it is the merchant that drives requests for authentication and authorization, however many merchants using Payment Facilitators may not have the capability or desire to do this in-house, and so it is anticipated they will use services provided by their Payment Facilitator or another technology/gateway provider.

For more details on requirements for transactions with Payment Facilitators, please refer to Visa rule ID #: 0030076.

5.17.4 Referral services

A referral service is a website that brings customers and merchants together, but unlike a Marketplace, the referral service does not handle payments on the merchant's (i.e. seller's) behalf. The payment between the buyer & seller occurs through a separate, unrelated channel from that of the original website.

For example:

- A website that dog owners use to find local dog walkers and compare location and prices

- A website that brings together people needing care in the community with different care agencies
- A classifieds website for individuals to list personal items or services for sale
- A website that brings together many artists selling their own products directly

From an SCA perspective, it is the merchant (i.e. the actual seller of goods/services) that drives requests for authentication and authorization, not the referral service. The referral service is not involved in any way in the payment and authentication process. The end merchant could implement their processes themselves or use a Payment Facilitator.

If the referral service wished to expand their service offering, they could consider offering authentication and authorization services to their merchants, but this would require them successfully undertaking all the processes required to register with Visa as a third party agent. When registered as a Merchant Servicer with Visa, they could perform a single authentication that can be used for each merchant (via each merchant's Acquirer) processing a separate authorization related to a single customer order. This should follow the same methodology used by Travel Agencies and described in *Implementing Strong Customer Authentication for Travel and Hospitality*. After the single customer authentication has taken place, the referral service can use 3RI[174] to obtain a CAVV for each merchant in need of processing its own authorization.

Alternatively, a Referral Service wishing to provide authentication and authorization services to multiple merchants could enhance their offering to become a qualified & registered Marketplace and aggregate all the payments for their suppliers/retailers, thus enabling them to perform a single authentication for a basket containing goods from multiple merchants.

5.18 Industry Specific Best Practice

Industry Specific Best Practice MITs are primarily relevant to the Travel and Hospitality sector. This sector handles many types of payment including:

- No Show at a hotel or car rental agency
- Delayed Charges at a hotel or card rental agency
- Other additional changes such as for an additional night stay, mini bar charges in hotel
- Balance payment(s) on purchase or service on which a deposit has been paid

Further details on how these industry specific scenarios should be processed are provided in an addendum to this guide titled *"Implementing Strong Customer Authentication for Travel and Hospitality"*. For information on processing balance payments for use cases other than Travel and Hospitality please refer to section 5.14.1.

[174] Until 18 October 2024, if 3RI is not available, merchant servicers can provide the initial CAVV to separate merchants and the CAVV may be used up to a total of 5 times.

5.19 Non-financial scenarios

This section covers some example ecommerce scenarios for non-financial transactions. In some circumstances, SCA should still be performed when considering the non-financial transaction in the context of any financial transactions that might follow.

5.19.1 Adding a card to a merchant account/customer profile

This describes the use case when a customer requests addition of a card to a merchant account for future customer-initiated purchases only, but no financial transaction is performed at time of addition. For example, the customer is setting up payment details for a new account.

Before storing and when using a stored credential, a merchant must comply with the relevant disclosure, consent, cancellation procedure and processing rules summarised in Appendix A.1 and detailed in Visa Rule ID # 0029267.

For this scenario, SCA is required if there is a risk of fraud, as determined by the risk policy Issuer and it is important that Issuers are able to correctly identify non financial add card transactions to avoid unnecessary declines. Please refer to the information on use case 1 in sections 4.7.1 and 4.7.2 for guidance on SCA requirements and correctly indicating this transaction type via EMV 3DS.

Scenario
Customer logs on to merchant and adds a payment credentials to their account
1. Disclose use of stored credential • The merchant must ***disclose*** to the customer how the stored credential will be used. • For more information about the Stored Credential Framework and the requirements a merchant must meet, see Appendix A.1. and Visa Rule ID # 0029267.
2. Obtain cardholder consent • The merchant must ***obtain*** cardholder consent.
3. Authenticate customer, if risk of fraud • SCA is required if there is a risk of fraud. A merchant is recommended to submit a non-payment ***authentication (NPA) for "add card"*** request via EMV 3DS to confirm the customer's identity and disclose to Issuers that this is an add card use case (this does not provide fraud liability protection but may assist in preventing SCA declines).   • Refer to use case 1 in Table 31 in section 4.7.2.6 on how to indicate such authentication request.
4. Perform a zero-value *account verification* • Merchant must perform a zero-value authorization (account verification), using indicators according to the Stored Credential Framework, to inform the Issuer that the credential is being stored (and incidentally verify the validity of the credential).   • Refer to use case 1a in Table 18 in section 4.2.3.1 for key information required in this authorization to inform the Issuer a credential is being stored • Merchants must be aware that if the transaction is declined, the credentials cannot be stored
Customer makes future payment using stored credential
Note: If a new card is added, go back to step 1

5. Future CITs using a previously stored credential must be *authenticated* unless a valid exemption applies.

- They must also be indicated with POS entry mode 10 (stored credentials):
- Refer to use case 1b in Table 18 in section 4.2.3.1 for key information required in this authorization to inform the Issuer the transaction is being performed with a credential that was previously stored.

5.19.2 Adding a card to an account during a purchase

A customer requests the addition of a Credential-on-File for future use with the merchant during a purchase transaction.

Scenario
Customer agrees to add payment credentials to their account as part of a purchase
1. Disclose use of stored credential • Merchant must ***disclose*** to the customer how the stored credential will be used. • For more information about the Stored Credential Framework and the requirements a merchant must meet, see Appendix A.1: Stored Credential Framework and Visa Rule ID # 0029267.
2. Obtain cardholder consent • Merchant must ***obtain*** cardholder consent.
3. Authenticate customer • As this is a financial transaction, ***authentication*** *is required for the amount of the financial transaction* unless an exemption applies. However, adding the card may require SCA if there is a risk of fraud in which case exemptions cannot be used. To minimize the risk of SCA declines, it is recommended that merchants indicate to Issuers via EMV 3DS that a card is being added during this transaction   • Refer to use case 2 in Table 31 section 4.7.2.6 for guidance on how to indicate such an authentication request.
4. Authorize transaction • Merchant submits an authorization for the transaction amount and includes the appropriate identifier to indicate that a card is being stored according to the SCF Refer to scenario 1a in Table 18 in section 4.2.3.1 for key information required in this authorization to inform the Issuer a credential is being stored   • The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1 • Merchants must be aware that if the transaction is declined, the credentials cannot be stored.
Customer makes future payment using stored credential
Note: If a new card is added, go back to step 1 **5. Future CITs using the stored credential must be *authenticated* unless a valid exemption applies.** • They must also be indicated with POS entry mode 10 (stored credentials). • Refer to scenario 1b in Table 18 for key information required in this authorization to inform the Issuer the transaction is being performed with a credential that was previously stored

5.19.3 Adding a card at the same time as setting up an agreement

A customer requests the addition of a Credential-on-File for future use with the merchant at the same time as establishing an agreement for MITs.

