PSD2 SCA for Remote Electronic Transactions

Implementation Guide

February 2019

Version 1.1
11th March 2019

VISA

Contents

VISA

Important Information

Note on references to 3-D Secure 2.0 (3DS 2.0): When in this document we refer to 3-D Secure 2.0 or 3DS 2.0 this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification.

Some 3-D Secure features are only available under versions 2.1, 2.2 or later of the EMVCo specification. Readers will need to refer to the EMVCo specifications or more detailed guidance being published by Visa for information on which version support.

VISA

Using this document

This guide forms part of a set of Visa guidance documents that are relevant to the implementation of Strong Customer Authentication under PSD2. The guide is written for business, technology and payments managers responsible for the planning and implementation of PSD2 compliance 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 plan for the implementation of SCA.   It is supported by more detailed implementation guides and other documents that are listed in the bibliography in section 7.

This guide covers remote electronic payments (e-commerce and m-commerce).

The guide is structured as follows:

Section	Title	Description
1	Introduction & Document Purpose	An overview of Visa's guiding principles for PSD2 and corresponding focus for SCA compliance
2	PSD2 SCA Requirements	Summarising Visa's interpretation of the PSD2 SCA requirements, including the application of SCA and the exemptions allowed
3	Visa's PSD2 SCA Solutions	Providing the essential information needed to interpret Sections 4 and 5 of this document It details the range of tools and services Visa is making available to merchants, Issuers and Acquirers to optimise the application of SCA and allowable exemptions, including 3DS 2.0, authentication and authorization message fields & values and Visa rules
4	Optimising the payment experience under PSD2 SCA	Providing information and guidance to help clients set their policies for application of SCA and exemptions. It describes the: • 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

VISA

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	Planning for PSD2 – what you need to do	Providing checklists for merchants, Acquirers and Issuers, highlighting the actions they need to take to ensure they are ready for PSD2 SCA, in September 2019
7	Bibliography	A list of key additional reference documents
8	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. 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 local competent authorities**

- **Visa core rules**

- **Technical information and guidance published in EMVCo specs and Visa Implementation guides listed in the bibliography**

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

VISA

Audience

This guide is intended for anyone involved in the processing of eCommerce transactions in the Visa Europe region. 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 recognise transactions that are in and out of scope of SCA so they can maintain security without their cardholder's 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.

Feedback

We welcome feedback from readers on ways in which future editions of the guide could be improved. Please send any comments or requests for clarifications to PSD2questions@visa.com

VISA

Section 1

Introduction: Visa's guiding
principles for PSD2

1. Introduction: Visa's guiding principles for PSD2

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) 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 programmes and initiatives including 3-D Secure (3DS) and the Visa Token Service (VTS) support PSPs to be PSD2 compliant. 3DS, along with our new 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 consumers through increasing their trust and confidence and delivering a frictionless 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 compliance 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

Section 2

The requirements of PSD2 Strong Customer Authentication (SCA) and Visa's interpretation

VISA

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, remote and m-payments - within the European Economic Area (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 specific rules on SCA come into force on 14th September 2019.

For a more detailed definition and discussion of these and other requirements, please refer to the Visa paper "Preparing for PSD2 SCA" November 2018. Clients should also refer to guidance produced by national competent authorities when considering their compliance policies.

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 summarised in Table 1.

Table 1: Strong Customer Authentication Factors

Category	Description	Example
Knowledge	Something only the payer knows	A password
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, finger print, voice recognition, behavioural biometric)

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

For more information on the application of factors please refer to section 2.2 of the Visa paper "Preparing for PSD2 SCA" November 2018.

2.2   Exemptions

The main exemptions to the application of SCA relevant to Visa e-commerce transactions are summarised below. It should be noted that not all exemptions are available to all PSPs. For more detail please refer to section 4.

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, 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 card payments, set out in table 2.

Table 2: Specific Fraud Thresholds for Card Payments

Transaction value band	PSP Fraud Rate
<€100	13 bps / 0.13%
€100 - €250	6 bps / 0.06%
€250 - €500	1 bps / 0.01%

2.2.2   Low value transactions

Remote transactions up to €30 do not require SCA up to a maximum of 5 consecutive transactions or a cumulative limit of €100.

2.2.3   Trusted beneficiaries

Where Visa cardholders shop regularly at merchants they trust, they may add them to a list of "trusted beneficiaries" held by their Issuer. Subsequent payments to such merchants do not require SCA.

2.2.4   Secure corporate payments

Payments made through dedicated corporate processes and protocols (e.g. lodge cards, central travel accounts and virtual cards) which are initiated by business entities, not available to consumers and which already offer high levels of protection from fraud may be exempted from SCA.

Lodge Cards, Central Travel Accounts and Virtual Cards that are not associated with an individual cardholder and are used within a secure dedicated corporate payment process are examples that may fall into this category.

VISA

2.3 Out of scope transactions

The following transaction types are out of scope of SCA:

- **Merchant Initiated Transactions (MITs) -** A transaction, or series of transactions, of a fixed or variable amount and fixed or variable intervals 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. Visa's position is that these are out of scope. Where the initial mandate is set up through a remote electronic channel, SCA is required in most cases but is not necessary for subsequent payments initiated by the merchant. This applies to all payment instruments including cards and tokens.
- **Mail Order/Telephone Order (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[1]. However, SCA should still be applied on a "best efforts" basis.
- **Anonymous transactions -** Transactions through anonymous payment instruments are not subject to the SCA mandate, for example anonymous prepaid cards.

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.   An authentication code must be produced but does not need to be visible to the cardholder.

Visa's programmes such as 3DS, and Visa Token Service (VTS), deliver an authentication code - Cardholder Authentication Verification Value (CAVV) and/or Token Authentication Verification Value (TAVV) - which can be linked directly to the transaction. The authentication code accepted by the PSP that is processing the transaction must correspond to the amount and payee. Visa systems enable the authentication code to be linked back to the amount and payee.

2.5 Use of SMS one time passwords (OTP) and card data as SCA factors

Where SMS OTP is used as a strong authentication method for card payments, the following criteria should apply:

1. Sufficient measures must be taken by the Issuer to mitigate the risk of security being compromised, through exploitation of known vulnerabilities in the channel for example through SIM swaps or man in the middle attacks.

1. Where SMS OTP is used alongside card data, a "layered", risk-based authentication approach should be deployed.

---

[1] Refer to Appendix A.7 for a list of EEA countries

VISA

Section 3

Visa PSD2 solutions

VISA

3. Visa's PSD2 solutions

3.1 Solution summary

Visa is implementing 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 summarised in Figure 1 below.

Figure 1: Summary of Visa's PSD2 solutions

Technology	Rules	Policies
3DS 2.2 Exemption Flags	Abandonment Rates	STIP Policy
Authorization Flags		
Trusted Listing	Risk Based Authentication	PSD2 Payment Policy
Biometrics		
Transaction Advisor	Minimum data requirements	PSD2 Regulatory Guide
Attempts Server		
Visa Token Service	Biometrics Mandate	
SCA Required Decline Code		Guidelines on common e-commerce payment use cases
STIP	Liability Activation Date	

The technology-based solutions include a suite of new product and programmes 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 new products & programmes

Foundational products and programmes	New SCA products and programmes in development
Predictive analysis • Dynamic modelling based on current fraud trends, geographies and segments to effectively manage risk • Models built and maintained by Visa and refreshed every 12 months **3-D secure** • Industry standard for authentication • 2.0 has an enhanced user experience, expanded device usage, greater data sharing and is regulatory smart **Tokenization** • Protecting payment data by replacing traditional card account numbers with a unique token that can be restricted by device, merchant or channel	**Visa Trusted Listing** **Visa Transaction Advisor** **Visa Biometrics** **Delegated Authentication Programme**

3.2   Authorization options

3.2.1   Overview

New indicators in the authorization request message will be used by Issuers to identify Acquirer exemptions. If a merchant would like to indicate that an Acquirer exemption is to be applied, an exemption flag should be submitted in the authorization request. If the transaction is out of scope, the merchant must also ensure that the correct mechanism and indicator is used to identify that it is out of scope.

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. The Electronic Commerce Indicator (ECI) value and Cardholder Authentication Verification Value (CAVV) and / or Token Authentication Verification Value (TAVV) cryptograms are used to communicate the authentication status of the transaction (for more information see section 3.3.5). The messages work as follows:

Figure 3: Authorization request message (transaction authenticated via 3DS)

Acquirer / Acquirer Processor	VisaNet

• Creates the authorization request including:
   o The ECI, CAVV and/or TAVV
   o MIT indicators if the transaction is an MIT
   o Using appropriate MOTO indicating data if transaction is MOTO
   o Exemption flags if exemptions are being used
• Forwards the authorization request to the issuer through VisaNet
	• Recognises ECI 05 and 06 as Visa 3DS 2.0 program transactions and where a CAVV is present (for ECI 05, 06 06 07), - either:
	   • VisaNet will verify the CAVV and send the issuer the CAVV verification results, or
	   • VisaNet will forward the CAVV to the Issuer to verify
	• Includes the 3DS Indicator to the Issuer in the authorization request, if the Issuer has elected to receive it
	• Verify the TAVV and send the issuer the TAVV verification results
	• Forwards the authorization request to the Issuer Host for processing

Figure 4: Authorization response message (transaction authenticated via 3DS)

Issuer Host	VisaNet	Acquirer / Acquirer Processor	Merchant
• Receives the ECI, CAVV, and CAVV Results (if signed up for the Visa CAVV Verification Service) in the authorization message • Verifies the CAVV and updates the CAVV Results field (if issuer performs CAVV verification) • Completes their authorization decision • Returns the authorization response (approve or decline) to the acquirer via VisaNet.	• Includes the 3DS indicator to the Acquirer in the authorization request • Forwards the authorization response to the Acquirer for processing	• Forwards the authorization decision to the merchant	• Provides authorization response to cardholder

Table 3 summarises the key relevant ECI values returned by 3DS. The format and role of the CAVV is summarised in more detail in section 3.2.5

Table 3: ECI values

ECI Value	Authentication Status	Liability
ECI 5	Cardholder authenticated by the Issuer	Issuer
ECI 6	Merchant attempted to authenticate the cardholder but either the cardholder or Issuer is not participating in 3DS	Issuer
ECI 7	Payment authentication has not been performed	Acquirer

Table 4 summarises the key relevant message fields in the authorization message flow.

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

VISA

Table 4: Summary of authorization fields and messages used to communicate SCA and authorization status

Field	Set by	Function	Tag Position	Field Value/Indicator
F25	Acquirer	Point-of-Service Condition Code – required for CAVV processing		Existing values as defined in the Visa technical specification
F34	Acquirer	Allows Acquirer to indicate that authorization is being requested without the application of SCA because one of the following exemptions applies: • Low Value • TRA • Trusted Beneficiary • Corporate Cards		Tags: • 9F7C: Low Value exemption Indicator • 9F7D: TRA Exemption Indicator • 9F7E: Trusted Merchant Exemption Indicator • 9F7F: Secure Corporate Payment Indicator
F39	Issuer	Response to F34 exemption request indicating additional customer authentication required		Response code 1A (Note the Issuer has the option to use other decline codes if they prefer)
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
F60.10	Acquirer	Indicate a transaction performed with an estimated amount		2 or 3
F63.3	Acquirer	Indicate if the transaction is an out of scope MIT of the following type: • Incremental • Delayed Charges • No Show • Resubmission • Reauthorization		Values 3900 to 3904
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 transaction associated with the current MIT in either F62.2 or F125. Visa forwards this information to Issuers only in F125		In an MIT transaction, the Tran ID associated with initial CIT where agreement was set up (and SCA performed) see section 3.8 for more details
F126.13	Acquirer	Indicate if the transaction is a Recurring, Installments/Prepayment or Unscheduled Credential on File out of scope MIT		Value R, I or C

VISA

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 Tables in Section 3.2.4
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 3DS 2.0. If CAVV is present, this filed 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.

Figure 5: Main message flows for a simple e-commerce transaction
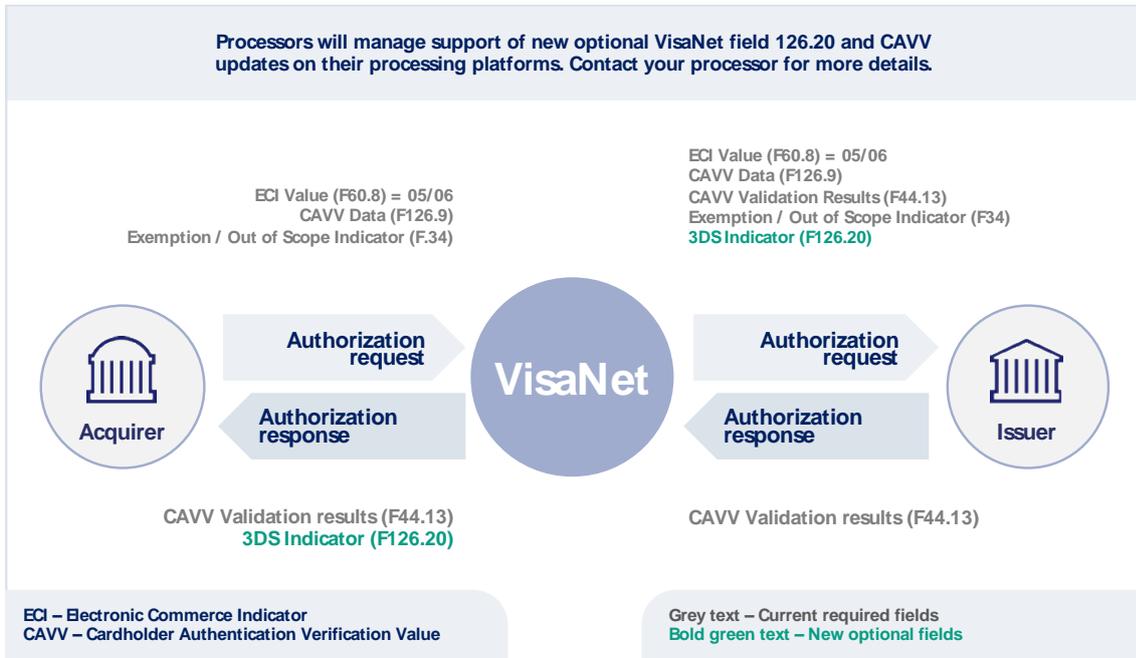
3.2.3 VisaNet Field 34 & Response Code 1A in Field 39

Visa is implementing a new field, Field 34, to support PSD2 SCA requirements by indicating an Acquirer applied exemption. Additionally, a new response code 1A in Field 39 will be available to Issuers to indicate that the transaction cannot be approved until SCA is applied.

Acquirers may use Field 34 to submit e-commerce transactions that may include one or more of the SCA exemption indicators in order to communicate to the Issuer why SCA was not performed on an e-commerce transaction. However, Visa requires that Acquirers 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 Issuer's approval rates. Issuers are required to consider SCA exemption indicators and out of scope information when deciding whether or not to approve an authorization request.

Field 34 Dataset ID 56 also supports the addition of optional supplemental data through two new tags. These carry the consumer device IP address and the Visa Consumer Authentication Service (VCAS) score, for Issuers using VCAS. This supplementary information aims to help Issuers improve their approval rates.

Acquirers and Issuers in the Europe region can choose to support these changes from the January 2019 release. Effective with the October 2019 release, the changes will become mandatory for Acquirers and Issuers in the Europe region. 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 by October 2019.

Issuers that want to receive F34 must complete VisaNet Certification Management Service (VCMS) testing before the field is activated.

Table 5 provides a simple summary of the indicators for the key exemptions.

Table 5: Summary of Field 34 and 3DS2.2 indicators for exemptions

Exemption / Out of Scope Reason/ Reason PSP does not require SCA	Acquirer or Issuer applied	EMVCo 3DS2.2 Indicator Yes or No	ECI Value	Field 34 Yes or No	Visa or Merchant Populated
Transaction Risk Analysis	Acquirer	Yes	7	Yes	Merchant
	Issuer	No	5	No	N/A
Low Value	Acquirer	No	7	Yes	Merchant
Secure Corporate Payment	Issuer	No	7	Yes	Merchant

Delegated Authority	Acquirer	Yes	7	Yes	Merchant

3.2.3.1 Impact for Acquirers

Acquirers must be able to:

1. Support the new Field 34—Electronic Commerce Data, Dataset ID 56—Supplemental Data in TLV format with new tags to indicate whether an e-commerce transaction is exempt from the PSD2/RTS SCA mandate
2. Receive the response code 1A (Additional customer authentication required) in existing Field 39
3. Support the MIT Framework for both PAN and token transactions to ensure out of scope MITs can be identified as such by Issuers

Testing is required for Acquirers to support the new SCA exemption indicators in the new TLV Field 34, Dataset ID 56. Testing is not required for Acquirers to receive the new response code 1A in existing Field 39.