This option for merchants has already been covered as part of the new agreement scenario descriptions in Section 5.12.

5.19.4 Card details updated by the Issuer

Merchants storing credentials can receive updated payment credentials from the Issuer (e.g. via Visa Account Updater (VAU) or the Visa Token Service). Examples of events that could cause this include:

- Regular card re-issuance due to expiry date being reached, and
- An Issuer switching their card portfolio from another card scheme to Visa

Whilst authentication is not required, it is Visa's recommended practice that merchants using a cardholder's stored credential who receive updates on account information from Visa inform customers in their T&Cs and/or privacy policy that the card details may be automatically updated by participating Issuers in order to ensure payment continuity and uninterrupted service.

5.19.5 Cardholder switching Issuers under the UK Current Account Switch Service

It is possible for a Cardholder to switch their current account (and any associated Visa payment cards) from one Issuer to another. Proof of consent from the Cardholder must be obtained to perform the switch. In the UK Visa Account Updater supports the current account switching service as follows:

- The bank the customer has switched to will send an update to Visa Account Updater to indicate that the old account has been replaced because of an account switch along with a new account number
- The bank the customer is leaving will send an update to Visa Account Updater to indicate that the old account has been closed because of an account switch

Merchants storing details of payment cards can query Visa Account Updater to ensure they have up-to-date information. A merchant who becomes aware of an account switch by querying Visa Account Updater is not required to perform additional cardholder authentication before updating their records with the new account details. However, it is Visa's recommended practice that merchants who update a cardholder's stored credential based on account information from Visa Account Updater inform customers in their T&Cs and/or privacy policy that the card details may be automatically updated by participating Issuers in order to ensure payment continuity and uninterrupted service.

5.19.6 Card details updated by the Customer

If a cardholder goes into their merchant account and updates their card details, either because they wish to pay via a new card, or because the old card had expired, SCA is required if there is a risk of fraud. As documented in section 4.7, it is the Issuer who has the ultimate decision as to whether there is a risk of fraud or not and may require SCA if not already provided by the merchant.

If only the expiry date is changed and the card number remains the same, authentication is not required.

5.19.7 Change Delivery Address

If a cardholder goes into their merchant account and updates the delivery address for an order, authentication is not required, but Visa recommends that it is performed if the customer changes the delivery address linked to an order that is already being processed as this represents a risk of fraud.

5.20 Provisioning Network Tokens

Merchants that use Visa Token Service (VTS) to provision tokens for eCommerce and Credential-on-File (CoF) transactions should refer to the VTS Implementation Guide for details of how to ensure tokens are provisioned correctly. In the context of establishing agreements for ongoing payments such as subscriptions, please refer to Section 5.12.

5.21 Mass tokenizing existing credential on file

For bulk tokenization, SCA is not required as this is just changing the format of a credential already held on file based on an existing agreement which can continue without having to re-authenticate.

6. Bibliography

The following documents provide additional detailed guidance as described in the text of this guide. Version numbers/dates given are correct at the time of publication of this guide, but please note that any subsequent versions of the documents referenced will take precedence.

Table 42: Bibliography

Document/Resource	Latest Version/Date at time of publication	Description
Implementing Strong Customer Authentication for Travel and Hospitality	Version 2.0 June 2021	An addendum to this implementation guide which provides merchants and Acquirers with examples of performing SCA across common payment use cases common in the travel and hospitality sectors.
PSD2 SCA Regulatory Guide	Version 1.0 December 2020	Summarises the main requirements of the PSD2 SCA regulation as it applies to electronic card payments and Visa's guidance on the practical application of SCA in a PSD2 environment.
Visa Core Rules and Visa Product and Service Rules (referred to as the "Visa Rules")	April 2022	The Visa Core Rules and Visa Product and Service Rules, which govern the participation of our financial institution clients in the Visa system and are updated every 6 months (April and October).
PSD2 SCA Optimisation Best Practice guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising the number of transactions that will require Issuers to apply SCA challenges. Please note that until the next version of the Optimisation Guide is published in case of any divergence in information between this guide and the Optimisation guide, this guide takes precedence.
PSD2 SCA Challenge Design Best Practice Guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising friction when SCA challenges are required.
PSD2 SCA Commercial Cards Guide	Version 1.1 March 2021	Summarises considerations for meeting the requirements of SCA for Issuers of commercial card products

PSD2 SCA Secure Corporate Payments Exemption Implementation Guide	Version 1.2 June 2021	Provides additional guidance on the use and support of the Secure Corporate Payments exemption.
European EMV 3DS 2.2 Implementation Guide	Version 1.0 30 October 2019	Provides a summary of the features, benefits and implementation considerations for EMV 3DS 2.2
Remote Electronic Commerce Transactions – European Economic Area and United Kingdom: Visa Supplemental Requirements	Version 3.0 August 2022	Guide summarizing Visa Rules relevant to the application of SCA.
Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.3, 23 April 2021	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of EMV 3DS.
Visa Secure Issuer Implementation Guide for EMV 3-D Secure	Version 1.3, 23 April 2021	The Visa Secure Issuer Implementation Guide for EMV 3-D Secure contains operational guidance for Issuers on the Visa implementation of EMV 3DS.
Visa Secure Cardholder Authentication Verification Value (CAVV) Guide	Version 3.3.2 October 2021	Provides detailed information on CAVV creation and verification and use in authorization for both 3DS 1.0 and EMV 3DS.
PSD2 Exemptions - EMV 3DS Supplementary Guide	Version 1.0 March 2020	Provides guidance on the technical implementation of the ACC extension and the SCP exemption This document is available on Visa Online.
Visa Secure Using EMV 3DS Best Practices for Merchants	Version 1.0 - 06 October 2021	Provides Merchants with the necessary tools and knowledge to successfully use EMV 3DS.
Minimum Data Requirements for Merchants	N/A	An infographic describing the critical data fields for Merchants and their importance in the authentication process.

Visa Network Merchant Initiated Transactions Service – Implementation Guide	Version 1.5 Effective: 01 April 2022	The Visa Network MIT Service is a network solution that Visa Acquirers can offer to their merchant clients to manage the Transaction Identifier lifecycle of MITs. This document outlines the process for key stakeholders to participate in the Network MIT service.
VisaNet Business Enhancements Global Technical Letter and Implementation Guide.	Versions effective: -6 September 2018 -5 September 2019 12 March 2020 -18 June 2020 8 September 2022	Provides VisaNet Acquirers, Issuers, and processors with updates to the technical changes for each business enhancement to VisaNet processing systems and detailed information on implementation, activation, and testing activities.
Visa Merchant Purchase Inquiry (VMPI) information on the Visa Developer Center	N/A	Additional information on the service and the API https://developer.visa.com/capabilities/vmpi
Visa Technology Partner Portal	N/A	Portal with additional resources including details on EMV 3DS available at: https://technologypartner.visa.com/Library/3DSecure2.aspx
EMVCo 3-D Secure Specification	V2.2	Specification for the core 3DS technology that includes message flows, field values etc. available at: https://www.emvco.com/emv-technologies/3d-secure/
VisaNet Authorization-Only Online Messages – Technical Specifications	15 October 2022	Technical Specifications for VisaNet Authorizations
BASE I Processing Specifications V.I.P. System	Effective: 10 June 2022	V.I.P. System BASE I Processing Specifications describes processing requirements and options for the BASE I System within the VisaNet Integrated Payment (V.I.P.) System.
Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance	5 September 2019	VBN stating Visa requirements for the implementation of EMV 3DS.
Visa Business News: Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions	20 August 2020	VBN outlining travel and hospitality merchants' options for avoiding declines for online booking transactions performed via third parties