3.2.3.2 Impact for Issuers

Issuers in the Europe region must:

1. Be able to receive TLV Field 34—Electronic Commerce Data

2. Use response code 1A when a transaction has been declined due to the absence of SCA

3. Not use response code 1A for a transaction where the Acquirer or merchant is located outside the EEA

4. Receive initial Transaction ID in Field 125 if they do not already receive it (currently optional)

Issuers may respond with the new response code 1A for both e-commerce and card present contactless point of sale (POS) transactions.

Issuers that choose to receive the supplemental data must be able to receive the new Field 34—Electronic Commerce Data, Dataset ID 56—Supplemental Data in TLV format with new tags and must be aware of new processing rules to support the new supplemental data.

Issuers should not use response code 1A for Merchant Initiated Transactions, MOTO or One Leg Out transactions.

3.2.4   The new VisaNet 3DS Indicator Field 126.20

Visa has included a new optional field in an 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, OTP, etc.)

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 utilise the new 3DS Indicator Field 126.20 will need to take account of the following:

- A new CAVV format is required, which includes the authentication result for all 3DS 2.0 transactions

- The Updated CAVV format can be used with 1.0 transactions, but the authentication method will not be provided

- Issuers that want to receive F126.20 must complete VisaNet Certification Management Service (VCMS) testing before the field is activated

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

Table 6: The values for Field 126.20

3DS Indicator Value	3DS Description
0	3DS 1.0.2 or prior all authentication methods
1	3DS 2.0 Challenge flow using Static Passcode
2	3DS 2.0 Challenge flow using OTP via SMS method
3	3DS 2.0 Challenge flow using OTP via key fob or card reader method
4	3DS 2.0 Challenge flow using OTP via App method
5	3DS 2.0 Challenge flow using OTP via any other method
6	3DS 2.0 Challenge flow using KBA method
7	3DS 2.0 Challenge flow using OOB with Biometric method
8	3DS 2.0 Challenge flow using OOB with App login method
9	3DS 2.0 Challenge flow using OOB with any other method
A	3DS 2.0 Challenge flow using any other authentication method
B	3DS unrecognized authentication method
D	3DS 2.0 Frictionless flow, RBA Review

E	3DS 2.0 Attempts Server responding
F	3DS 2.0 Frictionless flow, RBA

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

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

Visa will require Acquirers to include the CAVV data for all 3DS e-commerce transactions (ECI 5 and ECI 6). Any transactions that do not have a CAVV will be downgraded to ECI 7.

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 5 and ECI 6). Any ECI 5 or ECI 6 transactions without a CAVV will be downgraded to ECI 7 and the acquirer will no longer benefit from fraud liability protection.

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

Visa will be enhancing the CAVV in the near future to support new 3DS use-cases, multiple authentication methods, a merchant identifier, etc.

3.2.5.1   TAVV Data in Field 126.8

Filed 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 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 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 3DS, Field 126.9 can optionally be populated with the TAVV.

3.2.5.2   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 5 or ECI 6 transaction, the ECI value will be downgraded to ECI 7 (non-authenticated)

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

3.2.5.3   Field 44.13 CAVV Results Code

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

- The classification of the transaction (either an authentication transaction where the Issuer ACS has created the CAVV or an attempts transaction where the Issuer attempts server or Visa Attempts Service has created the CAVV)

- For an authentication transaction, where the Issuer ACS created the CAVV

- For an attempts transaction, where the Issuer attempts server or Visa Attempts Service created the CAVV

- The CAVV verification result:

    o   CAVV verification passed

    o   CAVV verification failed

For token transactions that go straight to authorization without first performing 3DS, Field 44.13 can optionally be populated by 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.

3.2.6   Non-authenticated secure transaction with 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 7 in existing Field 60.8—Mail/Phone/Electronic Commerce and Payments Indicator in authorization request messages

- ECI 7 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: 3-D Secure CAVV, Revised Format in authorization and full financial request messages

- ECI 7 in BASE II Draft Data

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

3.3   3-D Secure 2.0

This section provides a brief summary of the key features of the 3-D Secure 2.0 protocol. More details and the full specifications are available from EMVCo at https://www.emvco.com/emv-technologies/3d-secure/

3-D Secure provides a strong customer authentication solution that supports Issuers, Acquirers and merchants to provide SCA. 3DS 1.0.2 is widely used in Europe and provides basic SCA functionality.

3-D Secure 2.0 (3DS 2.0) is the new 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.

Information about Visa's 3-D Secure programme can be found on the Visa Technology Partner site https://technologypartner.visa.com/Library/3DSecure2.aspx

3.3.1   The benefits of 3DS 2.0

3DS 2.0 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, utilising a significantly increased number of transaction and customer data elements to securely authenticate the majority of transactions, without the need for the customer to go through SCA

- 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

3DS 2.0 also supports non-payment authentication use cases, for example the setting up of a payment mandate or enrolling a merchant to a cardholder's list of trusted beneficiaries.

3.3.2   3DS 2.0 terminology

3DS 2.0 differs in a number of ways from 3DS 1.0 and the terminology used has changed to reflect this.

Table 7: Comparison of commonly used terms

Previous 3DS 1.0 Term	3DS 2.0 Term
Merchant	3DS Requestor (a merchant is an example)
Merchant Plug-in (MPI)	3DS Server
n/a	3DS Requester Environment
Merchant Integrator	3DS Integrator
n/a	3DS Requestor App

3.3.3 3DS 2.0 domains and components

Visa's 3-D Secure 2.0 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 below:

Figure 6: Domains and components

Merchant / Acquirer Domain	Visa Interoperability Domain	Issuer Domain
3DS Server / 3DS SDK 3DS Server (software)　　3DS SDK (software)	**Visa Directory Server** Visa Directory Server	**Issuer Access Control Server (ACS)** Issuer ACS server
Merchant's E-Commerce Software	**Visa Attempts Service** Visa Attempts Server	
Acquirer / Acquirer Processor Payment processing system	**VisaNet** VisaNet	**Issuer / Issuer Processor Host System** Issuer Host

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

Table 8: The role of the main components

Component	Description
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 3-D Secure messages • Authenticating the DS • Validating the DS, the 3DS SDK, and the 3DS Requestor • Ensuring that message contents are protected
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
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 programme rules (for example, logos, time-out values, etc.) • Onboarding 3DS Servers and ACSs • Maintaining ACS and DS Start and End Protocol Versions and 3DS Method URLs • Interacts with VTS to de-tokenise 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 Service	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

VISA

3DS 2.0 enables merchants to send a message to an Issuer to carry out the authentication process.

The environment and basic message flow that comprises 3DS 2.0 and underpins both the frictionless and challenge flows is summarised in figure 7. Familiarity with this will help readers understand the concepts around application of 3DS 2.0, discussed in this guidance.

Figure 7: The 3DS 2.0 secure environment and message flows
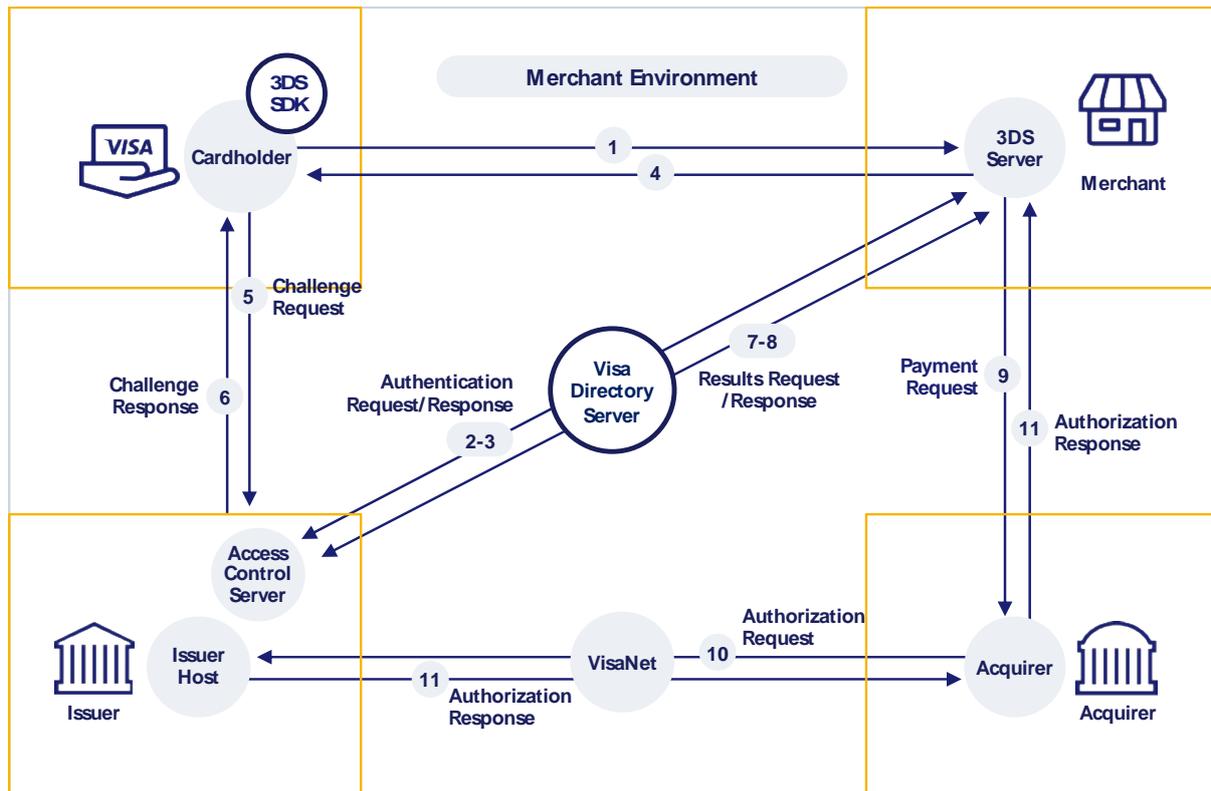
3DS 2.0 supports two primary authentication flows:

- 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 an 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 flags requesting an exemption is applied

- Step 3: The Issuer's Access Control Server (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, an 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 an SCA challenge is required.

For more detail on the messages, refer to the Visa Merchant/Acquirer and Issuer Implementation Guides for Visa's 3-D Secure 2.0 Program.

3.3.5 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 9 provides full details:

Table 9: Visa authentication elements

Data Elements	Created by	Purpose
Electronic Commerce Indicator (ECI)	Issuer ACS, Issuer Attempts Server, or Visa's Attempts Service	Indicates the level of authentication that was performed on the transaction The ECI value is passed to merchant and included by the merchant in the authorization request.
Cardholder Authentication Verification Value (CAVV)	Issuer ACS, Issuer Attempts Server, or Visa's Attempts Service	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 a field that the Issuer or Acquirer can choose to receive in authorization Communicates the 3DS version number and the 3DS 2.0 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 Merchant/Acquirer Implementation Guide for Visa's 3-D Secure 2.0 Program section 1.3.

3.3.6 Risk Based Authentication

3.3.6.1 Introduction to RBA

Risk Based Authentication (RBA) is a process that may be used by Issuers to risk assess and score 3DS transactions to reduce the volumes that require active authentication. It enables Issuers 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)

- Risk assess transactions submitted via 3DS 2.0 with an Acquirer exemption flag (3DS specification version 2.2 onwards) and decide whether to apply the right of final say over whether SCA should be applied to a transaction

- Reduce false declines

Visa considers RBA to be critical to reducing unnecessary challenges and friction and has issued a global rule mandating that Issuers support it.

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 3DS 2.0 and enables "frictionless" authentication of low risk transactions. The 3DS 2.0 specification defines up to 135 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. The data elements are listed in Appendix A.1. They 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 assessed as high, or the Issuer's fraud rate is outside the reference fraud rate, a challenge will need to be completed.

3.3.6.2 Benefits of RBA

Risk Based Authentication has already delivered significant benefits in the markets where it has been deployed. Today, in a UK pre-PSD2 environment, 95% of transactions that undergo a risk-based assessment do not require 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 3DS 2.0 will increase the effectiveness of RBA even further. Visa analysis shows that the addition of just one of those data points – device ID information – improves fraud detection rates by 200%+. In cases where it is necessary to apply SCA, applying behavioural biometrics and/or undertaking RBA alongside the application of two independent SCA factors further strengthens the effectiveness of authentication. This is what Visa refers to as a "layered approach".

3.3.7 Data elements

The Data Element Types supported with 3DS 2.0 include:

Table 10: 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 Info (e.g., dollar amount, transaction type, recurring/installment, etc.) • 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 data
Merchant Risk Indicator	• Pre-order indicator • Gift card amount, currency, count • Shipping & delivery information
Cardholder Account Information	• Cardholder account age, date, change • Password change
Device Information	• Platform Type • Device Model • Browser/SDK

Visa is introducing a rule to ensure that minimum data provision standards are applied. A complete list of data elements is at Appendix A.1.

3.3.8 Token transactions and 3DS

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

VISA

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

3.3.9   UX considerations

3DS 2.0 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 8.

Figure 8: Relative benefits of native UI v HTML

Native UI Benefits	HTML Benefits
• Integrates seamlessly into the Merchant App UI • Merchant look and feel customisations • Positions for future devices that do not support HTML	• Allows for use of Issuer branding, Issuer design, and Payment System branding familiar to Cardholder • Provides flexibility to the Issuer to leverage an established authentication experience for the cardholder • Consistent with browser-based transactions

It should be noted that while the merchant has the option to brand aspects of the native UI and customise the wording of the header, the content of the challenge messages is determined by the Issuer and served by the Issuer's ACS. Visa will provide best practice guidelines on the content of challenge messages. For more information please refer to the 3DS UX Guidelines available on the Visa Developer Center.

3.3.10 3DS 2.0 on different platforms

3DS 2.0 has initially been specified to support desktop browser and mobile (HTML and native app) platforms. Future versions of the specification will extend support to other platforms including games consoles, allowing seamless support of in game purchases.

3.3.11 The transition from 3DS 1.0 to 3DS 2.0

3DS 2.0 began deployment across Europe from the end of 2018 and will continue through 2019. To take advantage of the new services summarised in Section 3.3.14, it is highly recommended that clients and merchants upgrade to 3DS 2.0 by September 2019.

As a global protocol, Visa will continue to support 3DS 1.0, but in Europe 3DS 2.0 is expected to be the most used version.

3.3.12 3DS 1.0 as a fall-back option for application of SCA

Issuers in the EEA who are unable to implement 3DS 2.0 before September 2019 will be able to provide SCA through 3DS 1.0 for a limited transition period, subject to the following:

- Effective transaction monitoring mechanisms must be in place, to detect unauthorized or fraudulent payment transactions in order to meet the General Authentication Requirements defined in Article 2 of the Regulatory and Technical Standards. These mechanisms should allow capturing of the following information:

    o Lists of compromised or stolen authentication elements;

    o The amount of each payment transaction;

    o Known fraud scenarios;

    o Signs of malware infection in any sessions of the authentication procedure;

    o In the case that the access device or the software is provided by the PSP, a log of the use of the access device or the software and any abnormal use.

- Challenge methods must be deployed that are compliant with the PSD2 requirement and that meet Visa rules (please refer to The Visa Paper Preparing for PSD2 SCA November 2018 section 2.2 and Visa programme requirements as detailed in Visa's 3DS Implementation Guides) and that minimise friction in the customer experience

- Risk Based Authentication must be deployed to ensure that challenges are only applied appropriately

3.3.13 The co-existence of 3DS 1.0 and 3DS 2.0

3DS 2.0 and 3DS 1.0 are two separate, distinct protocols, supported by two separate Directory Servers that will co-exist independently in parallel for a transition period. Both protocols will continue to be supported until 3DS 2.0 reaches maturity in the market. Visa expects to announce a sunset date for 3DS 1.0, after which 3DS1.0 will no longer be supported, in due course.

During the transition period, when not all Issuers support 3DS 2.0, 3DS Server Providers will utilize protocol version information to package messages accordingly and send to appropriate 3DS Directory Server as illustrated below.