Glossary

Table 43: Glossary of terms

Term	Description
1-9	
3-D Secure (3DS) 2.0	The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing Issuers with the ability to authenticate customers during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance. Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns EMV 3DS. Visa's offering of 3DS is called Visa Secure.
3-D Secure Server (3DS Server)	A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa's EMV 3DS Program authentication processing.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa's EMV 3DS Program and other functions. The ACS is operated by the Issuer or the Issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the customer, and provides digitally signed authentication response messages (containing the authentication results and other Visa's EMV 3DS Program data) to the merchant.
Account Binding	The process of verifying that the merchant or wallet customer is also the Issuer's cardholder by performing Issuer authentication when binding is established. This can occur during token provisioning or as a standalone action. Account

Term	Description
	binding links a token to the Token Requestor's customer and enables a customer's authentication into their merchant or wallet account to be used in the performance of SCA under the Delegated Authentication Program.
Account Funding Transaction (AFT)	A Transaction that transfers funds from an account linked to a Visa cardholder to another account.
Authentication	Authentication allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be EMV 3DS
Authorization	Authorization determines if a specific transaction request receives an approval or a decline from the issuing bank, or from VisaNet standing in on the issuing bank's behalf. Once a cardholder initiates a purchase, VisaNet informs the Issuer of the transaction, and receives back their approval or decline response. VisaNet then informs the requestor of the response, who passes the information along to the Merchant.
B	
Bank Identification Number (BIN)	A 6-digit number assigned by Visa and used to identify a member or VisaNet Processor for Authorization, Clearing, or Settlement processing
BASE I	A component of the V.I.P. System that provides Authorization related services for Transactions that are subsequently cleared and settled through BASE II.
BASE II	A VisaNet system that provides deferred Clearing and Settlement services to Members.

Term	Description
C	
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted in response to an Authentication Request.
Cloud Token Framework	The Cloud Token Framework is an enhancement to the Visa Token Service for e-commerce and card on file tokens bringing the benefits of device based tokens and cardholder verification to all tokens used for e-commerce
Commercial Card	A Visa Card or a Virtual Account issued to a Client Organization for business-related purchases, as specified in the Visa Rules, and associated with a BIN, account range, or an account designated as one of the following: • Visa Corporate Card • Visa Business Card • Visa Purchasing Card
Customer Initiated Transaction (CIT)	Is any transaction that is not an MIT as defined in section 3.8.1.3, and includes any transaction where the cardholder is available to initiate or authenticate the transaction. Authentication is required for all CITs, unless the transaction qualifies for an exemption or is otherwise out of scope of PSD2
D	
Delegated Authentication	The Visa Delegated Authentication Programme (VDAP) provides the framework and conditions for Issuers to trust qualifying transactions based on specific authentication approaches' or similar
Device Binding	The process of verifying that the Issuer's cardholder has possession of the device on which the token is being used or provisioned to by performing Issuer authentication when the binding is established. Device binding also includes account binding by default. Device binding can occur during token provisioning or as a standalone action. Device binding links a token to a specific Token Requestor's device id and enables the linked device to satisfy the possession

Term	Description
	factor for SCA where the Token Requestor can reliably and unambiguously identify the device.
DAF	Digital Authentication Framework The Digital Authentication Framework (DAF) is part of a global Visa initiative to expand the capabilities and requirements that enable merchants to deliver frictionless shopping experiences while ensuring effective fraud management. The DAF will apply to PAN and Visa Payment Token eCommerce Transactions. Merchants that meet the DAF criteria on qualified authenticated purchase transactions will receive fraud dispute protection on those transaction (that is ECI 05).
Directory Server (DS)	An EMVCo 3DS server component operated in the Interoperability Domain; it performs a number of functions that include authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Dispute	A Transaction that an Issuer returns to an Acquirer.
Dynamic Linking	The process of associating the transaction to a payment amount and payee at the time of transaction processing
E	
Electronic Commerce Indicator (ECI)	A value used in an electronic commerce transaction to indicate the transaction's level of authentication and security.
Exemption	The PSD2 SCA RTS provides a number of exemptions to SCA, which could result in minimizing friction and attrition in the customer payment journey. These are: • Low value exemption • Recurring payment exemption • Trusted beneficiaries exemption • Secure corporate payments exemption • Transaction Risk Analysis (TRA)

Term	Description
Exemption Threshold Value (ETV)	The maximum transaction value for which the TRA exemption may be applied, subject to the PSP's fraud rate being within the Reference Fraud Rate for that transaction value band. The ETV may also be thought of as the upper limit for each transaction value band shown in Table 2.
L	
Liability	Any and all damages (including lost profits or savings, indirect, consequential, special, exemplary, punitive, or incidental), penalties, fines, expenses and costs (including reasonable fees and expenses of legal and other advisers, court costs and other dispute resolution costs), or other losses.
M	
Merchant Initiated Transaction (MIT)	A transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. For a full definition please refer to section 3.8.1.3
O	
Original Credit Transaction (OCT)	A Transaction initiated by a Member either directly, or on behalf of its Merchants, that results in a credit to a Visa Account Number for a purpose other than refunding a Visa purchase.
Out-Of-Band (OOB) Authentication	A Challenge activity that is completed outside of, but in parallel to, the EMV 3DS flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed.
P	

Term	Description
Primary Account Number (PAN)	The Primary Account Number (PAN) is the number embossed and/or encoded on payment cards and tokens that identifies the card Issuer and the funding account and is used for transaction routing. PAN normally has 16 digits but may be up to 19 digits.
Payment Facilitator	A vendor or service provider that is not a regulated Acquirer but is providing services on behalf of a merchant enabling that merchant to authenticate and/or accept electronic payments.
PSD2	The Second European Payment Services Directive, whose requirements include that Strong Customer Authentication is applied to all electronic payments where both Issuer and Acquirer are within the European Economic Area (EEA). This requirement is effective as of 14 September 2019[175].
PSP	In the context of PSD2, Regulated PSPs are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP).
R	
Reference Fraud Rate (RFR)	The benchmark maximum fraud rate, defined by the PSD2 SCA RTS, that a PSP's calculated fraud rate must be equivalent to or below in order for that PSP to qualify to apply the TRA exemption to a transaction of a specified value. The PSD2 SCA RTS defines three reference fraud rates for three transaction value bands, each defined by an ETV. Equivalent GBP denominated transaction value bands have been defined by the FCA for the UK.
Regulatory Technical Standards (RTS)	An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2 by the European

[175] The European Banking Authority (EBA) has recognized the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement Strong Customer Authentication (SCA). Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.

.