Figure 9: Routing of authentication request messages during the transition period
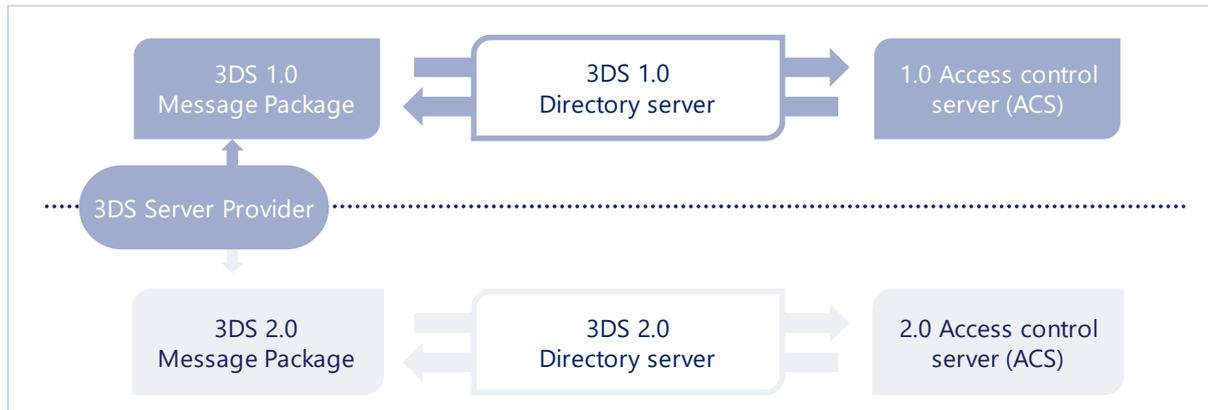
Visa is setting a 3DS 2.0 merchant liability protection activation date of April 2019 in Europe.

It should be noted that from the Implementation Date in April 2019, a merchant that has upgraded to 3DS 2.0 will retain liability protection for a 3DS 2.0 authenticated transaction under the Visa Rules even if the Issuer does not support 3DS 2.0.

In this case, if an Issuer's ACS is unable to respond to a 3DS 2.0 Authentication Request message, the Visa Attempt Server will respond. It provides a cryptogram to enable the merchant to prove they attempted authentication.

After the implementation date, merchants submitting 3DS 2.0 requests to Issuers that do not yet support 3DS 2.0 will benefit from liability protection, however merchants should note that these transactions will be returned by the Visa Attempt Server as ECI 6 and will be risk assessed by Issuers as part of the authorization process. As such they may be at a higher risk of decline if they fail the Issuers' risk score.

After April 2019, merchants should consider falling back to 3DS 1.0 when submitting transactions to Issuers that do not yet support 3DS 2.0 to maximise the probability of successful authorization.

Merchants should also note that submitting a 1.0 message to a 2.0 Directory Server will not get an appropriate response.

3.3.14 The 3DS 2.0 roadmap

3.3.14.1 The 3DS 2.0 Specification and feature roadmap

The 3DS specification will continue to evolve adding features through a number of releases.

Table 11: Key enhancements on the 3DS v2.1 specification release

EMV 3DS Specifications Version 2.1 – Released: October 2017	Live Date: Q4 2018	
Notable Features	Feature description
3DS Requestor Initiated (3RI) Messages	A channel that allows the merchant to initiate the authentication request without the cardholder being in-session
Support of App based purchases	Supports app-based purchases on mobile and other consumer devices
Checkout Integration	Enables merchants to integrate authentication into their checkout process for both app and browser-based implementations
Enriched data	Provides enriched data to support frictionless transactions
Challenge method support	Supports multiple options for step-up authentication.
ID&V	Enables merchant-initiated account verification

Table 12: Key enhancements in the 3DS v2.2 specification release

EMV 3DS Specifications Version 2.2: Released December 2018, Live Q2 2019	
Notable Features	Feature description
SCA/TRA Indicators	Indicator if the Acquirer Strong Consumer Authentication (SCA) or Transactional Risk Analysis (TRA) was already performed prior to the authentication message being sent
FIDO[2], Token, and Secure Remote Commerce (SRC) Data	Additional information as to how the cardholder logged in to their 3DS Requestor Account Specification has been updated to carry additional FIDO, Token and SRC data from the merchant to the Issuer
Whitelisting support	Support for enrollment at checkout and subsequent frictionless transactions
3DS Requestor Initiated (3RI) payments	This channel only supported non-payment transactions within v2.1.0 for account verification purposes only This channel has been expanded to payments in 2.2.0
Decoupled Authentication	A new authentication method which allows cardholder authentication to occur if the cardholder is off-line This authentication method can also be used if the cardholder is on-line via our Browser and App channels
Support of MOTO	3DS can be applied to MOTO transactions by utilising 3RI and Decoupled Authentication
Improvements to the EMV 3DS Caching process (PReq/PRes cycles)	The PReq/PRes messages are utilised by the 3DS Server to cache information about the Protocol Version Numbers(s) supported by available ACSs, the DS, and also any URL to be used for the 3DS Method call

Much of the functionality in Version 2.2 will enable management of the more complex of the payment use cases summarised in Section 5.

---

[2] The FIDO Alliance is an open industry association focussed on developing strong authentication standards. For more information see https://fidoalliance.org/

VISA

3.3.14.2 Notable roadmap features

3.3.14.2.1 3DS Requestor Initiated (3RI) payments

3DS Requestor Initiated (3RI) is a 3-D Secure transaction initiated by the 3DS Requestor for the purposes of confirming that an account is still valid or for Cardholder authentication. For merchants, a 3RI transaction enables the ability to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions previously authenticated. For issuers, a 3RI transaction's prior transaction data improve risk management and provide secondary evaluation on a previously authenticated transaction. This feature allows merchants who have performed authentication for a transaction to maintain their fraud liability protection under legitimate circumstances, such as delayed or split shipment.

The feature can be used to enable merchants to effectively manage some complex payment use cases by for example:

- Allowing an authorized entity in a Multi-Party Commerce scenario to request a CAVV on behalf of a merchant.
- Allowing a merchant to obtain a new CAVV in case of split or delayed shipment when only 1 or more item is not ready for shipment til a much later date
- Requesting a new CAVV to maintain liability protection when authorization is sought more than 90 days after a transaction has been authenticated.

Examples of where this may be used for specific transaction types are included in section 5.

3.3.15 The Visa 3DS 2.0 implementation roadmap

Figure 11: Visa's roadmap for implementation of 3DS
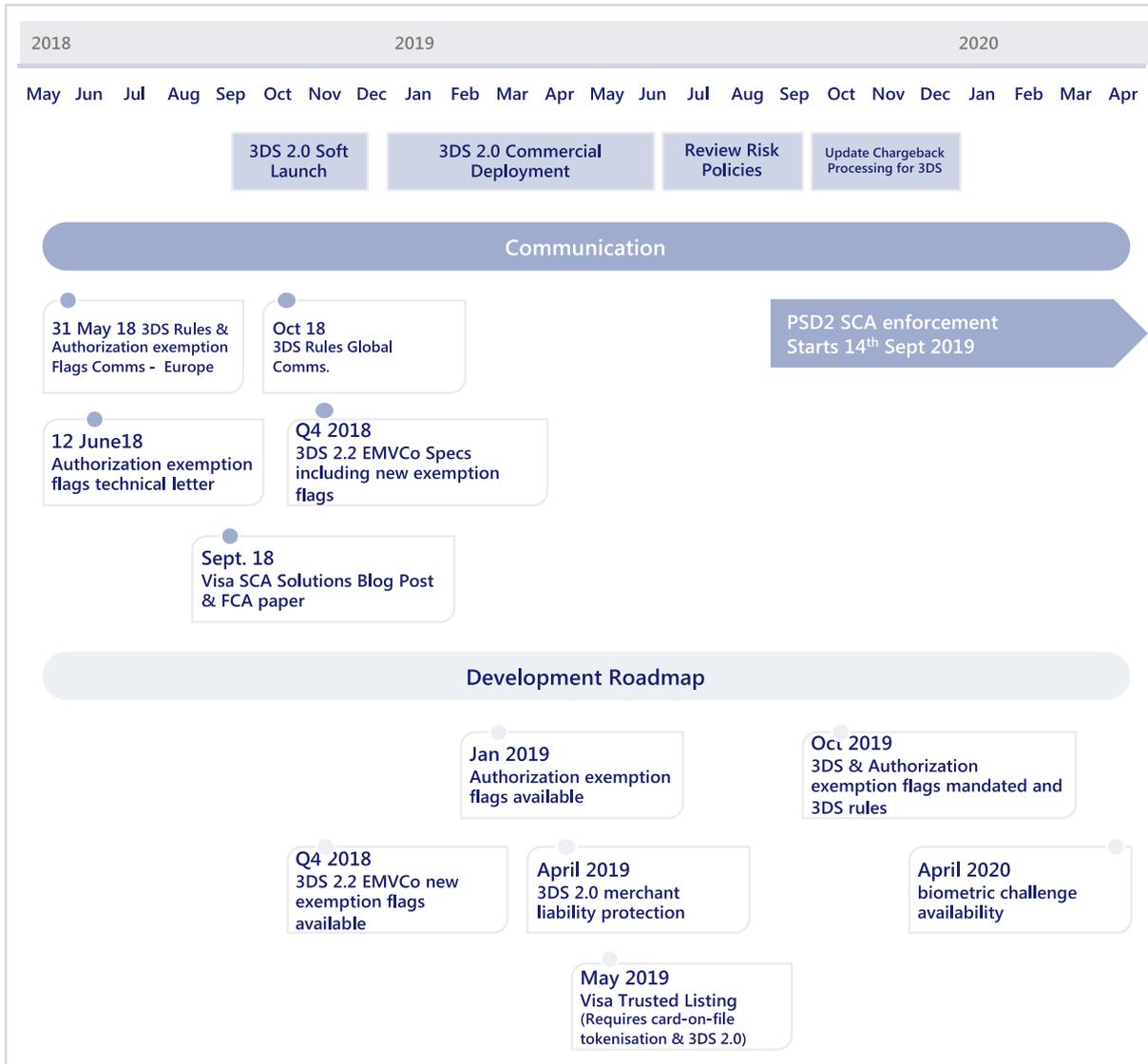
3.4 Visa rules & policies for PSD2 & 3DS

Visa is applying rule changes to ensure consistent and optimum application of the new framework and to encourage Issuers to balance risk management with the minimisation of friction. Minimum standards for authentication abandonment, risk analysis technology, the application of biometrics and minimum data requirements will all contribute to a smoother authentication experience and lower fraud rates.

Currently proposed rules are summarised in the table 13 and more detail is given in Appendix A.3. However, as the new rules are currently going through Visa's approvals process, stakeholders should be aware that these rules are subject to change.

Table 13: Proposed new rules summary (*subject to change)

Rules	Description	Effective Date
Risk Based Authentication Capability	Issuers are required to support RBA for 3DS 2.0 and must evaluate the risk level of each transaction using some form of risk-model, rules engine, or risk analysis, and then apply SCA as required according to the risk level.	19 October 2019
Authentication Abandonment Rate	Abandonment rates should not exceed 5% (measured as cancelled or timed out 3DS authentication requests divided by the total number of authentication requests)	19 October 2019
Authentication Response Time Threshold	Issuer must provide response to initial 3DS 2.0 authentication request (AReq) within 5 seconds	19 October 2019
Issuer Access Control Server (ACS) Availability	An Issuer's ACS must be available at least 99% of the time. Availability will be measured by: number AReq timeouts / total number of AReqs.	19 October 2019
Biometrics Challenge Availability	Issuers must provide biometric authentication capability for 3DS 2.0	April 2020
Minimum Data Requirements	Merchants must provide the data elements as defined listed in Appendix A.1	April 2019
Processing	For a 3DS 2.0 transaction, in order to receive liability protection, an Acquirer/merchant must submit the same ECI value in clearing that was submitted in authorization. Applies to ECI 05 and ECI 06.	Existing requirement
Exemption Enablement	Merchants or their Acquirers submitting transactions under an Acquirer PSD2 SCA exemption must include exemption indicators in the authorization request.	October 2019*
Issuer SCA requirement (1)	Issuers needing SCA to be performed by a merchant may decline authorizations with the SCA required decline code	October 2019*
Issuer SCA requirement (2)	Issuers may not decline transactions with an SCA required decline code if the authorization request includes a valid CAVV	October 2019*
Indicating a transaction is an MIT	When processing a merchant initiated transaction, for it to be understood as out of scope of SCA, Acquirers must ensure it contains indicators informing Issuers this is an out of scope MIT	October 2019*

VISA

Issuer requirement to recognise MITs	Issuers must be able to recognise transactions are MITs, this includes receiving F125. Note – there is an existing requirement for Issuers to recognise MITs that has been in force since October 2016, however Issuers may have previously elected not receive the initial Tran ID in F125	October 2019*
Issuer requirement to Evaluate each Transaction	An Issuer must evaluate each Transaction that has been properly accepted, processed, and submitted in order to make an Authorization, a payment Token provisioning, or other decision, and 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. Applies to EU.	Existing rule
Systematic exemption declines	Visa Issuers may not systematically decline Acquirer exemptions or out of scope transactions unless they are flagged incorrectly	October 2019*
Systematic 3DS declines	Transactions sent via 3DS with a TRA request flag may not be systematically challenged	October 2019*
SCA declines for MITs	Issuers may not use a SCA required decline code for an authorization request with an MIT indicator	October 2019*
Exemption exceptions	Issuers receiving ECI 6 or ECI 7 authorization requests without a valid exemption indicator in F34 should use VAA or equivalent risk scoring technology to enable Issuer TRA exemptions to be applied	*Guideline*
3DS decline rule for TRA	If an Issuer receives an authentication request via 3DS with a TRA Acquirer exemption indicator, they may not decline the same transaction at authorization with a SCA required decline code.	October 2019*

3.5   Visa Trusted Listing

Visa is building a capability for consumers to speed checkout at preferred digital merchants, by adding merchants to their Issuer's "trusted" list. When making a purchase with a participating merchant, consumers will be asked during checkout if they'd like to add this merchant to their trusted list. Once SCA has been completed, the merchant will, subject to Issuer approval, be added to the consumer's list of trusted merchants on their Issuer's web or mobile banking application. Subsequent visits to trusted merchants should generally not require SCA.

The Visa Trusted Listing solution aims to deliver enhanced security, improve fraud performance and minimise the possibility of transaction declines. It also provides a complete hosted solution for Issuers minimising the development and operational overhead associated with offering a trusted beneficiaries solution.

The service is expected to be available mid-2019.

Merchants who use Visa Token Service (VTS), and wish to take advantage of trusted listing can benefit from some enhanced features including:

- **Trusted Listing enrollment:** merchants can partner with Issuers to enable the push provisioning of trusted tokens via the Issuer app, further streamlining the authentication process

- **Trusted Listing Lifecycle management:** Issuers integrated with VTS can use the VTS LCM API to cancel trusted listing entries on behalf of their customers

- **Trusted Listing notifications:** merchants integrated with VTS can receive notifications of changes made to trusted listings relating to their customers enabling them to optimise their user experience and transaction flow.

3.6   Visa Transaction Advisor

Visa is creating a tool to help merchants, gateways and Acquirers identify low risk transactions and, in the case of remote transactions, apply for SCA exemptions. Visa Transaction Advisor will conduct a pre-authorization status check and return values for SCA exemption qualification, transaction risk analysis, exemption recommendation and a reason code. The service is expected to be available mid-2019 and will be available through 3DS or an API.

3.7   Visa Delegated Authentication

The PSD2 regulation allows PSPs to outsource operational functions of payment services to a third-party. Visa is establishing a Delegated Authentication Program that will facilitate the delegation of the authentication process, making it easier for members to delegate authentication to third parties that are eligible to participate in the programme.

The Visa Delegated Authentication Programme provides delegates with the opportunity to use either 3DS or VTS for the establishment of the authentication code needed for dynamic linking, together with indicators as to the identity factors used as part of the delegated authentication.

To assist in the establishment of the identification factors used, VTS also supports the capability for merchants using tokens to bind those tokens to customer accounts and customer devices. Device binding enables the device to be used as a possession factor within the delegated authentication framework.

3.8 The Visa MIT Framework

Visa has already established the MIT Framework to enable Acquirers and Issuers to correctly flag and identify MIT transactions.

> ### Best Practice
>
> To avoid Issuers inappropriately declining transactions and requesting SCA even though the cardholder is not available, merchants must implement the MIT Framework.

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

The MIT framework includes requiring the initial CIT performed at mandate set up to be linked to subsequent MITs for increased visibility during disputes. While the MIT framework is not mandated to be used by merchants for PAN based transactions[3] (it is mandated for token based transactions), in the PSD2 context, if the framework is not used to identify transactions where the cardholder is not available to be authenticated, the Issuer will not be able to recognise the transaction as out of scope of PSD2 and may unnecessarily decline even though the cardholder is not available. To avoid this experience, the MIT Framework needs to be implemented by the ecosystem for all merchant initiated transactions, PAN or token based.

The Visa MIT framework defines a number of different types of MIT as summarised in the table below.

---

[3] Not mandated by Visa for merchant 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.