Term	Description
	Banking Authority (EBA) and is then adopted by the Commission by means of a delegated act. The PSD2 SCA RTS, (formally titled *Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication*) establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.
S	
SCA decline code	A decline code (Response code 1A) used by an Issuer to request that a transaction sent to Authorization without SCA needs to be resubmitted with SCA. This process is also sometimes referred to as a "soft decline".
Soft decline	The process by which an Issuer requests that a Merchant resubmits for authentication a transaction that has been sent directly to authorization without SCA or with an incorrect out of scope or exemption indicator. This is done using the SCA decline code.
Stand in Processing (STIP)	The component that provides Authorization services on behalf of an Issuer when the Positive Cardholder Authorization System is used or when the Issuer, its VisaNet Processor, or a Visa Scheme Processor is unavailable.
Stored Credential	Information (including, but not limited to, an Account Number or payment Token) that is stored by a merchant or its agent, a Payment Facilitator, or a Staged Digital Wallet Operator to process future Transactions.
Strong Customer Authentication (SCA)	SCA, as defined by PSD2 SCA RTS, requires (among other things) that the payer is authenticated by a PSP through independent factors from at least two of the categories of knowledge, possession and inherence.

Term	Description
T	
Token Requestor	A Token Requestor (TR) is an entity that requests payment tokens for end-users. Some examples of TRs include digital wallet providers, payment enablers and merchants.
Token Service Providers	Token Service Providers (TSPs) are approved partners - connected to VTS and other networks - who help token requestors enable tokenized payments. There are two TSP types: (i) an Issuer TSP (I-TSP) provides solutions for financial institutions in participating token requestors payment services; (ii) a Token Requestor TSP (TR-TSP) allows token requestors to develop consumer digital payment solutions powered by VTS.
Tokenization	Tokenization is the process of replacing the traditional payment card account number with a unique digital token in online and mobile transactions
Transaction Identifier or Tran ID	The unique identifier assigned to a transaction. This is used to link an out of scope MIT transaction to an original authenticated CIT used to set up the MIT agreement
Transaction Risk Analysis (TRA) Exemption	Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for remote transactions provided risk analysis is applied and the PSP's fraud rates, and transaction amounts are under certain thresholds (Article 18 of the PSD2 SCA RTS). The formula to calculate the PSP's fraud rate for the application of the TRA exemption is total value of unauthorized and fraudulent remote card transactions divided by the total value of all remote card transactions.
Trusted Beneficiaries Exemption	An exemption defined in the PSD2 RTS that allows, subject to certain restrictions, that a payer may add a trusted merchant to a list of trusted beneficiaries (Trusted List) held by their Issuer, completing an SCA challenge in the process. Sometimes referred to as "whitelisting".

Term	Description
Trusted List	A list of trusted merchants, or trusted beneficiaries, held by an Issuer on behalf of a customer. Sometimes referred to as a "whitelist"
V	
Visa Attempts Service / Visa Attempts Server	A Visa service that responds to authentication request messages on behalf of the Issuer when either the Issuer does not participate in Visa's 3-D Secure 2.0 Program, or the Issuer participates but their ACS is unavailable. The Visa Attempts Server provides proof, in the form of a CAVV, in the authentication response that the merchant attempted to obtain authentication.
Visa Directory Server (DS)	A server hardware/software entity that is operated by Visa, whose primary function is to route authentication requests from merchants to specific ACSs and to return the results of authentication.
Visa Secure	Visa's consumer brand name for EMV 3DS
Visa Token Service (VTS)	The Visa Token Service is a security technology from Visa which replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token. The Visa Token Service provides a complete integrated set of tokenization tools for merchants, Issuers, Acquirers and processors.
V.I.P.	The processing component of the VisaNet Integrated Payment System comprised of BASE I and the Single Message System used for single message Authorization in connection with financial Transaction processing.
VMID	Visa Merchant Identifier (VMID). A VMID is a unique 8-digit assigned by Visa to identify each merchant brand business entity, i.e., merchant DBA or Doing-Business-As, for use with some Visa programs.

A Appendices

A.1 Appendix 1 The Stored Credential Framework

A stored credential is information (including, but not limited to, an account number or payment token) that is stored by a merchant or its agent, a payment facilitator, or a staged digital wallet operator to process future transactions.

In order to use stored credentials, merchants and their third party agents, payment facilitators, or staged digital wallet operators that offer cardholders the opportunity to store their credentials on file must:

- Disclose the terms and conditions of usage of the stored credential
- Obtain cardholder consent for initial storage of credentials
- In Europe, SCA is required if, based on the Issuer's assessment, there is risk of fraud
- Inform the Issuer of consent and identify initial storage and usage of stored payment credentials via a transaction with the appropriate data values
    - This means that as part of establishing consent to store payment credentials, an initial CIT must be performed indicating that the credentials are being stored. Future transactions using that credential can then be indicated accordingly.

Details of what must be disclosed to the cardholder and other processing requirements and cancellation policies for the usage of stored credentials are documented in Visa Rule ID # 0029267.

Table 44: Key data fields for performing CIT transactions with stored credentials

Transaction Type	Description	POS Entry Mode (F22)	POS environment (F126.13)
CIT	Customer Initiated (CIT) – putting credential on file for first time (e.g. for future use; may be done during a transaction or at account set up via an account verification transaction)	01	C
CIT	Subsequent CIT performed with the Stored Credentials (e.g. shopping online at a merchant or using an app to order a ride)	10	--

Stored payment credentials can be used for CIT or MIT transactions. Details of the data values required for using stored credentials for MIT transactions are included in section 3.8.