Table 14: 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 considered by Visa to be out of scope of PSD2. Recurring transactions that are in scope of PSD2 (and therefore may benefit from the recurring exemption) are those that are customer (payer) initiated, 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 considered by Visa to be out of scope)
Incremental	An incremental authorization is typically found in hotel and car rental environments, where the cardholder has agreed to pay for any service incurred during the duration of the contract
Delayed Charges	A delayed charge is typically used in hotel, cruise lines and vehicle rental environments 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

VISA

The first six types of MITs occur where a new transaction is initiated by the merchant under an existing established agreement and are therefore considered by Visa to be out of scope of SCA[4]. However, to establish such an agreement, an initial CIT must be performed, when the mandate is set up or Ts&Cs agreed.

> ### Best Practice
>
> 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 more detail refer to Section 5.9).

The last two types (reauthorization and resubmission) are cases 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 was declined due to insufficient funds despite service already rendered, or because the order cannot be delivered in one shipment), therefore, no further authentication of the cardholder is required. The transaction is payer initiated and provided the reauthorization / resubmission is properly labelled as per the MIT framework, all parties processing the transaction will be able to identify the original authentication.

Table 15 identifies the key data fields to be used in authorizations for the eight different types of MIT, and the initial CIT to which the MIT is related.

Note that for any of the transactions in table 15, be they first or subsequent transactions, the merchant should use POS entry mode 10 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 therefore 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 and should not use it if they stored it only to complete this specific transaction only. For more information about the Stored Credential Framework and what is required to use it, see Appendix A.4.

---

[4] PSD2 specifically states that SCA applies to payments initiated by the payer. Visa's position, confirmed by the EBA and FCA, is therefore that transactions initiated by the payee are out of scope of SCA.

VISA

Table 15: Key data fields for performing MIT transactions

Description	Transaction Type	POS Entry Mode (PEM) (F22)	POS environment (F126.13)	Message Reason Code (F63.3)	Transaction ID (F125**)
Installment/Prepayment	First Transaction (CIT) (May be of zero value if set up only)	Any valid* (10 if stored credential)	I	--	--
	Subsequent Transactions (MIT)	10	I	--	Tran ID of first transaction
Recurring	First Transaction (CIT) (May be of zero value if set up only)	Any valid* (10 if stored credential)	R	--	--
	Subsequent Transactions (MIT)	10	R	--	Tran ID of first transaction
Unscheduled Credential on File (UCOF)	First Transaction (CIT) (May be of zero value if set up only)	Any valid* (10 if stored credential)	C	--	--
	Subsequent Transactions (MIT)	10	C	--	Tran ID of first transaction
Incremental	First Transaction (CIT) (Estimated transaction)[5]	Any valid* (10 If stored credential)	--	--	--
	Subsequent Transactions (MIT)	Any valid* (10 if stored credential)	--	3900	Tran ID of first transaction
Delayed Charges	First Transaction (CIT)	Any valid* (10 if stored credential)	--	--	--
	Subsequent Transactions (MIT)	01 or 10 if stored credential	--	3902	Tran ID of first transaction

---

[5] 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.

VISA

No Show	First Transaction (CIT)	Any valid* (10 if stored credential)	--	--	--
	Subsequent Transactions (MIT)	01 or 10 if stored credential	--	3904	Tran ID of first transaction
Reauthorization	First Transaction (CIT)	Any valid* (10 if stored credential)	--	--	--
	Subsequent Transactions (MIT)	01 or 10 if stored credential	--	3903	Tran ID of first transaction
Resubmission	First Transaction (CIT)	Any valid* (10 if stored credential)	--	--	--
	Subsequent Transactions (MIT)	01 or 10 if stored credential	--	3901	Tran ID of first transaction

*Any valid because these transactions can also originate in F2F channels.

** Acquirers may submit the original Transaction Identifier either in Field 62.2 or in Field 125 Usage 2 DS 03, but Visa always forwards to Issuers the original Transaction Identifier received in either Fields in Field 125. Not every Issuer participates to receive this Field 125, therefore in the PSD2 context, for Issuers to be able to recognize out of scope transactions and recognize links between transactions as appropriate, Visa intends that they be mandated to receive this Field from October 2019 (although these rules are subject to change before finalization). Note that Visa always generates a new, unique, Transaction Identifier for each transaction, including subsequent MITs (except in the case of incremental authorizations.) Field 62.2 in the MIT authorization request to Issuers and in the MIT response message to the Acquirer will carry this new Transaction Identifier value and not the original Transaction Identifier that the Acquirer may have submitted in Field 62.2 in the MIT request.

3.9   Visa Biometrics

Visa is developing biometric capabilities to provide a consumer-friendly alternative to one-time-passwords, when additional SCA is required. The Visa Biometric SDK and APIs will enable push notification to the Issuer's app. Consumers can securely approve the transaction details using their fingerprint, face or even voice. The service is expected to be available mid-2019.

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 3-D Secure.

At the core of the product are Transaction Risk Analysis (TRA) authentication 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 behaviours. This network-wide level of intelligence gives Issuers the ability to decide if and when additional authentication is needed. When SCA is required, VCAS supports multiple methods 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 Cardinal Commerce, an industry leader in digital payment authentication that is fully owned by Visa. VCAS will fully support 3DS 1.0 and 3DS 2.0 along with the other authentication products in the Visa portfolio. Issuers seeking support in migrating to 3DS 2.0 may wish to consider VCAS as an option to enable the transition.

Section 4

Optimising the payment experience under PSD2

VISA

4. Optimising 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 will be optional.

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

- Optimisation of user experience

- Liability protection

It is critical that merchants and Acquirers flag transactions correctly to ensure Issuers are able to identify transactions where SCA is not needed and authorize appropriately. Visa is providing 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 provides guidance on the:

- 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 provides guidance 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)

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

VISA

4.2 Key principles

4.2.1 The difference between Authentication and Authorization

The application of SCA and exemptions may be delivered through and impacts both the authentication and authorization processes.

- Authentication ensures that the cardholder is the rightful owner of the Visa payment account and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 3-D Secure
- 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

Both systems can be used to indicate the nature of the transaction, whether it is out of scope, requires SCA, or is being processed under one of the exemptions. Transactions that are out of scope are most likely to be sent directly to authorization without authentication being deployed. However, merchants and Acquirers do have a choice in how to indicate an Acquirer exemption to the Issuer. They may either:

- Submit transactions via 3DS for authentication with an exemption request flag and then submit to authorization with the appropriate authentication data including an exemption flag[6]

- Bypass 3DS and submit transactions direct to authorization with an exemption flag. If the Issuer accepts the exemption no further additional authentication is needed, however Acquirers should note that the Issuer has the right to request resubmission via 3DS if it assesses that authentication is required.

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

4.2.2 MITs, CITs and stored credentials

In order to understand how to manage MITs in a PSD2 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.
- An MIT always relates to a previous CIT (even if it is a zero-value transaction) that was performed to establish the initial agreement with the cardholder.
- Note that subscription type payments are processed in the Visa system as "recurring payment". These are processed as MITs and considered by Visa to be out of scope.
- **A cardholder-initiated transaction (CIT)** is any transaction where the cardholder actively participates in the transaction. This can be either at a terminal in-store or

---

[6] Available for Trusted Beneficiaries and Low Risk exemptions

through a checkout experience online. When the transaction is online or via a mobile application it can be facilitated either as a guest checkout, or with a stored payment credential that the cardholder has previously consented to store with the merchant.

- **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. Visa has introduced a Stored Credential Framework to govern the use of stored credentials. More details are included in Appendix A.4.

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.

4.2.3 Principles for implementing SCA

Irrespective of the business processes that a merchant uses for eCommerce transactions, there are some fundamental principles, which PSD2 and Visa have defined, that shape the approach a merchant takes to performing an authorization. These principles are summarised below and are the basis for the approach in handling each of the different scenarios in Section 5.

4.2.3.1 PSD2 principles for implementing SCA

Table 16: PSD2 principles determining whether a payment transaction is within scope of PSD2 SCA

Principle	Rationale
CITs are in scope of SCA	If a customer initiates an electronic transaction, the transaction is within scope of SCA. Depending on circumstances, exemptions may be applied.
MITs are out of scope of SCA	If a merchant initiates an electronic transaction based on prior agreement with a customer and without the involvement of the customer, the transaction is out of scope of SCA. SCA is required in most cases when setting up an agreement to process future MITs.
MOTO transactions are out of scope of SCA	Mail order and telephone order (MOTO) transactions are out of scope of SCA.
One-leg-out transactions are out of scope of SCA	A transaction where either the Issuer or Acquirer is located outside the EEA are out of scope of SCA. SCA should be applied to these transactions on a 'best effort' basis.
Anonymous transactions are out of scope of SCA	Transactions through anonymous payment instructions are not subject to the SCA mandate, for example anonymous prepaid cards.

If a payment transaction is <u>out of scope</u> of SCA, then the merchant / Acquirer must submit an authorization ensuring that appropriate information is present that allows the Issuer to recognise that the transaction is out of scope of SCA. For example, by including relevant MIT indicators, or properly flagging as MOTO.

4.2.3.2 Visa principles for implementing SCA

4.2.3.2.1 Implementing SCA in common payment use cases

The following table summarises Visa's guiding principles for implementing SCA in common **payment use cases** for both CIT and MIT transactions.

Table 17: 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.
	Adjustment to existing order (e.g. change of available items or change of shipping costs)	Depending on the circumstances, SCA may not be required assuming this is addressed through T&Cs and other cardholder communications. If the update is a pricing change, SCA is required if the amount differs by more than a cardholder reasonably expects.[7]
	Establish agreement for ongoing/future payments (e.g. subscription, no show)	SCA is required in most cases when the initial mandate is set up via a remote electronic channel.
Merchant Initiated	Executes payment (e.g. subscriptions, no show)	In Visa's view, out of scope. SCA is required in most cases when the initial mandate set up via a remote electronic channel but is not necessary for subsequent payments initiated by the merchant.
	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 subsequent events can be linked to the initially authenticated or exempted authorization.

---

[7] What is within the reasonable expectations will depend on the circumstances and the transparency to the cardholder. If not within the reasonable expectations of the cardholder, SCA would be required.

VISA

4.2.3.2.2   Implementing SCA in common non-payment scenarios

Table 18: Summary of common non-payment scenarios.

Action	Use Cases	Recommendation for SCA Requirement
Loading of Credentials	Adding a Credential-on-File or provisioning of a token	Could be required when the cardholder is adding or provisioning a card.
	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 in most cases 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.

VISA

4.2.3.3 Visa authentication, authorization and clearing principles for implementing SCA

Table 19: 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; 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 of "1A" (SCA required). The CAVV must always be submitted with the associated ECI value it has received with it. As a matter of the Visa Rules 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), where no Acquirer SCA exemption has been applied. When an exemption has been applied, the ECI value is 07 (indicating SCA was not performed or attempted) and fraud liability protection under the Visa Rules is not applicable.
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.	This is a feature available in 3-D Secure version 2.1 and above which 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 complex payment use cases by for example: • Allowing an authorized entity in a Multi-Party Commerce scenario to request a CAVV on behalf of a merchant. • Allowing merchant to obtain a new CAVV in case of split or delayed shipment when only 1 or more item is not ready for shipment till a much 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 Trans 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.)

VISA

Principle	Rationale
4. **Token Authentication Verification Value based on Cloud Token Framework (CTF TAVV) can be used by qualifying token requestors for cardholder authentication**	In some cases, qualifying token requestors can use the CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance. CTF TAVVs used in this way do not currently qualify the merchant for liability protection under the Visa Rules. More information will be provided by the Visa Token Service as these new options become available.
5. **Token Transactions require a TAVV unless they are being submitted as MITs**	Visa requires a TAVV (existing or new CTF TAVV) to be present in all Token transactions unless the transaction is identified as a Merchant Initiated Transaction.
Visa Authorization Principles	
6. **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.
7. **An MIT can only occur after an initial CIT has been performed to establish a customer agreement**	Where the initial mandate is set up through a remote electronic channel, SCA is required in most cases but should not be necessary for subsequent payments initiated by the merchant.
8. **MITs must be properly indicated as MITs to ensure they are treated as out of scope of SCA**	If a merchant initiates an electronic transaction based on a prior agreement with a customer, the transaction is out of scope of SCA as long as Issuers can indeed recognise it as an MIT. In the Visa system, this is done by adding the MIT indicators to any MIT
9. **Merchants need to store the Transaction ID of the CIT that established the agreement for future MITs.**	An MIT must reference the original CIT used to establish the agreement by including the Transaction ID of that CIT in the authorization message. Therefore, merchants who might perform MITs need to store the Transaction ID of their associated CIT until no further MITs are required and any agreement with the customer is complete.
10. **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 # 27797). In addition, merchants should only request authorization when they have confirmed that the goods are available and ready to be shipped. This minimises the impact to the customer's open to buy and ensures that the CAVV is not used ineffectually.

Principle	Rationale
11. Authorizations are valid for a maximum of up to 7 days	If an authorization cannot be fully cleared after 7 calendar days[8] 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.
12. 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 the authorization for more than 90 days as if the transaction is performed with a token, it will no longer be valid. If a merchant cannot avoid being in a position of a greater than 90 day delay, they will need a touch point with the customer to perform a new account verification 90 days and the Transaction ID of this account verification must be stored for usage in the delayed authorization. If a token is used, this new account verification will require a 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 those 90 days, albeit, without fraud liability protection. For delays over 90 days: - A merchant wishing to still include a CAVV for fraud liability protection must first use 3RI (if available) to obtain a new CAVV (with ECI 05 or 06) for the relevant amount. - 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 or 06) that is older than 90 days, but Issuers will still have dispute rights. The benefit for the merchant is that including a valid CAVV should prevent the Issuer declining with a response code 1A (SCA required)*. - 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. *A merchant should not submit a CAVV older than one year as the CAVV will fail validation.

---

[8] 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.

VISA

Principle	Rationale

13. **When an authorization must be delayed until after 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 knows that the cardholder is not available for authentication**
	If an authorization cannot be performed at checkout and must be delayed, the merchant must perform an account verification immediately (following any required authentication) and store the Transaction ID of this account verification transaction. Later, when the shipment is ready to be made, the merchant must submit a delayed authorization with message reason code (MRC) 3903 and the transaction ID of the account verification (original CIT). If authentication was performed via 3-D Secure and a CAVV was obtained, the merchant process differs depending on whether the CAVV was included in the original CIT or not.
	
	CAVV <u>used</u> in original CIT: If the CAVV was submitted during the account verification (original CIT), then the delayed authorization 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).
	
	CAVV <u>not used</u> in original CIT: If the CAVV was not submitted during account verification (original CIT), then the CAVV must be stored for later submission in the delayed authorization. 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), since the original CIT does not contain a CAVV that can be referenced; otherwise, there is a risk that the Issuer might decline (i.e. response code 1A – SCA required) the transaction for not having a valid CAVV.
	
	Important note: This principle ensures a consistent approach in handling payment scenarios with delayed authorization, <u>that works for both PAN and Token</u>[9].

14. **Transaction amounts can vary between authentication, authorization and clearing within "reasonable" customer expectations**	• **The final transaction amount authorized can vary from the amount authenticated as long as it remains within the customer's reasonable expectations.** The amount of the authorization should not be higher than the amount the cardholder can reasonably expect based on the circumstances and amount presented to the cardholder at time of authentication.

---

[9] If the Merchant / Acquirer know with **absolute** certainty that the payment credential is a PAN, then they could implement an alternative approach, whereby they do not need to submit an account verification immediately, but rather retain the CAVV to include it in a standard authorization when the goods are ready to be shipped (i.e. without MRC 3903 or an initial Transaction ID).

VISA

Principle	Rationale

	<u>**As an outside limit,**</u> Visa requires that the authorized amount must never exceed the amount authenticated by more than 15%. Any authorization amount that is greater than this is not subject to Visa's 3-D Secure 2.0 Program chargeback protection and may be charged back by the Issuer. (Refer to Merchant/Acquirer Implementation Guide for 3-D Secure 2.0, Section 2.7.1 for more information).
	
	It is best practice that when the final transaction amount is not known in advance, that a merchant / Acquirer should authenticate the customer for the estimated maximum transaction amount. In this situation, to avoid abandonment due to confusion, it is essential to clearly communicate to the customer before the authentication step that:
	
	    o They are authenticated for a maximum amount
	    o They will only be charged for what they purchase (which may be lower than the authenticated amount)
	    o No charges will appear on their card statement until the order is finalised
	
	• It is also considered best practice that if the previously communicated maximum amount is exceeded, then customer re-authentication for a new amount should be sought immediately.
	
	• **The final amount cleared can vary from the amount authorized as long as it remains within the customer's reasonable expectations.** The amount cleared should not be higher than the amount the cardholder can reasonably expect based on the circumstances and amount presented to the cardholder at time of authentication.
	
	    o **As an outside limit,** Visa requires that the cleared amount must never exceed the amount authorized by more than 15%. The exact percentage varies for some MCCs. For more information please refer to Visa Rule ID# 0025596.
	
	• **The final transaction amount cleared can be lower than the amount authorized.** Visa rules allow for the cleared amount to be lower than the amount authenticated and authorized. If the authentication provides the merchant with fraud liability protection, the protection still applies despite the variance.
	
	• **The authenticated amount, the authorized amount and the cleared amount can be different.** There are many legitimate reasons why the amount authenticated, amount authorized and amount cleared could be

VISA

Principle	Rationale
	different. This is acceptable provided the variance is within the customer's reasonable expectations and the other limits defined above. Where the final amount is not known when the cardholder authenticates the transaction, the authentication code should be specific to the amount the cardholder agreed to be blocked (e.g. the 'maximum amount').
15. Issuers should avoid responding to the authorization request for an MIT with a response code of 1A (SCA required).	Issuers should avoid asking for authentication in response to authorization transactions identified as MITs, as the cardholder is not available for authentication during those transactions. Therefore, it is essential that merchants use the MIT framework to enable Issuers to identify transactions where the cardholder is not available and for the Issuer to be able to identify transactions flagged as MITs.
16. Grandfathering can be applied to MITs performed based on agreements made prior to 14th September 2019	A merchant with an existing agreement with a customer established prior to 14th September 2019 does not need to establish a new agreement with their customer with SCA. Instead, all MIT authorizations performed after the 14th September 2019 can reference as a proxy to the "initial" CIT, the transaction ID of any previous related transaction processed before the 14th September 2019 (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 14th September 2019. 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 14th September 2019.
17. When setting up an agreement to process future MITs, only authenticate and authorize for amount needed on the day of the agreement	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. For example: • For subscriptions (recurring and unscheduled credential on file (UCOF) transactions in the Visa system): o If first monthly payment is 5 Euros, authenticate and authorize for 5 Euros

VISA

Principle	Rationale
	o If free trial period, authenticate and authorize for zero amount o If first payment is a reduced promotion amount of 2 Euros, rising to 5 Euros after 3 months, authenticate and authorize for 2 Euros. • For installments: o If first installment is not due at time of agreement, authenticate and authorize for zero amount, otherwise use the amount of the first installment. • For other **Industry Specific** MITs such as "No Show", Incremental and Delayed Charges, also only authenticate and authorize for the amount due that day. For example, if booking a hotel with no deposit required, use zero value.
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[10]. Because a CAVV is not included in clearing, submitting multiple clearing records to fulfil a single authorization does not impact merchant fraud liability.

---

[10] For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

VISA

4.2.4 Who can apply exemptions?

Under the regulation, the application of exemptions is restricted to regulated PSPs (in the case of card payments Issuers and Acquirers) however there is scope for merchants to work with their Acquirers to set and execute exemption policies.

The table below summarises which PSP is able to apply which relevant exemption for remote card transactions according to the regulation.

Table 20: Summary of who may apply an exemption[11]

Exemption	Issuer	Acquirer
Trusted beneficiaries	Yes	No[1]
Transaction Risk Analysis (TRA)	Yes	Yes[2]
Low Value Transactions	Yes	Yes[2,3]
Secure corporate payment processes & protocols	Yes	N/A
Recurring Transactions[4]	Yes	Yes

Notes:

1) Under the PSD2 regulation, an Acquirer may not apply the trusted beneficiaries exemption, however 3DS 2.2 and the Visa Trusted Listing solution allow for:

   o A cardholder to enrol a merchant in their trusted beneficiaries list while completing an SCA authenticated transaction; and

   o A merchant to be advised 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.

2) 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.

3) 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.

4) Visa recommends that recurring card transactions are treated as out of scope MITs in preference to applying the recurring transactions exemption.

---

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

4.2.5 Options for merchants and Acquirers regarding the application of exemptions

If a payment transaction is in scope of PSD2 (and SCA), then the merchant / Acquirer must determine whether an SCA exemption can be exercised or not.

A merchant / Acquirer can exercise an exemption through one of the following options:

- **Exemption via authentication:** The merchant can exercise an exemption via a 3DS message first, before performing an authorization request. This is done by setting the relevant indicators in the 3DS message and in the subsequent authorization. The advantage of this approach is that if the exemption is rejected by the Issuer, the cardholder is still present to complete any required step-up, even if authorization will be delayed. Merchants should be aware that if taking this approach, the exemptions exercised during authentication must be re-stated in the authorization message along with the CAVV and ECI value received at the authentication step.

- **Exemption directly via authorization:** The merchant can go directly to authorization, flagging the exemption used in Field 34. The advantage of this approach is that the authentication step can be skipped altogether, if the Issuer accepts the exemption. Furthermore, there are specific types of exemptions that are only available in the authorization (but not in the authentication). However, merchants considering this option should be aware that the Issuer can decline the exemption and request an authentication. In the case where authorization is delayed and the Issuer rejects the exemption, the cardholder will no longer be available to perform authentication. Acquirers/merchant should review market specific requirements before adopting this exemption option, since some markets may require exemptions to be raised via an authentication message first.

Otherwise, if the merchant / Acquirer does not exercise an exemption, then:

- **No exemption exercised:** The merchant can perform authentication and authorization without populating any exemption indicators in 3DS and in authorization Field 34.

4.3 Step by step guide to managing the authentication flow

Strategies to optimise the application of SCA and exemptions in a PSD2 environment will be driven by decisions that merchants, Acquirers and Issuers need to take at key points in the transaction process flow.

This section summarises these flows and decision points from the perspective of:

1. The merchant/Acquirer

2. The Issuer

At each decision point, is a description of the options available to the merchant/Acquirer and the factors that should be taken into account when deciding how to treat the transaction from the perspective of applying SCA or an exemption. This is done for:

1) A Standard Customer Initiated E-Commerce Transaction

2) Setting up an MIT agreement

3) A Merchant Initiated Transaction

Detailed differences and options that arise with other common and complex use cases are covered in section5. More detailed practical guidance on the application of exemptions is given in section 4.5.

Note, these flows are based on the example where the merchant uses 3DS for authentication. If an alternative authentication method is used, for example under the Delegated Authentication Programme) then variations may apply. More information will be made available during 2019.

4.3.1   Merchants/Acquirer Decision Flow

Figure 12: The key decision points in the merchant/Acquirer flow
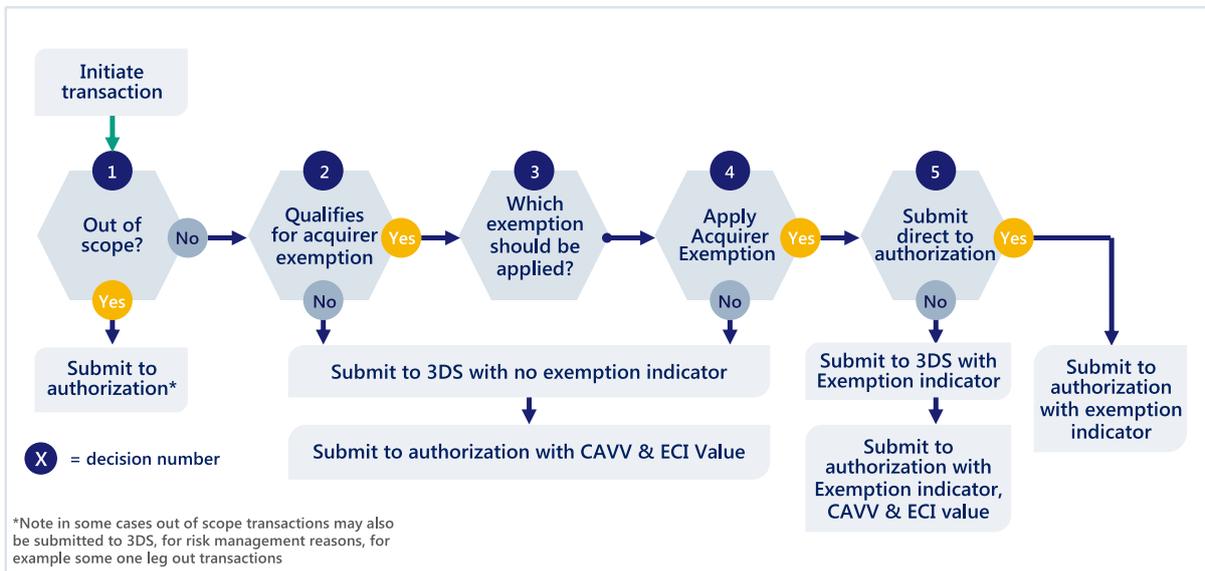
Figure 13: Merchant/Acquirer SCA/exemption simplified process flows and decision points

| Decision 1 | Is the transaction out of scope of SCA? |

Summary
Merchants and their acquirers assess whether a transaction is in or out of scope of SCA

| Out of scope reason 1 | Merchant Initiated Transaction |

How does a transaction qualify?
The cardholder has previously entered into an agreement with the merchant that allows the merchant to take payments without direct intervention of the cardholder.

Merchant / acquirer questions & actions

Is this transaction the first in the series?

No →

Has the cardholder or the merchant made any changes to the pre-existing agreement since the last in the series?

Yes →

The transaction may require SCA. Refer to section 5.10 for detailed guidance

Yes ↓

The transaction is likely to be in scope and require SCA. Refer to section 5.9 for detailed guidance

No ↓

In Visa's view, the transaction is out of scope of SCA. Submit to authorization with initial transaction ID using the MIT framework (See section 3.7 for more guidance)

| Out of scope reason 2 | MOTO |

How does a transaction qualify?
The Purchase is initiated in a Card-Absent Environment where a cardholder orders goods or services from a Merchant via a paper-based payment transaction, mail order or telephone order

▶ **Merchant / acquirer questions & actions**
Submit to authorization ensuring it is identified as a MOTO transaction

| Out of scope reason 3 | Anonymous payment |

How does a transaction qualify?
The payment credential is not directly linked to an individual consumer (for example an anonymous prepaid gift card)

*Note: In both cases, upon receipt of the transaction the issuer should recognise the transaction as out of scope and not request SCA.

▶ **Merchant / acquirer questions & actions**
Does the merchant have access to the BIN table and is it able to recognise the transaction as anonymous?*
Yes - Send the transaction direct to authorization. No exemption flags are needed
No – Move to decision 2

| Out of scope reason 4 | One leg out |

How does a transaction qualify?
The payment credential is issued outside the EEA

▶ TBC

| All other transactions | |

Assess whether an exemption may be applied or requested & submit to authorization with appropriate field values or to authentication via 3DS

VISA

Decision 2	Does the transaction qualify for an acquirer exemption?

Summary

Assessment of whether there is an option for the acquirer to apply an exemption

Under the PSD2 regulation, an acquirer may apply the following exemptions to remote electronic card transactions:

Transaction Risk Analysis (TRA)   Low-value transactions   Recurring transactions

Under the PSD2 regulation an acquirer may not apply the trusted beneficiaries exemption, however 3DS 2.2 and the Visa Trusted Listing solution allow for:

- A cardholder to enrol a merchant in their trusted beneficiaries list while completing an SCA authenticated transaction *and*
- A merchant to be advised 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

Guidance on assessing the applicability of each transaction type is given below.

Exemption 1	Transaction Risk Analysis (TRA) Exemption

How does a transaction qualify?
- The value of the transaction must be less than €500, *and:*
- The acquirer's fraud rate must be within the reference fraud rate for the relevant transaction value band, *and:*
- The acquirer must be prepared to apply the exemption on behalf of the merchant, *and:*
- Transaction Risk Analysis must have been undertaken by the acquirer or by the merchant on behalf of the acquirer; *and:*
- The transaction must be assessed to be at low risk of fraud

Merchant / acquirer questions & actions
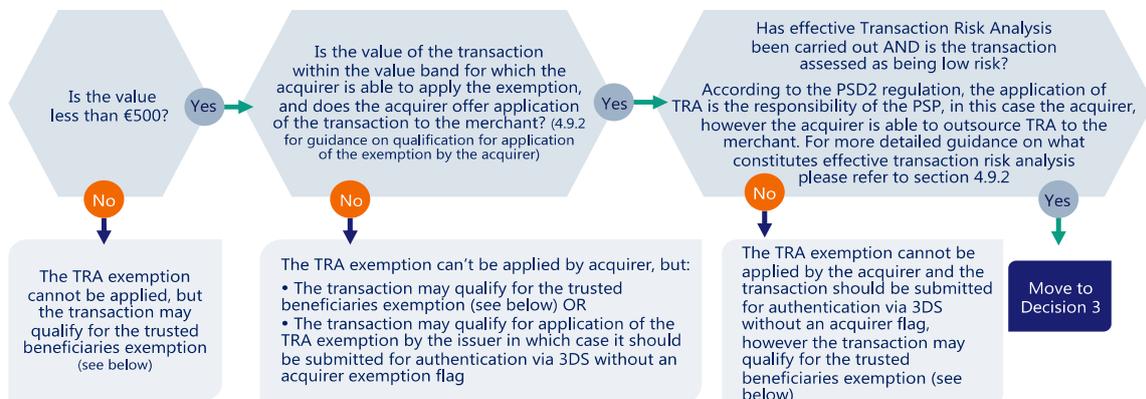
Exemption 2	Low value exemption

How does a transaction qualify?
- The value of the transaction must be less than €30, *and:*
- The number of number of consecutive transactions since the last application of SCA must not exceed 5, or the cumulative value of consecutive transactions since the last application of SCA must not exceed €100

Merchant/Acquirer application not recommended
While the PSD2 regulation allows for the acquirer to apply this exemption, in reality only the issuer will know whether the transaction qualifies under the velocity limits so it is not recommended that the acquirer applies this exemption.

Exemption 3	Recurring Transactions Exemption

How does a transaction qualify?
- The transaction is one of a recurring series of transactions, *and:*
- SCA has been applied when the series was set up, *and:*
- All the payments in the series are of the same amount and made to the same payee.

Merchant/Acquirer application to be considered as an alternative to flagging as an MIT

Recurring payments must be of the same value to qualify so using this exemption may be problematic if the merchant plans to change prices or vary the amount at a future date. For situations where this is likely, flagging transactions as an MIT may be a better option.

Exemption 4	Trusted Beneficiaries Exemption

How does a transaction qualify?
- Merchant is qualified for application of the trusted beneficiary exemption by the issuer, *and:*
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the issuer (existing trusted beneficiary)

Step a) Is the merchant approved by the issuer to qualify for the trusted beneficiaries exemption?

If yes, move to step b below.

If no, During the 3DS enrolment, Visa will notify the merchant whether or not the cardholder's whitelisting request was successfully accepted by the issuer. If the enrolment was not successful, then the trusted beneficiaries exemption cannot be applied. Submit the transaction for authentication via 3DS without an exemption flag

Step b) Do the merchant's fraud rates meet the eligibility criteria to participate in Visa's Trusted Listing solution?

If yes, move to decision 3.

If no, Trusted beneficiaries exemption cannot be applied. Submit the transaction for authentication via 3DS without an exemption flag

VISA

Summary

Assuming the transaction could qualify for either the trusted listing or TRA exemption, which exemption should take precedence?

Note: only one exemption should be applied

Decision & Actions

Has the cardholder previously enrolled the merchant on their trusted beneficiaries list?

No →

Would the merchant like the cardholder to add them to their list of trusted beneficiaries?*

Yes →

Merchant should request through 3DS or VTS to add the cardholder's card to the trusted list

Yes ↓

Apply Trusted Beneficiary Exemption as the preference & move to decision 4

No ↓

Apply the TRA Exemption

Note, if the merchant does not want a customer to be able to enrol it on their trusted merchant list, it can avoid showing any messaging or option to the cardholder to allow them to enrol.

*The merchant should take into account that it will not benefit from liability protection under the Visa Rules for future transactions for which the trusted beneficiary exemption is applied

This decision should be based upon factors including:

- Whether the issuer supports trusted listing
- The risk profile of the customer/current transaction determined through TRA and whether, according to the merchant's risk policy, the customer is considered a low enough risk to allow future transactions of any value to be processed without the application of SCA.
- Whether the cardholder is expected to make future purchases
- Whether the cardholder has previously been offered the opportunity to add the merchant to their list but has declined
- Whether the merchant has communicated the concept of trusted beneficiaries effectively to its customers and can be expected to understand and accept listing the merchant
- Whether the merchant is prepared to accept the application of SCA on this transaction in exchange for potential future transactions not being subject to SCA

VISA

Summary

Should an allowable exemption be applied by the acquirer or requested by the merchant?

This decision will be based on the merchant/acquirer's risk strategy and their view on the relative balance between the following factors:

1. Liability protection – which is not available if the exemption is applied by the acquirer in the case of TRA or at all in the case of trusted beneficiaries
2. The probability of the issuer still applying SCA when the acquirer has applied or requested an exemption

Note: only one exemption may be requested or applied per transaction

Transaction Risk Analysis

Is the merchant acquirer prepared to accept liability for fraud?