A.2 Appendix 2 STIP SCA Flowchart

Figure 22: STIP SCA flowchart effective through 13 April 2023

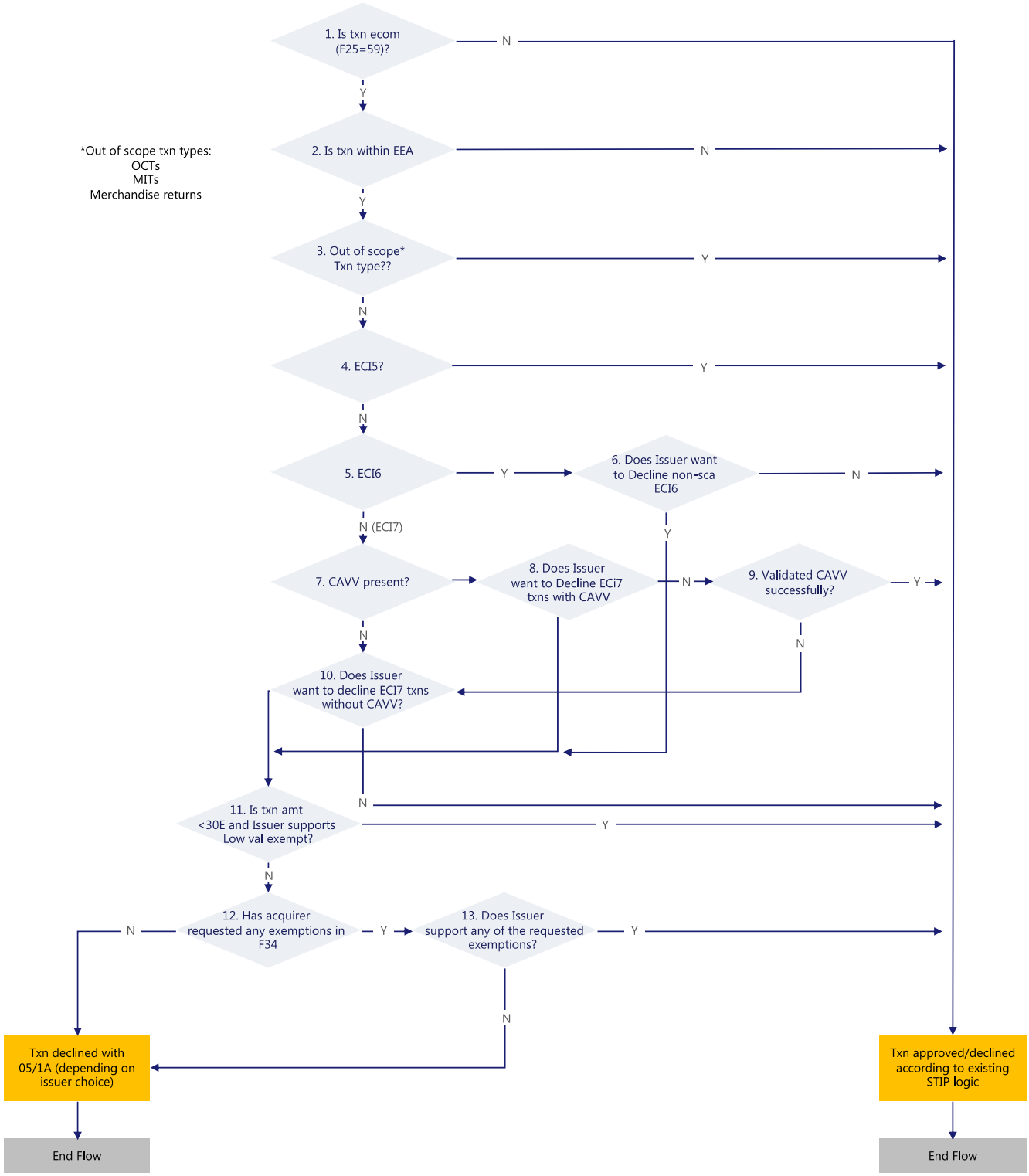
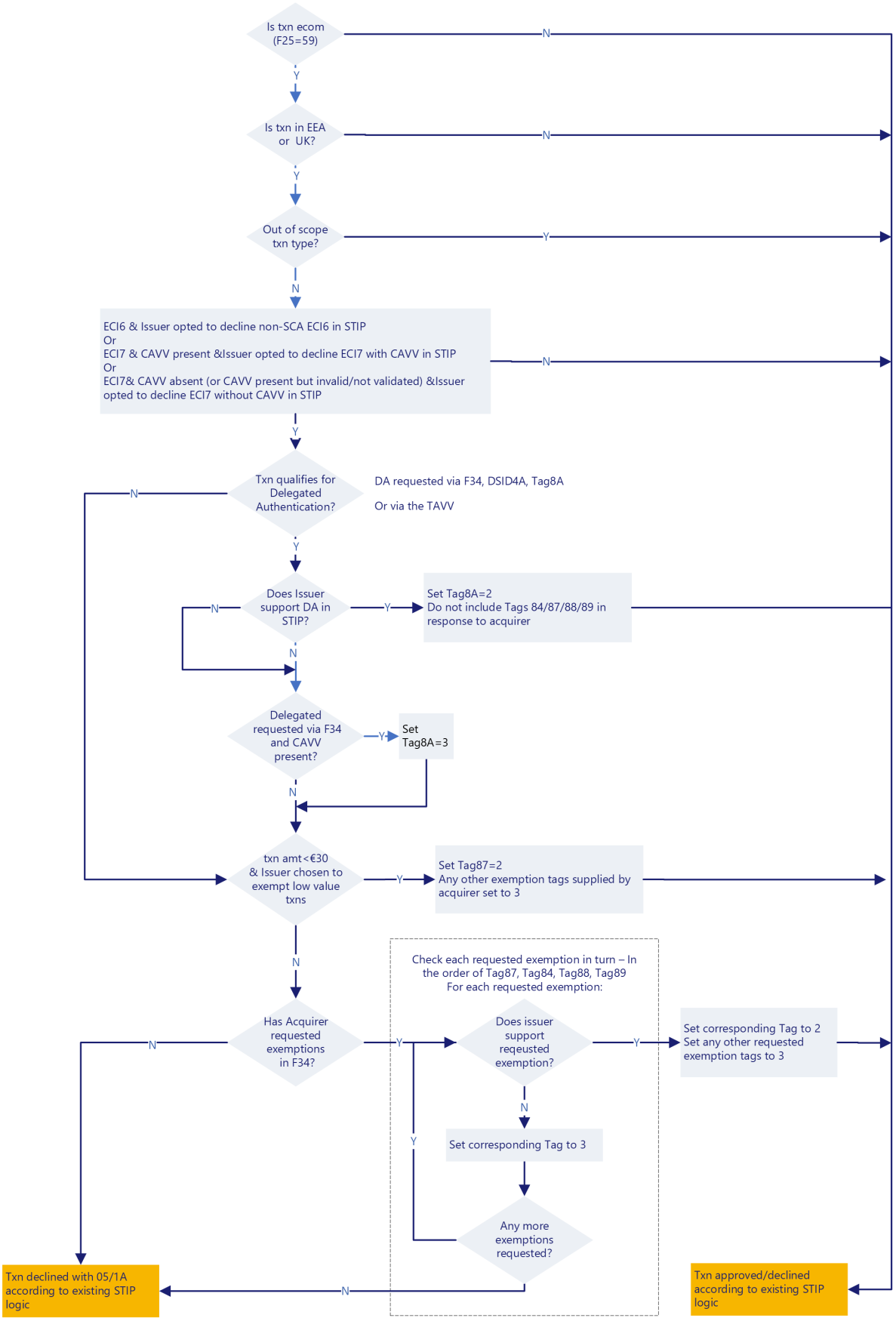


Figure 23: STIP SCA flowchart effective from 14 April 2023



A.3 Appendix 3 Merchant Initiated Transactions

Merchants commonly perform MITs without the active participation of the cardholder to:

- Perform a transaction as a follow-up to a cardholder-initiated transaction (CIT)
- Perform a pre-agreed instruction from the cardholder for the provision of goods or services

Examples of MITs include:

- A hotel charge for mini-bar expenses tallied after the guest has checked-out and closed the folio
- A subsequent recurring payment for a magazine subscription

The definition of an MIT and of transactions that do and do not qualify as MITs is given in section 3.8.1.3 and the Visa MIT Framework is summarized in section 0. This appendix provides more detail on the types of MIT and the values used to identify them in authorization messages.

The MIT framework covers two types of MITs:

- Industry-Specific Business Practice MITs
- Standing-Instruction MITs

Each transaction type included in the categories is outlined below.