Based upon the TRA assessment and the merchant/acquirer's risk policy, is the fraud risk score of the transaction low enough for:
- The merchant/acquirer to accept financial liability in the case that the transaction is fraudulent?
- The acquirer to accept that any fraud on the transaction will be included in its fraud count for the purposes of calculating qualification to apply the TRA exemption?

Yes

No → Submit the transaction for authentication via 3DS without an exemption flag

Does the merchant consider the probability of the transaction being approved without the application of SCA is higher if the acquirer applies the TRA exemption?

This decision will need to be based on experience of the response of individual issuers to transactions submitted by the merchant. It should be noted that the issuer retains the right to apply or require SCA even if the acquirer applies a TRA exemption on behalf of the merchant

Yes

No → Submit the transaction for authentication via 3DS without an exemption flag

Yes → Move to decision 5

Trusted Beneficiary: Merchant already enrolled on the card holder's list

Note, the default position is that if the cardholder is enrolled, the issuer will apply the trusted beneficiaries exemption unless:
- The acquirer assesses there is risk associated with the transaction and submits it via 3DS for authentication, *or*
- The issuer assesses there is risk associated with the transaction and applies SCA

Is there any risk associated with this transaction that would prompt the Merchant not to want the trusted beneficiaries exemption to be applied?

If the merchant may undertake TRA and assess that there is a high risk of fraud, for example due to a change in device type, location, purchase type, purchase amount or delivery address

Yes → Submit the transaction for authentication via 3DS

No → Request application of the trusted beneficiaries exemption. The merchant and its acquirer will submit an authorization request for the cardholder's card and include the Trusted Beneficiary flag in the authorization message Field 34.

VISA

Decision 5	Submit the transaction straight to authorization?

Summary

A merchant submitting a transaction with an acquirer exemption applied has the option to either submit via 3DS or direct to authorization with appropriate flags set (see section 3.2.2 for details)

The decision will be based on the merchant's assessment of the balance between the following factors:

- The merchant's own level of confidence in their assessment of the risk of the transaction
- A balanced evaluation of the risk that any challenge may present to the cardholder abandoning the transaction. Whilst this should not be an issue with 3DS 2.0, any friction in the purchase always carries a risk no matter how small that something might disrupt the purchase
- In consideration of the above, a merchant must also evaluate the potential benefit of liability protection that comes with a fully authenticated 3DS transaction
- Their confidence that the issuer will accept their assessment that the transaction is low risk and will not require SCA to be applied
- The cost of submission via 3DS vs. direct to authorization

It should be noted that if a transaction is submitted straight to authorization with an acquirer TRA exemption flag, the issuer has the right to request that it is resubmitted for authentication via 3DS potentially adding latency and cost to transaction authentication and authorization process.

Transaction Risk Analysis

Is the merchant confident that the issuer will accept their assessment that the transaction is low risk and will not require authentication?

The merchant should take the following factors into account when taking this decision:
- The effectiveness of their own risk assessment systems in predicting fraud in comparison to the full risk based assessment that an issuer will undertake with 3DS 2.0
- The amount of transaction data provided to the issuer. Merchants should be aware that in submitting transactions direct to authorization, the issuer may have poorer transaction data on which to make its risk assessment and may be more likely to require resubmission via 3DS.
- Any known local market preferences held by issuers for transactions to pass via 3DS

Yes → Submit direct to authorization with a 9F7D flag in Field 34 (see section 3.2.2) for details

No → Submit the transaction for authentication via 3DS without an exemption flag (Value 05 in the 3DS Requestor Challenge Indicator field – see Appendix 2 for more details)

Trusted Beneficiary

Is the merchant confident that there is no suspicious behaviour from the cardholder's account?

For example, a cardholder may have successfully enrolled in Trusted Listing. However, their account may have been compromised at a later point. The merchant should be confident that the cardholder, not a fraudster, is making the transaction.

Yes → Submit direct to authorization with a Trusted Listing flag in Field 34 (see section 3.2.2) for details

No → Submit the transaction for authentication via 3DS without an exemption flag (Value 05 in the 3DS Requestor Challenge Indicator field – see Appendix 2 for more details)

VISA

4.3.1.1 Additional Considerations for merchants and Acquirers considering sending transactions straight to authorization

If a merchant/Acquirer sends a transaction straight to authorization and the Issuer's risk assessment determines it high risk, it may issue an SCA required decline (1A) requesting that the transaction is resubmitted for the application of SCA, for example via 3DS. Merchants and Acquirers should 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 3DS 2.0 and they may therefore be more likely to request resubmission via 3DS 2.0.

- The issuing of an SCA required decline (1A) and resubmission via 3DS 2.0 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 3DS, the cardholder may no longer be available to complete authentication resulting in a decline.

Merchants and Acquirers should therefore exercise caution when submitting transactions straight to authorization.

Acquirers must include an exemption flag in the authorization request if they are submitting transactions under an Acquirer exemption. Transactions without exemption flags or without having had SCA applied are likely to receive an SCA required decline (1A) from the Issuer, as the Issuer will not know that the exemption is being requested and thus will not have an audit trail in the data.

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

4.3.1.2 Acquirer Policy Decisions

Acquirers will need to develop policies on risk assessing transactions that are sent straight to authorization with or without exemption fields set. These should aim to minimise the unnecessary application of SCA required declines (1A) while staying in line with the Issuers risk management policy.

Key Point

Acquirers must also ensure they pass any SCA required declines (1A) 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

Acquirers should develop policies on the risk profile of transactions that may be sent straight to authorization with exemption flags 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 required declines (1A).

VISA

4.3.2   Issuers

Issuers may receive transactions either direct to authorization or via 3DS. The Key Decision points in the Issuer flow for both sets of transactions is summarised below:

Figure 14: Key Issuer decision points

Version 1.1
11 th March 2019
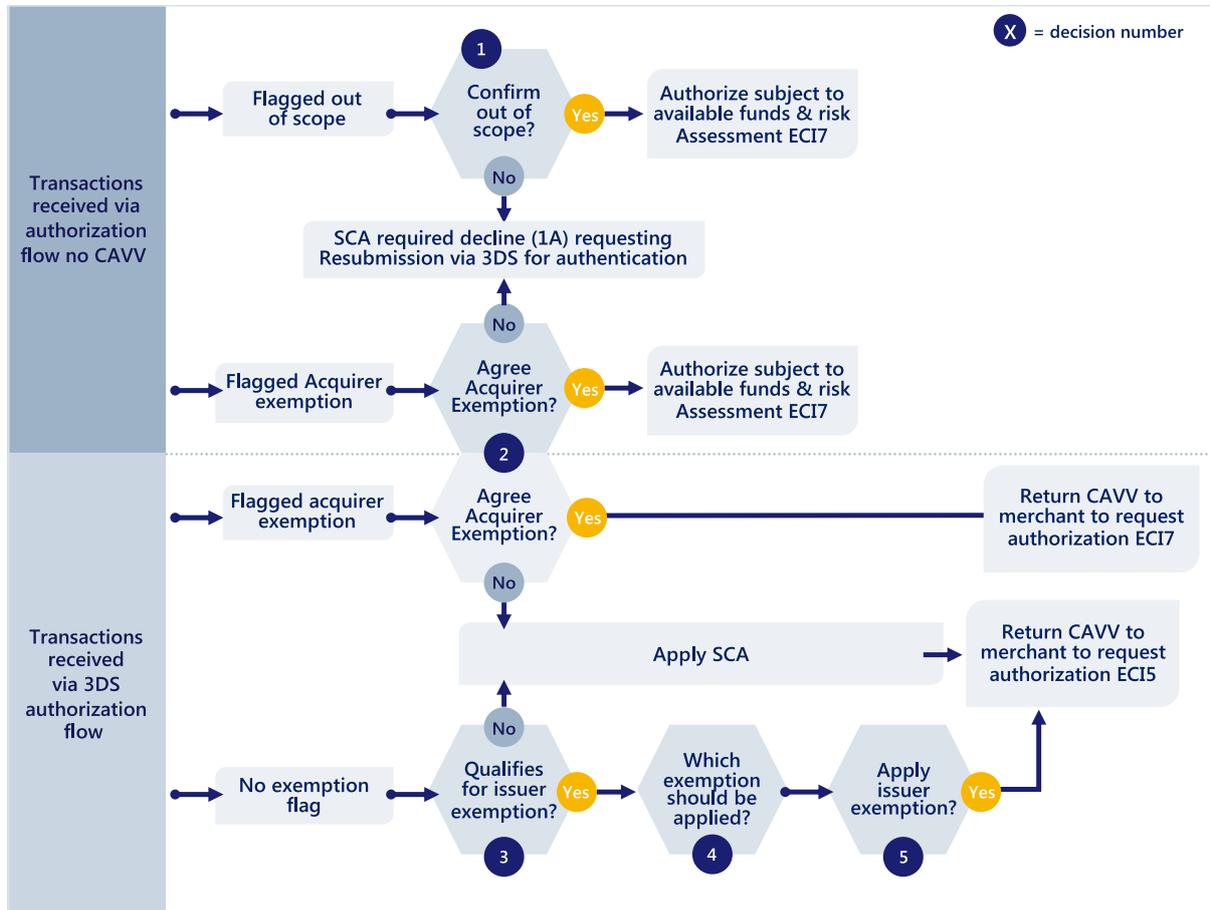
Figure 15: Issuer key decision flow

Decision 1	Confirm the Transaction is out of scope of SCA

Summary
Issuer assess whether a transaction received with an out of scope indicator is out of scope of SCA

Out of scope reason 1	Merchant Initiated Transaction

How does a transaction qualify?
The transaction is received with an appropriate indicator

Issuer actions
If the correct MIT indicator is present, the transaction is an MIT and in Visa's view, SCA is not required (subject to the interpretation of your local competent authority). You may optionally wish to check the Tran ID to ensure it refers to a valid CIT, however be aware that there are valid reasons why the initial CIT may not have been authenticated.

Authorize, subject to normal authorization assessment criteria (availability of funds etc).

The issuer should avoid issuing an SCA required decline (1A) due to lack of authentication

Out of scope reason 2	MOTO

How does a transaction qualify?
The transaction is received with an appropriate indicator

Issuer actions
Authorize, subject to normal authorization assessment criteria (availability of funds etc).

Do not decline or issue an SCA required decline (1A) due to lack of authentication

Out of scope reason 3	Anonymous payment

How does a transaction qualify?
The payment credential is not directly linked to an individual consumer (for example an anonymous prepaid gift card)

Issuer actions
When you receive an authorization for a card from an anonymous card BIN, authorize, subject to normal authorization assessment criteria (availability of funds etc).

Do not decline or issue an SCA required decline (1A) due to lack of authentication

Out of scope reason 4	One Leg Out

How does a transaction qualify?
The acquirer is outside the EEA.

Issuer actions
Authorize, subject to normal authorization assessment criteria (availability of funds etc).

Do not decline or issue an SCA required decline (1A) due to lack of authentication

Issuers should continue to use their ACS to authenticate whenever the merchant has initiated a 3DS authentication request (subject to applicable exemptions, or application of SCA on a best efforts basis) or authorize accordingly.

VISA

| Decision 2 | Does the issuer agree with the acquirer exemption? |

Summary

Under the PSD2 regulation, an acquirer may apply the following exemptions to remote electronic card transactions:

| Transaction Risk Analysis (TRA) | Low-value transactions | Recurring transactions |

Under the PSD2 regulation an acquirer may not apply the trusted beneficiaries exemption, however 3DS 2.2 and the Visa Trusted Listing solution allow for:

• A cardholder to enrol a merchant in their trusted beneficiaries list while completing an SCA authenticated transaction and

• A merchant to be advised 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

Visa recommends that in practice acquirers should not apply the low value transaction exemption as they do not have visibility of the velocity limits, or the Recurring transactions exemption as recurring card transactions should be treated as MITs and out of scope.

The issuer has the right to apply SCA if it assesses a transaction to be high risk even if the acquirer has applied or requested an exemption.

Issuer may receive transactions flagged with an acquirer exemption through either the authorization or authentication flow. The acquirer assumes liability unless the issuer overrides the application of the exemption and applies SCA.

| Exemption 1 | Transaction Risk Analysis (TRA) Exemption |

How does a transaction qualify?
• The value of the transaction must be less than €500, and:
• The acquirer's fraud rate must be within the reference fraud rate for the relevant transaction value band, and:
• The acquirer must be prepared to apply the exemption on behalf of the merchant, and:
• Transaction Risk Analysis must have been undertaken by the acquirer or by the merchant on behalf of the acquirer; and:
• The transaction must be assessed to be at low risk of fraud; and:
• The merchant/acquirer submits the transaction straight to authorization or via 3DS 2.0 with an appropriate exemption indicator (requires support of version 2.2 of the 3DS spec)

Issuer options and actions:

a)   Allow the exemption

The issuer may choose to do this on the basis that:
• RBA has been applied and the issuer considers the transaction to be low risk
• The acquirer is within its TRA permitted fraud rate
• The merchant/acquirer will assume liability for fraud
• The acquirer will assume liability for fraud count in the context of qualification to apply the exemption against reference fraud rates

Note: some local competent authorities may require that any fraud is taken into account in the fraud counts of both acquirer and issuer regardless of which party applies the exemption

| Transaction received via Authorization Flow | Authorize, subject to normal authorization assessment criteria (availability of funds etc). |
| Transaction received via 3DS Authentication flow | Return the authentication result/CAVV to the merchant/acquirer without applying SCA |

b) Require the application of SCA

The issuer may choose to do this on the basis that:
• RBA has been applied and the issuer considers the transaction to be high risk
• The issuer has received insufficient transaction data to confidently assess the risk of the transaction

| Transaction received via Authorization Flow | Issue an SCA required decline (1A) message to the acquirer requesting resubmission with authentication |
| Transaction received via 3DS Authentication flow | Apply an SCA challenge |

| Exemption 2 | Trusted beneficiaries Exemption |

How does a transaction qualify?
•   Merchant is qualified for application of the trusted beneficiary exemption by the issuer, *and*
•   The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the issuer (existing trusted beneficiary)

Issuer options and actions
The issuer may accept the exemption if:
•   The issuer considers the transaction to be low risk
•   There is no suspicious activity on this card

| Yes | Apply Trusted Beneficiary exemption |
| No | Send an SCA required decline (1A) message to the acquirer requesting resubmission for authentication, for example via 3DS |

VISA

Decision 3	Does the transaction qualify for an issuer exemption?

Summary

Assessment of whether there is an option for the issuer to apply an exemption

Where the issuer has received a transaction via 3DS without an acquirer exemption indicator, the issuer should assess whether the transaction qualifies for an exemption and should seek to apply the most appropriate qualifying exemption to minimise the impact of authentication on the customer experience.

Under the PSD2 regulation, an issuer may apply the following exemptions to remote electronic card transactions:

Transaction Risk Analysis (TRA)　　Low-value transactions　　Recurring transactions　　Trusted beneficiaries

Secure corporate payments

Note: Guidance on the application of the Secure Corporate Payments Exemption is under development and will be included in a later version of the guide.

Exemption 1	Transaction Risk Analysis (TRA)

How does a transaction qualify?

- The value of the transaction must be less than €500, and:
- The issuer's fraud rate must be within the reference fraud rate for the relevant transaction value band, and:
- Transaction Risk Analysis must have been undertaken by the issuer, and:
- The transaction must be assessed to be at low risk of fraud

Merchant / acquirer questions & actions

Is the value less than €500?
(see section 4.9.2 for guidance on conversion to other currencies)　→ Yes →

Is the value of the transaction within the value band for which the issuer is able to apply the exemption?　→ Yes →

Has effective Transaction Risk Analysis been carried out AND is the transaction assessed as being low risk? For more detailed guidance on what constitutes effective transaction risk analysis please refer to section 4.9.2

No → The TRA exemption cannot be applied, but the transaction may qualify for the trusted beneficiaries exemption (see below)

No → The transaction does not qualify for the TRA & SCA should be applied, unless the transaction qualifies for one of the other exemptions described below

No →

Exemption 2	Low Value

How does a transaction qualify?
- The value of the transaction must be less than €30, and:
- The number of number of consecutive transactions since the last application of SCA must not exceed 5, or the cumulative value of consecutive transactions since the last application of SCA must not exceed €100

Issuer options and actions
- So long as the issuer determines that the qualifying criteria apply, the issuer may apply the low value transaction exemption.
- The issuer should still however apply RBA as required by the PSD2 regulation and should apply SCA if the transaction is perceived to be at risk of fraud.
- The issuer should consider that it will be liable for any fraud and will also be have to take account of the value of that fraud in its fraud count in determining whether it qualifies for application of the TRA exemption

Exemption 3	Recurring transactions

How does a transaction qualify?
- The transaction is one of a recurring series of transactions, *and:*
- SCA has been applied when the series was set up, and:
- All the payments in the series are of the same amount and made to the same payee

Issuer options and actions
While the PSD2 regulation allows for the issuer to apply this exemption for card transactions, Visa considers that this exemption is really only applicable to push payments such as standing orders and that recurring card transactions should be treated as MITs and out of scope.