A.3.1 Industry Specific Business Practice MITs

MITs defined under this category are performed to fulfil a business practice as a follow-up to an original cardholder-merchant interaction that could not be completed with one single transaction. The following transaction types are industry-specific transactions.

- Incremental Authorization Transaction
- Resubmission Transaction
- Delayed Charges Transaction
- Reauthorization Transaction
- No Show Transaction

A.3.2 Incremental Authorization Transaction - Reason Code 3900 in Field 63.3—Message Reason Code

Description	Incremental authorizations can be used to increase the total amount authorized if the authorized amount is insufficient. An incremental authorization request may also be based on a revised estimate of what the cardholder may spend. Incremental authorizations do not replace the original authorization— they are additional to previously authorized amounts. The sum of all linked estimated and incremental authorizations represents the total amount authorized for a given transaction. An incremental authorization must be preceded by an estimated/initial authorization. One or more incremental authorizations can be requested while the transaction has not yet been finalized (submitted for clearing). Incremental authorizations must not be used once the original transaction has been submitted for clearing. Instead, a new authorization must be requested, with the appropriate reason code (e.g., delayed charges, Reauthorization).
Maximum Timeframe between Original Transaction and MIT	Incremental authorizations can be performed during the approval response validity period of the original estimated/initial authorization. For more details, please refer to Visa Rules (ID#: 0029524).
Relevant Merchant Segments	In the EEA and the UK, incremental transactions can be used by e-commerce merchants from any MCC to authorize any additional amount above the initial or estimated authorization request, if the price of merchandise or services, including shipping costs and applicable taxes, has changed. Note that outside of the EEA and the UK, incremental transactions are limited to certain merchant categories. Examples include car rental, lodging, transit, amusement parks, restaurants, and bars. For complete list of all eligible MCCs, refer to the Visa Rules (ID#: 0025596).
Examples	A lodging merchant performs an incremental authorization while adding room service expenses to cardholder's folio, revising previous estimate of cardholder's total charges

A.3.3 Resubmission Transaction—Reason Code 3901 in Field 63.3—Message Reason Code

Description	A merchant performs a Resubmission in cases where it requested an authorization but received a decline due to insufficient funds after it has already delivered the goods or services to the cardholder. Merchants in such scenarios can resubmit the request to recover outstanding debt from cardholders.
Maximum Timeframe between Original Transaction and MIT	Resubmission must be submitted within 14 days from the original transaction. This timeframe limit only applies to token-based resubmissions.

Relevant Merchant Segments	This type of transaction is most prevalent in transit merchant segments, such as commuter transportation including bus lines and passenger railways.
Examples	A transit merchant performs a Resubmission transaction for debt collection after a decline is received due to insufficient funds and the cardholder has already availed the services.

A.3.4 Delayed Charges Transaction—Reason Code 3902 in Field 63.3—Message Reason Code

Description	Delayed charge transaction is performed to process a supplemental account charge after original services have been rendered and respective payment has been processed.
Maximum Timeframe between Original Transaction and MIT	Delayed charges must be submitted within 90 days from the date of the rental return, check-out, or disembarkation date, in accordance with the Visa Rules (ID#: 0007398).
Relevant Merchant Segments	Relevant merchant segments are limited to vehicle rental, lodging, cruise lines, and other rentals. For a full list of eligible MCCs for delayed charges, please refer to Visa Rules (ID#: 0007398).
Examples	A lodging merchant performs delayed charge transaction to charge the cardholder for incidental charges such as "mini-bar" charge, after the cardholder has checked out.

A.3.5 Reauthorization Transaction—Message Reason Code 3903 in Field 63.3—Message Reason Code

Description	A merchant initiates a Reauthorization when the completion or fulfilment of the original order or service extends beyond the authorization validity limit set by Visa. There are two common Reauthorization scenarios: • Split or delayed shipments at e-commerce retailers. A split shipment occurs when not all of the goods ordered are available for shipment at the time of purchase. If the fulfilment of the goods takes place after the authorization validity limit set by Visa, e-commerce merchants perform a separate authorization to ensure that consumer funds are available. • Extended stay hotels, car rentals, and cruise lines. A Reauthorization is used for stays, voyages, and/or rentals that extend beyond the authorization validity period set by Visa

Maximum Timeframe between Original Transaction and MIT	The following timeframe limits only apply to token-based Reauthorizations. A Reauthorization can be submitted up to 90 days from original purchase except for specific MCCs, which can submit a Reauthorization up to 120 days from the original date of purchase. For the current list of MCCs that can reauthorize for up to 120 days, contact your Visa Representative.
Relevant Merchant Segments	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in e-commerce retail, lodging, car rental, and cruise lines.
Examples	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in e-commerce retail, lodging, car rental, and cruise lines.

A.3.6 No Show Transaction—Reason Code 3904 in Field 63.3—Message Reason Code

Description	Cardholders can use their Visa cards to make a guaranteed reservation with certain merchant segments. A guaranteed reservation ensures that the reservation will be honored and allows a merchant to perform a no-show transaction to charge the cardholder a penalty according to the merchant's cancellation policy. For merchants that accept token-based payment credentials to guarantee a reservation, it is necessary to perform a CIT (Account Verification Service) at the time of reservation to be able perform a no-show transaction later.
Maximum Timeframe between Original Transaction and MIT	There is no timeframe limit to submit a no-show transaction.
Relevant Merchant Segments	Only certain merchant categories are eligible to guarantee reservations and perform no-show transactions. Qualifying merchant segments include lodging, car rental and other rentals. For complete list of all eligible MCCs that can submit no-show transactions refer to Visa Rules (ID#: 0029266)
Examples	A lodging merchant can perform a no-show transaction to charge a cardholder a penalty for a guaranteed reservation if the cardholder did not cancel the reservation according to the merchant's cancellation policy.

A.3.7 Standing-Instruction MITs

MITs defined under this category are performed to address pre-agreed standing instructions from the cardholder for the provision of goods or services. The following transaction types are standing-instruction transactions.

- Installment and Prepayment (partial & full) Payment Transaction
- Recurring Payment Transaction

- Unscheduled COF Transaction

A.3.8 Installment Payment Transaction and Prepayment (partial & full) Transaction —Value "I" in POS Environment Field 126.13

Description	An installment is a transaction in a series of transactions that use a stored credential and that represent a cardholder agreement for the merchant to initiate one or more future transactions over a period for a single purchase of goods or services. A prepayment is one or many payment(s) towards a future purchase of goods/services.
Maximum Timeframe between Original Transaction and MIT	The timeframe is governed by a contract between the consumer and the merchant for that specific installment or prepayment relationship.
Relevant Merchant Segments	Any merchant category can submit installment payment or partial prepayment transactions. Full prepayments are limited to: • Merchants in the T&E (and related) sectors • Merchants taking an order for custom merchandise or services Or in a face-to-face environment, where not all goods are able to be collected at the time of purchase and will be shipped at a later date
Examples	A furniture retailer allows a cardholder to pay for goods purchased in installments over a pre-agreed period of time. **Prepayment (partial):** A customer confirms booking a hotel booking, and pays for what is due that day but also agrees to additional prepayment(s) as needed prior to check-in **Prepayment (full):** A customer is pre-ordering a music record that is not scheduled to be released until a later date.