Exemption 4	Trusted beneficiaries

How does a transaction qualify?
- The merchant is qualified for application of the trusted beneficiary exemption by the issuer, *and*
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the issuer (existing trusted beneficiary)

Issuer options and actions
So long as the issuer determines that the qualifying criteria apply, the issuer may apply the Trusted Beneficiary exemption.

VISA

| Decision 4 | Which applicable exemption should take priority? |

Summary

Assuming the transaction could qualify for either the trusted beneficiaries, or low value, or TRA exemption, which exemption should take precedence?

Note only one exemption should be applied

The decision on which exemption should take precedence when the transaction qualifies for more than one will depend upon factors including:

- Liability protection
- The benefits of the additional data shared under a TRA exemption applied through 3DS

| Decision 5 | Apply an Issuer Exemption? |

Summary

Summary: Should an allowable exemption be applied by the issuer?

So long as a transaction qualifies for an exemption and the issuer does not asses that there is an unacceptable risk of fraud, the issuer should apply the exemption in order to minimise cardholder friction and abandonment.

Note, only one exemption may be applied per transaction

4.3.2.1 Issuer Policy Decisions

Issuers need to develop policies on risk assessing transactions that are sent straight to authorization with or without exemption fields set. These should aim to minimise the unnecessary application of SCA required declines (1A) while staying in line with the Issuers risk management policy.

4.4 Liability for fraud-related chargeback

The table below summarises how liabilities for fraud-related chargeback apply between the Issuer and the Acquirer under the Visa Rules depending on which PSP applies an exemption and whether the transaction is submitted via 3DS[12]. Exemptions applied by the Acquirer must have an exemption flag in F34 in the authorization request to be considered valid by the Issuer.

Table 21: Use of 3DS and Application of Liabilities for Common Transaction Use Cases

SCA Provision		PSP Applying Exemption	Submitted Via 3DS	Challenge Applied	Fraud Liability
Exemption	Transaction Risk Analysis (TRA)	Issuer	Yes	No	Issuer ECI 5
		Acquirer	Yes	No	Acquirer ECI 7
		Acquirer	Yes	Yes	Issuer ECI 5
		Acquirer	No	N/A	Acquirer ECI 7
	Trusted Beneficiaries	Issuer	Yes	No	Acquirer ECI 7
	Low Value	Issuer	Yes	No	Issuer ECI 5

---

[12] PSD2 sets out its own principles of liability as a matter of regulation, but does not preclude PSPs from making additional arrangements.

VISA

		Acquirer	No	N/A	Acquirer ECI 7
	Corporate processes and protocols	Issuer	Yes	No	Issuer ECI 5
		Issuer	No	N/A	Acquirer ECI 7
		Acquirer	No	N/A	Acquirer ECI 7
Out of Scope	Merchant Initiated Transaction (MIT)	N/A	Yes (initial transaction	Yes	Issuer ECI 5
			No (subsequent transaction)	No	Acquirer ECI 7
			Yes (transaction using the reauthorization indicator that carry a CAVV and associated ECI 5)	Yes (however exemption may be applicable)	Issuer ECI 5
	MOTO		No	No	Acquirer ECI blank, 1, or 4
	One Leg Out	N/A	Yes	Optional	Issuer ECI 5
		N/A	No	N/A	Acquirer ECI 7
SCA Required	Does not qualify for an exemption or transaction is a CIT setting up or changing an MIT series agreement when such a change requires SCA	N/A	Yes	Yes	Issuer ECI 5

VISA

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.

4.5.1 The low value exemption

The difficulties in deploying the low value exemption have been described in section 4.3. While this may prove to be a useful exemption to apply for payments that do not warrant the application of complex risk and authentication technology, they should also not be considered low risk just because they are of low value. Issuers need to ensure they have velocity checking in place and are able to provide an SCA required decline (1A) should the maximum value or transaction count be exceeded.

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 summarised 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 Regulatory and Technical Standards for SCA lays down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs.

Recital 14 of the RTS states that: "risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments".

Article 2 of the RTS also states that: "Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors: (a) lists of compromised or stolen authentication elements; (b) the amount of each payment transaction; (c) known fraud scenarios in the provision of payment services; (d) signs of malware infection in any sessions of the authentication procedure; (e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software."

Visa requirements for the deployment of Risk Based Analysis and EMVCo 3DS 2.0 specifications for the data elements that should be provided as the basis for RBA risk scoring are summarised in sections 0 and 0. Visa has also recommended standards for transaction monitoring and fraud detection and has best practice guides available on these subjects.

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

4.5.2.3 Outsourcing the application of TRA

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

Under the regulation, Acquirers may contractually outsource the application of TRA to merchants (ref EBA Opinion Paper on the implementation of the RTS on SCA and CSC June 2018, para 47).

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 22: Reference fraud rates

Transaction value band	PSP fraud rate
<€100	13 bps/0.13 %
€100-€250	6 bps/0.06 %
€250-€500	1 bps/0.01 %

Merchants, Acquirers and Issuers can all apply measures to ensure that they maximise 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 minimise 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 minimising customer friction. While over aggressive application of SCA may decrease fraud rates, the inconvenience to consumers brings the risk of:

  o Increased transaction abandonment, reducing ecommerce transaction rates and consumers switching to alternative, lower friction payment methods or Issuers.

  o Breaching the Visa rule limiting transaction abandonment (see section 3.4 for more details).

VISA

4.5.2.5   Calculation of fraud rates

The PSD2 regulation[13] requires that:

- The calculation of the fraud rate includes both unauthorized transactions and fraudulent transactions resulting from the manipulation of the payer; and

- 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.

- 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 once they go over the reference fraud rates.

Visa's view is that in the case that one of the PSPs (the Issuer or the Acquirer) applies the TRA exemption, any fraud from that transaction should only be attributable to the fraud count of the PSP that applied or requested the exemption, but PSPs need to be responsible for determining their own fraud rates in accordance with the legal requirements of PSD2. We are currently engaging with regulators on this.

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 with the trusted merchant should generally not be required.

It should be noted that in order to be compliant with SCA provisions:

- Only Issuers can create/maintain lists of trusted beneficiaries on behalf of cardholders and use the trusted beneficiaries exemption, although Issuers are allowed to outsource or delegate this solution (such as through Visa Trusted Listing).
- Only cardholders can add/remove a merchant to/from a list of trusted beneficiaries, or consent to a suggested addition/removal provided by the Issuer.
- Acquirers cannot apply this exemption and a merchant cannot set up the list for the purpose of the SCA exemption.

---

[13] 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 13th June 2018.

4.5.3.2   Issuer options

Issuers are not under any obligation to provide their cardholders with a trusted beneficiary capability. However, supporting 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.

4.5.3.3   Merchant options

While merchants cannot manage lists of trusted beneficiaries or enrol themselves in a customer's trusted beneficiaries list, they can advise their customers of the benefits of using trusted lists and facilitate the enrollment process through:

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

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 3-D Secure.

4.5.3.4   Application of the trusted beneficiaries exemption through the Visa Trusted Listing solution

This section describes how the trusted beneficiaries exemption may be implemented through the Visa Trusted Listing solution.

The Visa Trusted Listing solution provides a complete hosted solution for Issuers minimising the development and operational overhead associated with offering a trusted beneficiaries solution.

4.5.3.4.1   Merchant Eligibility

4.5.3.4.1.1   Visa Merchant Identifier (VMID)

Each merchant who participates in the Visa Trusted Listing program will be assigned a unique identifier to be used across all Acquirers. The VMID is a unique eight digit number, for each merchant's branded business entity.   For the initial phase, the VMID will assigned manually. The merchant and/or the 3DS Server Provider can request a VMID following the process in the 3DS implementation guide.

4.5.3.4.1.2   Compliance program

Visa is creating a compliance program to monitor merchants who are participating in Visa Trusted Listing, by the merchant's VMID. The criteria to enter the program are still under review, but once in the program, merchant must maintain a fraud rate similar to the 3-D Secure rate for the market for trusted beneficiaries exempted transactions. More information about the compliance program will be shared once finalized.

4.5.3.4.2 Customer Experience

4.5.3.4.2.1 Enrollment

3-D Secure:

Visa will support PAN or token enrollment through 3-D Secure 2.2 or VTS. The cardholder, who is eligible to participate, can add a merchant in two ways:

1. During a transaction, a customer can be prompted to list their card through the ACS screens of 3-D Secure. Once the customer opts in and preforms strong customer authentication, then the merchant is saved to the customer's trusted list and the transaction completes.
2. A customer can be prompted to add a merchant to their list, outside of a purchase flow (e.g. when saving a card on file with a merchant) to opt in and add the merchant to their list and perform strong customer authentication through 3-D Secure.

The 3DS 2.2 functionality is expected to be available May 2019.

Token Network Push Provisioning:

The merchant can prompt the cardholder to enrol in Trusted Listing during token provisioning or outside of provisioning using the standalone Trusted Listing request. In this flow, Visa will generate an OTP for the Issuer, validate the OTP, and prompt the customer to add the merchant to his/her trusted list.

The Trusted Listing enrollment through token provisioning is expected to be available late 2019.

4.5.3.4.2.2 Authorization

Once the customer has listed a merchant, subsequent transactions should not require additional authentication. The Acquirer can send the transaction through authorization, with the Trusted Listing exemption flag in Field 34 and the VMID in Field 126.5. The transaction will flow to Visa, where Visa will validate the status of the PAN and VMID to determine if the relationship is still in an active list.

Visa will support both PAN and token in the authorization flow, the functionality is expected to be available by May 2019.

4.5.3.4.3 Liability

PSD2 sets out regulatory liability rules. The current Visa Rules around liability for chargebacks remain in place and their application in relation to SCA is set out above. If a merchant or Acquirer would like chargeback protection, they can choose to submit a 3DS authentication request to the Issuer who can then decide to perform SCA or apply an exemption.

4.6   Additional Guidelines for Issuers

4.6.1   Issuer selection and deployment of 3DS 2.0 challenge methods - ensuring security with a seamless UX

Providing both secure and consumer friendly challenge methods are vital to ensure all cardholders in an Issuer's portfolio are able to complete an SCA challenge with minimal abandonment. Visa currently intends to introduce minimum abandonment rate thresholds from October 2019 which require Issuers to ensure abandonment rates are below 5%. How easy it is for consumers to transact online will be a key factor in their decision to keep a card top of wallet.

4.6.1.1   Factors driving selection of challenge methods

Issuers need to develop strategies for adoption of challenge methods that achieve an appropriate balance between the following considerations:

- Compliance with the SCA factor requirements of PSD2 as summarised in section 2.1

- Simplicity of user experience and minimisation of friction when a challenge is required

- Effective support of app and browser-based checkouts

- Compliance with Visa rules on abandonment and latency (see section)

- Social inclusion

- Security of challenge methods and resistance to exploitation by fraudsters

- Availability/reliability

- Cost

4.6.1.2   The development of inclusive strategies

3-D secure supports multiple SCA challenge options, many of which are delivered via a smartphone or standard mobile handset. It is expected that most Issuers will offer options to customers to ensure that they are able to complete SCA challenges independently of device ownership, mobile network coverage, physical disability etc.

Visa's view is that biometric based challenges delivered via pre-registered, trusted smart phones will deliver the best balance between compliance, security and minimisation of UX friction in the medium term. Visa is implementing a rule that will require Issuers to support biometric solutions. However, it is recognised that not all customers will own a biometric capable device or wish to use biometric challenge methods.

Table 23: Potential SCA Challenge Options

Challenge Method	Description	Advantages	Disadvantages
SMS OTP	OTP is delivered via SMS to validate device possession or to provide knowledge factor. Used alongside second independent factor	• Inclusive – most customers can access SMS • Already widely deployed • Works in conjunction with browser and app checkouts on various devices	• Security vulnerabilities • Uncertainty over whether SMS OTP is acceptable to some local regulators • Requires mobile network coverage • Message cost • UX not as integrated as other options
Out of Band App delivered OTP	As SMS, but OTP is delivered via a banking or other mobile app	• More secure than SMS OTP • Does not require mobile network coverage	• Requires smartphone and use of app • Requires user to manually open out of band app (3DS2.1 & 2.2)
Native device Biometric	Built in phone biometric (for example Apple touch ID) is used to provide inherence factor or prove possession of device. In the case of fraud, merchant is liable if outside 3DS, the Issuer is liable if the biometric is used as a 3DS challenge	• Seamless user experience • Consistent biometric experience for all authentication experiences provides familiarity for customer • Does not require mobile network coverage	• Requires delegated authentication agreement with handset platform vendor • Issuer is reliant on third party
App based biometric	Facial, voice or behavioural biometric enabled by a banking or dedicated app	• Seamless user experience • Handset does not require biometric sensor • Issuer controls authentication • Does not require mobile network coverage	• Requires stand-alone app • Inconsistent authentication experiences between services from different providers

VISA

OTP generator token	Standalone OTP generator device	• Allows those without a mobile phone to authenticate • Does not require any connectivity	• Consumer needs to carry device • UX is more complex than alternatives • Cost of device distribution

Issuers will therefore need to offer alternatives including SMS OTP and provision of stand-alone PIN Entry devices.

Given the effectiveness of SMS OTP plus card data in mitigating fraud across Europe, a sudden replacement of this authentication method by September 2019 is both impracticable and potentially disruptive for European cardholders including those who do not own a smartphone.

Issuers that use, or plan to use SMS OTP should however ensure that they have auditable measures in place to mitigate known risks associated with SMS and should develop a roadmap to migrate customers to more secure authentication methods. More guidance on the use of SMS OTP and biometrics can be found in section 5.3.1 of the Visa paper Preparing for PSD2 SCA.

3DS UX guidelines for Issuers are available on the Visa Developer Centre.

4.6.2   Issuer Processing Guidelines

This section summarises the key points that Issuers need to be aware of when considering their role in the smooth implementing of SCA for eCommerce.

There are a number of important areas for Issuers to consider when processing e-commerce transactions.

4.6.2.1   Zero value authorizations

There are a number of reasons why a merchant may do a zero value transaction (Account Number Verification transaction) as documented in Section 5. It is important that Issuers understand these reasons as described below and adopt appropriate processing policies as several zero value transactions do not necessarily require SCA. Therefore, even if a transaction has no CAVV, no exemption indicator and is not of a type that is out of scope of PSD2, it should not be declined with a response code of 1A (SCA required) if it is of zero value. Note that, Token-based zero value authorizations that are not identfied as MIT will continue to be submitted with a TAVV[14] even if the CAVV is not present.

---

[14] 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 24: Summary of Information Provided in Following Subsections

#	Conditions	Is SCA Required?
1	• Zero value • No CAVV • TAVV (if token) • No POS environment (F126.13) • No message reason code (F63.3) • No initial Transaction ID (F125)	**No –** Issuers should avoid issuing an SCA required decline (1A) on the basis that authentication is required. Refer to Standard Account Verification below. Also see info in #4 of this table. Note: Even though SCA is not required, Visa requires the merchant to provide a TAVV in all Token transactions unless the transaction is identified as an MIT.
2	• Zero value • CAVV (present in most cases but could be absent in some) • TAVV (if token) • **'C' in POS environment (F126.13)** • No message reason code (F63.3) • No initial Transaction ID (F125)	SCA is required in most cases. Future CITs performed with the credential will also require SCA, or a suitable exemption. Refer to Setting up a Stored Credential below.
3	• Zero value • **CAVV** • TAVV (if token) • **'R', 'I' or 'C' in POS environment (F126.13)** • No message reason code (F63.3) • **No initial Transaction ID (F125)**	**Yes –** If CAVV is not valid, then the Issuer can decline with reason code 1A. Refer to Setting up an agreement for Subscription and Installment MITs below.
4	• Zero value • **CAVV** • TAVV (if token) • No POS environment (F126.13) • No message reason code (F63.3) • No initial Transaction ID (F125)	**Yes** – When authentication data is included in a standard account verification, it is because the merchant knows there is a reason for authenticating. The presence of a CAVV is legitimate in many cases. Refer to "Setting up an agreement for No Show, delayed charges and incremental". However, at this stage, an Issuer will not be able to tell if the transaction is setting up an agreement for those use cases or if it is just a standard account verification as in set of condition 1 in this table.