A.3.9 Recurring Payment Transaction —Value "R" in POS Environment Field 126.13

Description	A transaction in a series of transactions that use a stored credential and that are processed at fixed, regular intervals (not to exceed one year between transactions), representing cardholder agreement for the merchant to initiate future transactions for the purchase of goods or services provided at regular intervals.
Maximum Timeframe between Original Transaction and MIT	The timeframe is governed by a contract between the consumer and the merchant for that specific recurring relationship.
Relevant Merchant Segments	Any merchant category can submit Recurring Payment transactions.
Examples	A magazine publisher charges cardholder for monthly subscription.

A.3.10 Unscheduled COF Transaction —Value "C" in POS Environment Field 126.13

Description	A transaction using a stored credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date, where the cardholder has provided consent for the merchant to initiate one or more future transactions.
Maximum Timeframe between Original Transaction and MIT	The timeframe is generally undetermined, as payment is prompted by a pre-agreed event between the cardholder and merchant in the contract governing their relationship.
Relevant Merchant Segments	Any merchant category can submit unscheduled COF transactions.
Examples	An example of such transaction is an account auto-top up transaction.

A.4 Appendix 4 EEA Countries in scope of PSD2 SCA

The countries below represent those participating in the European Economic Area and therefore subject to PSD2 SCA regulation.

Table 45 EEA countries understood to be in scope of PSD2 SCA

AUSTRIA AT 040	ITALY IT 380
BELGIUM BE 056	LATVIA LV 428
BULGARIA BG 100	LICHTENSTEIN LI 438
CROATIA HR 191	LITHUANIA LT 440
CYPRUS CY 196	LUXEMBOURG LU 442
CZECH_REP CZ 203	MALTA MT 470
DENMARK DK 208	NETHERLANDS NL 528
ESTONIA EE 233	NORWAY NO 578
FINLAND FI 246	POLAND PL 616
FRANCE FR 250	PORTUGAL PT 620
GERMANY DE 276	ROMANIA RO 642
GREECE GR 300	SLOVAKIA SK 703
HUNGARY HU 348	SLOVENIA SI 705
ICELAND IS 352	SPAIN ES 724
IRELAND IE 372	SWEDEN SE 752

While the UK is no longer in the EEA, equivalent requirements apply in the UK.

Although not part of the European Economic Area (EEA), based on local law, strong customer authentication may apply to transactions in regions that are associated with countries within the EEA. Examples include micro-states and city-states in Europe, along with territories of EEA Countries outside of Europe. Clients in those regions should contact their NCA to determine if SCA applies and if so how to comply and their Visa representative to determine how to optimize their performance of SCA.

European non-EEA countries such as Switzerland or Turkey do not have to apply SCA. However, Issuers/merchants in those countries may still decide to authenticate using EMV 3DS in many instances. Note that any merchants located in those countries but acquired by EEA or UK Acquirers are subject to the regulation for transactions with EEA and UK issued cards.

A.5 Appendix 5 Trusted beneficiaries exemption – use of EMV 3DS and authorization indicators in key process flows

This appendix provides information on how the EMV 3DS and authorization messages and fields described in section 4.5.3.8 are used in the process flows for adding merchants to a Trusted List and applying the exemption and authorizing subsequent qualifying transactions.

A.5.1 Adding to the Trusted List during and outside the purchase flow

A.5.1.1 Adding to the Trusted List – authentication

Table 46 below describes the high-level EMV 3DS authentication flow for the customer adding a merchant to their Trusted List via EMV 3DS 2.2. This flow is applicable to the addition of a merchant which is initiated by an EMV 3DS authentication request in both the purchase flow and outside the purchase flow.

Table 46: 3DS authentication and adding a merchant as a trusted beneficiary

Step	Data	Comments
1. Customer purchases an item on merchant site. *Note: For addition outside of a transaction flow, the customer can be given the option to add to their Trusted List on the merchant site*	Required: • N/A	Merchant should first confirm that the Issuer card supports whitelisting before providing an option for the customer to add a merchant to their Trusted List. See Section 4.5.3.7.
2. Merchant initiates 3DS 2.2 call to the 3DS Server and populates fields for whitelisting in the Authentication Request (AReq) message.	Required (during purchase): • Message Category: 01 • 3DS Requestor Authentication Indicator: 01 Required (outside of a purchase): • Message Category: 02 • 3DS Requestor Authentication Indicator: 04 • Required (for both during purchase and outside of a purchase): • Customer Account Number: <PAN> • 3DS Requestor Challenge Indicator: 09 • whiteListStatus: 'N'	3DS Requestor Challenge Indicator = 09 means Challenge requested (whitelist option requested if challenge required). whiteListStatus = N means 3DS Requestor is not whitelisted by the customer whiteListStatusSource = 01 means the source of the request is from the 3DS Server.

Step	Data	Comments
	• whiteListStatusSource: 01	
3. Visa 3DS Directory Server checks the Issuer's card range supports whitelisting.		
4. Issuer ACS will provide an Authentication Response (ARes) with a challenge request to 3DS Directory Server. The 3DS Directory Server then sends Authentication Response (ARes) to Merchant and the standard 3DS challenge flow will then be initiated.	Required: • Transaction status: C (challenge) • whitelistingInfoText: <Message>	whitelistingInfoText is the Text provided by ACS/Issuer to customer during whitelisting transactions, applicable only for App. If browser, the ACS will display text as part of the HTML.
5. If the customer opts in to trust merchant, authenticates and SCA is successful, then Issuer ACS will respond with a Results Request Message (RReq) to confirm customer is opted in to add the merchant as a Trusted Beneficiary.	Required: • Electronic Commerce Indicator: 05 • Authentication Value: <CAVV> • Transaction status: 'Y' • whitelistStatus: 'Y' • whiteListStatusSource: 03	whitelistStatus = Y indicates that the 3DS Requestor is whitelisted by customer. whiteListStatusSource = 03 indicates the source is the ACS.
6. The combination is stored by the Issuer or the Issuer ACS as an approved trusted beneficiary.	Required: • N/A	
7. The merchant is informed that customer added them as a trusted beneficiary.	Required: • Electronic Commerce Indicator: 05 • Authentication Value: <CAVV> • Transaction status: 'Y'	

Step	Data	Comments
	• whitelistStatus: 'Y' • whiteListStatusSource: 03	

A.5.1.2 Adding a merchant to the Trusted List during a purchase – authorization flow

Once the transaction has been authenticated successfully, the transaction will be sent through to authorization as follows:

Table 47: Subsequent transaction authentication steps

Step	Spec	Comments
1. Acquirer sends Authorization Request.	Required: • Field 126.9: <CAVV> • Field 60.8 (ECI): 05	Value of '1' in Field 34 means the trusted merchant exemption has been claimed/requested. The value "1" in Field 34 (Dataset ID 4A, Tag 84) should not be used in this request as a challenge was obtained for this initial addition to the trusted list so the Trusted Beneficiary exemption was not used
2. Issuer checks the authorization request values, completes authorization decision, and returns the response to VisaNet.	Required: • Field 39: <Authorization response>	Issuer approves or declines the authorization request using Field 39 as part of standard protocol.
3. VisaNet sends the authorization response to the Acquirer / Acquirer Processor.	Required: • Field 39: <Authorization response>	

A.5.2 Subsequent authentication & authorization after a merchant is added to the Trusted List

A.5.2.1 Authentication flow for subsequent transactions

The flow below describes the EMV 3DS authentication processes after a merchant has been successfully added to the Trusted List:

Table 48: Subsequent transaction authentication steps

Step	Data	Comments
1. Merchant initiates 3DS 2.2 call to the 3DS Server and populates fields for whitelisting in the Authentication Request (AReq) message.	Required: • Customer Account Number: <PAN> • 3DS Requestor Challenge Indicator: 08 • whiteListStatus: 'Y' • whiteListStatusSource: 01	whiteListStatus = Y means 3DS Requestor is whitelisted by customer whiteListStatusSource = 01 means the source of the request is from the 3DS Server. 3DS Requestor Challenge Indicator = 08 means No challenge requested (utilize whitelist exemption if no challenge required)
2. Visa 3DS Directory Server checks the Issuer's card range supports whitelisting.		
3. Issuer's ACS will provide an Authentication Response (ARes)	Required: • Transaction Status: 'Y' • Electronic Commerce Indicator: 05 • Authentication Value: <CAVV> • whitelistStatus: 'Y' • whiteListStatusSource: 03	
4. The 3DS Directory Server will pass the ARes to the 3DS Server	Required: • Transaction Status: 'Y' • Electronic Commerce Indicator: 05 • Authentication Value: <CAVV> • whitelistStatus: 'Y' • whiteListStatusSource: 03	

A.5.2.2 Authorization flow for subsequent transactions

After the above authentication process has been completed, the Acquirer should submit the authorization request as follows.

Table 49: Transaction authorization steps

Step	Spec	Comments
1. Acquirer sends Authorization Request.	Required: • Field 126.9: <CAVV> • Field 60.8 (ECI): 05 • Field 34 (Dataset ID 4A, Tag 84): 1	Value of '1' in Field 34 means the trusted merchant exemption has been claimed/requested.
2. Issuer checks the authorization request values, completes authorization decision, and returns the response to VisaNet.	Required: • Field 39: <Authorization response> • Field 34 (Dataset ID 4A, Tag 84): 2 if exemption honored *or 3 if not honored*	Issuer approves or declines the authorization request using Field 39 as part of standard protocol.
3. VisaNet sends the authorization response to the Acquirer / Acquirer Processor.	Required: • Field 39: <Authorization response> • Field 34 (Dataset ID 4A, Tag 84): 2 *or 3 depending on response received. In some cases, this value maybe blank if no response was received.*	

A.5.3 Check status of a Trusted Beneficiary through EMV 3DS 2.2

Once the customer has added the merchant to their Trusted List, the merchant can check its Trusted Beneficiary status using the 3RI Non Payment Authentication (NPA) flow.

Table 50: Trusted beneficiaries status checking steps

Step	Data	Comments
1. Merchant sends AReq to request for a Status Check	Required: • Customer Account Number: <PAN> • Device Channel: 03 (3RI) • 3RI Indicator: 10 • Message Category: 02	3RI Indicator = 10 indicates whitelist status check Device Channel = 03 indicates 3RI (3DS Requestor Initiated)
2. Visa 3DS Directory Server checks the Issuer's card range supports whitelisting.		
3. Issuer ACS will check the status and return an ARes with the results	Required: • whitelistStatus: Y, N, E, P, R or U • whitelistStatusSource: 03	See EMV 3DS 2.2 specifications for full details of the whiteListStatus field responses. whiteListStatusSource = 03 means the source of the request is from the Issuer ACS.

A.5.4 Error and exception handling – Authentication

An authentication may not be successful for a number of reasons. In this case, the whitelistStatus may respond with the following status codes. Please refer to the *EMV 3-D Secure Protocol and Core Functions Specifications Version 2.2.0* for more information.

Table 51: Unsuccessful whitelisting request response codes as determined by Issuer ACS

Status	Actions
E = Not eligible as determined by Issuer	The Issuer will register account ranges in the Directory Server. However, the Issuer can decide at the individual PAN level that the customer is not eligible for this service. The customer would not be prompted to add the merchant as a Trusted Beneficiary.
R = Customer rejected	The customer was given the option to add the merchant as a Trusted Beneficiary. However, the customer decided not to add the merchant to their Trusted List.
U = Whitelist status unknown, unavailable, or does not apply	Whitelist status is unavailable.

Table 52: Authentication error handling responses as determined by Visa Directory Server

Error	Actions
ACS does not support whitelisting (i.e., Issuer BIN is not registered for this service in Visa Directory Server)	Visa 3DS Directory Server will update the below fields: • Transaction Status: 'N' • Response Code: 88 Requested programme not supported by the ACS
Issuer ACS only supports 3DS 2.1	Visa 3DS Directory Server will respond with the below: • Transaction Status: "N" • Reason Code: 86 Protocol version not supported by ACS
Issuer ACS does not support 3DS 2.2 or 3DS 2.1 and Issuer is not enrolled in Visa Attempts Service	Visa 3DS Directory Server will respond with the below: • Transaction Status: "N" • DS specific reason code 80, 81, 82, 83, or 86 depending on the specific scenario.
Issuer ACS does not support 3DS 2.2 or 3DS 2.1. Issuer is enrolled in Visa Attempts Service, but transaction is excluded from Attempts processing	Visa 3DS Directory Server will respond with the below: • Transaction Status: "N" • DS specific reason code 87 in the ARes to indicate that the transaction was excluded from Attempts processing based on card type or programme rules.

A.6 Appendix 6 Intelligent Data Exchange (IDX)

Issuers can subscribe to a new Visa service called Intelligence Data Exchange (IDX) where supplemental data is made available in various Tags of Field 34 as follows. IDX's supplemental data is expected to improve fraud rates and lower suspected fraud decline, which benefits both Issuers and merchants.

Data Group ID	Data Group Description	Field and Tag	Field Description
001Appendix	3–D Secure Protocol Version Number	F34 DS01 Tag 86	3–D Secure Protocol Version Number
002	3DS Data	F34 DS01 Tag 89	3DS Browser IP Address
		F34 DS01 Tag 92	3DS APP IP Address
		F34 DS01 Tag 93	Shipping Indicator
		F34 DS06 Tag 86	D021 - Device ID (Platform)
		F34 DS06 Tag 87	D022 - Device Type (Platform)
		F34 DS07 Tag 8D	C014 – SDK App ID (Common)
		F34 DS56 Tag 9F28	CAVV Version Number
		F34 DS56 Tag 9F29	CAVV Type
005	Data Part 2	F34 DS56 Tag 9F20	IP Address Velocity Count
005		F34 DS56 Tag 9F21	Device ID Velocity Count
006	Authentication Score	F34 DS56 Tag 9F22	Visa Risk-Based Authentication Score