VISA

4.6.2.1.1 Standard Account Number Verification

An Account Number Verification is a zero value transaction with:

- No value in Field 126.13 or in Field 63.3
- No CAVV
- TAVV (if token)
- No initial Transaction ID in Field 125

This is not a financial transaction, but a transaction processed purely to check the validity of a card: it is out of scope of PSD2 and Issuers should ensure it is not declined based on the lack of authentication. The merchant is checking validity and will likely be doing a financial authorization including authentication data or suitable exemption flags later.

4.6.2.1.2 Setting up a Stored Credential

A merchant may use a zero value transaction when storing credentials for future CIT transactions and no payment is due at the same time. The zero value transaction will have:

- The value 'C' in Field 126.13
- No message reason code in Field 63.3
- CAVV (present in most cases, but could be absent in some)
- TAVV (if token)
- No initial Transaction ID in Field 125

SCA would be generally required in this case, where it reflects the cardholder taking a remote action (i.e. providing card details) which entails a possible risk of payment fraud.

4.6.2.1.3 Setting up an agreement for subscription and installment MITs

A merchant may use a zero value transaction to establish an agreement for future MITs if no initial charge is made at the time the agreement is made. Where the initial mandate is set up via a remote electronic channel, SCA is required in most cases (see section 5.9). Therefore, the zero value transaction will have:

- An indicator in Field 126.13- R, C or I, depending on which type of agreement is being set up (and no value in Field 63.3)
- A CAVV and associated ECI value to prove authentication was performed
- A TAVV (if token)
- No exemption indicator in F34
- No initial Transaction ID in Field 125

This is a transaction to establish a mandate for future Standing instruction MITs, such as recurring payments (R), installments (I) or Unscheduled Credential-on-File (C) – these are subscriptions at non regular intervals, not to be confused with CITs performed with stored credentials).

4.6.2.1.4 Setting up an agreement for No Show, Delayed Charges and Incremental MITs

A merchant may use a zero value transaction to establish an agreement for future MITs if no initial charge is due at the time the agreement is made. Where the initial mandate is set up via a remote electronic channel, SCA is required in most cases (see section 5.9). Therefore, the zero value transaction will have:

- No value in Field 126.13 nor in Field 63.3
- A CAVV to prove authentication was performed
- A TAVV (if token)
- No initial Transaction ID in Field 125

This is a transaction to establish a mandate to perform a future industry specific MIT, such as No Show, Delayed Charges or Incremental. As there is no specific indicator to enable an Issuer to differentiate this zero value transaction from a standard account verification, the Issuer should not decline the zero value transaction on the basis that authentication is present or not in an account verification message. However, any future MITs using Message Reason Codes for No Show, Delayed Charges or Incrementals must refer back to an initial CIT where authentication was performed.

4.6.2.2 MIT transactions

MIT transactions received relating to a previous CIT to establish the agreement do not typically include CAVV or TAVV information, with the exception of reauthorizations, where authentication data may be included by a merchant in order to claim fraud liability protection.

4.6.2.3   Reauthorizations

A number of the scenarios in Section 5 use the reauthorization message reason code 3903 with an initial Transaction ID in Field 125 to identify cases where an authorization is being performed when the cardholder is not present to complete a previous transaction, for example in the case of a:

- delayed authorization or
- because multiple authorizations are processed, one for each individual shipment or item of one check out order.

The transaction was in scope, but exemptions could apply and in the case of split shipments, more than one CAVV may not be available to use in each transaction. Therefore, depending on the scenario a merchant may choose to include a CAVV in a reauthorization for fraud liability protection.

For token transactions, as reauthorizations are flagged under the Visa MIT Framework, no TAVV will be included.

It contains a CAVV when one was obtained during an earlier interaction where a zero value transaction was performed but the CAVV was kept for this later authorization (e.g. when a delayed order was placed) or a new one was obtained just prior to the delayed authorization or split shipment authorization by calling the 3RI feature of 3DS.

It does not contain a CAVV when either a valid exemption was used during the initial authorization and thus no CAVV was obtained (in this case the exemption flag should be populated in the authorization with message reason code 3903) or when the merchant already used the CAVV in an initial authorization and did not call 3RI to obtain a new one.

If there is no CAVV, the Issuer should only consider declining with a reason code 1A (SCA required) after checking the related CIT was not out of scope, exempted or authenticated.

4.6.2.3.1   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. Instead, the CAVV if otherwise valid, provides evidence that SCA has been performed and therefore Issuers should not decline with a reason code 1A (SCA required).

> ### Key Point
>
> **Merchants are liable for fraud on reauthorisations including a CAVV that is over 90 days old under the Visa rules, however, the CAVV can still be used as evidence that SCA was performed**

CAVVs over a year old will fail validation by Visa and will be flagged accordingly.

VISA

4.6.2.4   Resubmissions

MIT transactions identified as resubmissions will never be provided with a CAVV as the original CIT to which they refer in the initial Transaction ID field are either out of scope of PSD2, exempted or fully authenticated and there is no requirement to indicate this status in the resubmission. For more information refer to section 5.8. If a token is used, as resubmissions are flagged under the Visa MIT Framework, no TAVV will be included.

4.6.2.5   Transactions identified in accordance with the MIT framework

Transactions identified under the MIT framework will generally have been performed at a time when the cardholder is not available. For this reason, Issuers should avoid declining a transaction flagged with the Visa MIT framework solely on the basis that cardholder authentication was not performed (i.e. Issuers should avoid declining a transaction flagged according to the MIT framework based on the lack of authentication data).

> ### Best Practice
>
> **Issuers should avoid declining MITs on the basis that authentication is required (an SCA required decline – reason code 1A), as the cardholder is generally not present to authenticate.**

Issuers should note that where the initial mandate is set up via a remote electronic channel, SCA is required in most cases for all MITs.

A transaction identified with R, I or C in Field 126.13 but no transaction ID in Field 125 represents the transaction where the Recurring (R), Installment (I) or Unscheduled Credential Agreement (C) agreement is being set up. As such it is a CIT (not an MIT) and SCA is required in most cases. The amount may be zero if no money was due at agreement set up.

When a transaction is however identified with R, I or C in Field 126.13 and with a transaction ID in Field 125, it is an MIT, thus out of scope and no SCA is required.

Transaction using a reason code in Field 63.3 always require a Tran ID in Field 125 and as they are MITs, they are considered by Visa to be out of scope of PSD2 and SCA is not required.

For more information about the different types of MIT and how they are indicated in authorization messages, see section 5.7.1.

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 for more details.

4.6.2.6 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.

4.6.2.7 3RI authentication requests

Issuers supporting 3-D Secure version 2.1 and above may receive 3RI requests for a new CAVV for a transaction under some of the scenarios defined in Section 5, such as delayed or split shipments. Each request for an updated CAVV should be assessed on its merits. Issuers must not blanket decline 3RI requests.

4.6.2.8 Authentication provided by parties other than the merchant

In some cases, authentication may be performed by a party other than the merchant submitting authorization. Therefore, Issuers must be aware that the merchant name used in authentication may legitimately be different to the merchant name 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".

4.6.2.9 Using TAVVs to prove cardholder authentication

In some cases, qualifying token requestors will be able to use the new Cloud Token Framework (CTF) TAVV format as evidence cardholder authentication has been performed. In such cases a CAVV is not required for SCA compliance. TAVVs used in this way do not currently qualify the merchant for liability protection. Further information will be made available from the Visa Token Service as these new options become available.

Visa requires TAVV (existing or new CTF TAVV) to be present in all Token transactions unless the transaction is identified as a Merchant Initiated Transaction.

4.7   3DS and authorization fall-back options

If for any reason an Issuer is unable to authenticate a transaction using 3DS, or is unable to respond to an authorization request, Visa will step in through application of the Visa Attempts Server or Stand-in Processing Service (STIP) respectively.

4.7.1   The Visa Attempts Server

The Visa attempts server will respond to an authentication request if the Issuer does not support 3DS 2.0 (applicable from April 2019), or the Issuer's ACS is unavailable or does not respond in time. In these cases, the Attempts Server will respond with an ECI 6 and the Issuer assumes liability.

Figure 16: The role of the Visa Attempts Server
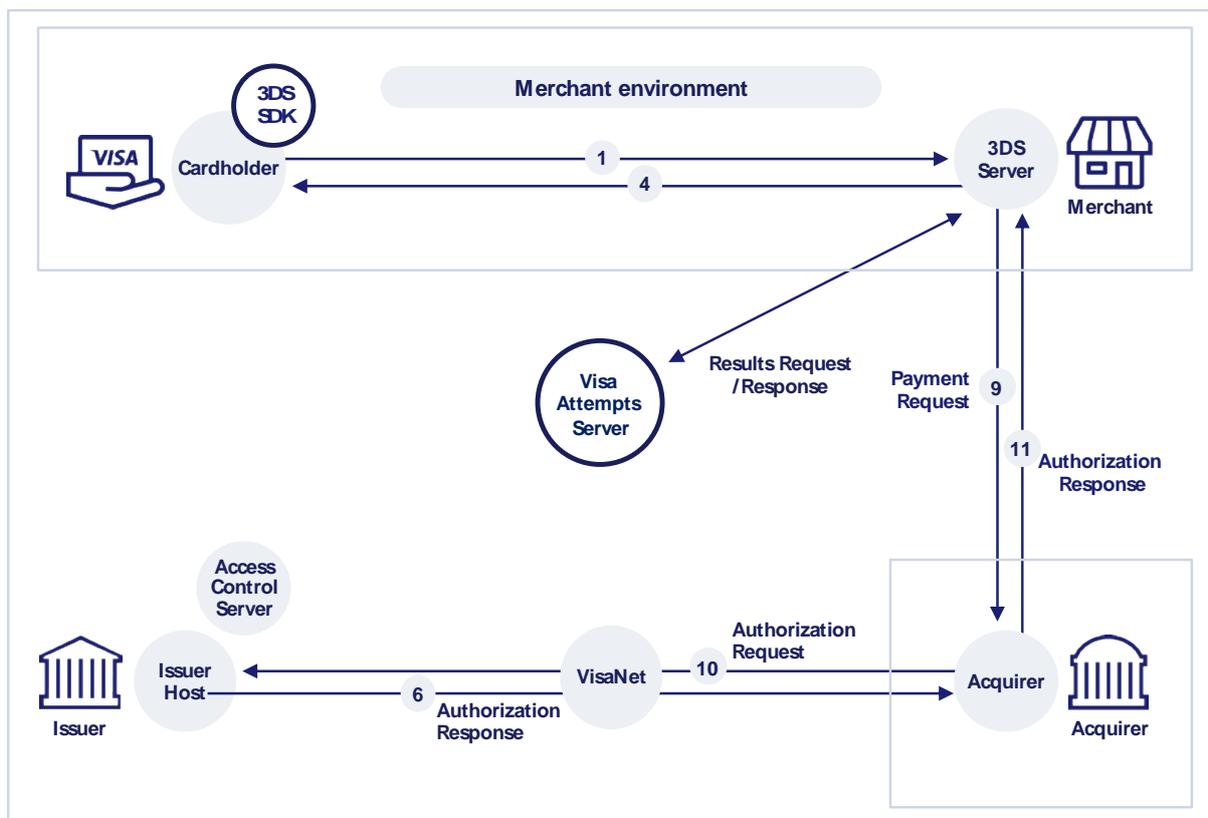
4.7.2   STIP

The VisaNet Stand-in Processing (STIP) approval service acts as a back-up processor when the Issuer is unable to respond, responding slowly or reaching authorization capacity.

When used properly, the VisaNet Stand-in Processing approval service (STIP) provides business continuity during Issuer maintenance or unexpected processing issues.

Issuers define spend limits, risk thresholds and authentication options used by the VisaNet STIP approval service to approve or decline transactions on their behalf.

Figure 17: Operation of the STIP approval service

1. Authorization request comes into VisaNet
2. Transaction characteristics and historical data are used to assign VAA score
3. Authentication data and business rules are evaluated
4. VIP determines issuer availability. If the issuer is unavailable, timing out or nearing capacity the authorization is routed to STIP
5. Transaction is evaluated against issuer STIP VAA risk limit and activity limits. Transaction that pass all verifications are approved, all others are declined
6. Approve/decline response sent to Acquirer. STIP advice sent to issuer.

Figure 18: The VisaNet STIP service offers a robust set of parameters to effectively manage STIP risk, including:

Business Risk	Counterfeit Risk	Fraud Risk	Credit Risk
Business restrictions allow issuers to manage restrictions such as: • Government sanctions • Valid countries • Illegal or unsupported transaction types • Lost / stolen / closed account • Stop payment orders	**VisaNet Card authentication** validates data within the transaction based on issuer defined settings: • Mod-10 check • Expiration date • CVV, CVV2, PIN, CAW, etc.	**VAA STIP risk score limits** allow issuer to define risk tolerance thresholds to be applied to each transaction: • Card present • Card not present • Cash	**Activity (spend) limits** allow issuers to define daily transaction limits separately for purchase and cash: • Daily transaction count • Daily transaction amount • Max single transaction size • Combined purchase and cash daily count and amount maximum

A STIP transaction must pass all VisaNet edits to be approved

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. Visa Advanced Authorization (VAA) Score evaluates risk for each transaction.

Figure 19: An example set of STIP Limits for an Issuer's BIN

VISA

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

✔ It supports different limits for debit and credit portfolios for both purchase and cash transactions.

✔ Issuers should review and update limits regularly in order to create a seamless customer experience.

✔ Every transaction is allocated a risk score, irrespective of whether the issuer subscribes to Visa Advanced Authorization or Visa Risk Manager. Visa will decline all transactions in STIP that are above the risk threshold accepted by an issuer.

✔ It can perform cardholder validation and checks on behalf of issuers.

✔ Issuers can identify and manage customers that require special treatment. Important customers can be treated differently, and any reported lost or stolen cards will not be approved in STIP.

✔ Having STIP limits in place can allow issuers to focus on fixing the underlying problem rather than handling calls from unhappy customers when the unexpected happens.

For Strong Customer Authentication, VisaNet STIP has been enhanced resulting in the following additional configuration options:

1. Does the Issuing BIN want to decline all ECI 6 e-commerce transactions without a valid exemption in STIP?

2. Does the Issuing BIN want to decline all ECI 7 e-commerce transactions without a CAVV and without a valid exemption in STIP?

3. Does the issuing BIN want to decline all ECI 7 e-commerce transactions with a CAVV and without a valid exemption in STIP?

In each case the Valid values are:
- "Y – Decline with Response Code 05"

- "Y – Decline with Response Code 1A" (i.e. require Step-up Authentication)

- "N" – approve the transaction

In each case the exemptions are as follows:

- Acquirer Low Value Payment Exemption – Y/N (default is N)

- Acquirer Transaction Risk Assessment Exemption – Y/N (default is N)

- Acquirer Trusted Merchant Exemption – Y/N (default is N)

- Acquirer Secure Corporate Payment Exemption – Y/N (default is N)

- Issuer Exemption - Transaction amount less than low value limit – Y/N (default is N)

A summary of the STIP process flow can be found at Appendix A.5.

VISA

Section 5

Payment use cases and
sector specific guidance
for merchants and PSPs

VISA

5. Payment use cases and sector specific guidance for merchants and PSPs

The following subsections provides 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 is provided for each payment scenario:

- Brief description introducing the payment scenario and when it is applicable, and
- 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 summarised in Section 4 and with any applicable laws, regulations and Visa Rules.

It is advisable that Issuers also familiarise themselves with the illustrated approach for handling each of the different eCommerce payment scenarios, so that they can adopt appropriate authorization policies to minimise unnecessary friction with their customers.

IMPORTANT NOTE:

The scenarios presented in this section are relevant to merchants meeting SCA authentication requirements for PANs and Tokens using 3-D Secure.

In some cases qualifying token requestors can use the Cloud Token Framework TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance. TAVVs used in this way do not currently qualify the merchant for fraud liability protection.   More information will be provided about the Visa Token Service as these new options become available.

VISA

5.1   One-time purchase

A merchant receives an order from a customer for a known amount that they are 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 A: Stored Credential Framework**

Scenario Steps
Customer Checks Out Basket
1.   The merchant **authenticates** the transaction immediately for the full amount, obtaining a CAVV or CTF 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.   The merchant immediately **authorizes** the transaction for the full amount[15], including either:
   a.   sufficient information to enable the identification of the transaction as out of scope or;
   b.   applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, or;
   c.   CAVV or CTF TAVV and associated ECI value
 	
The merchant only receives fraud liability protection under the Visa Rules if a CAVV is provided with an ECI value of 05 or 06. For options (b) and (c), the CAVV should always be included, if obtained, in order to prevent the Issuer responding to the authorization with a SCA decline (response code 1A - SCA required).
 	
Note: When processing a transaction with tokens, qualifying token requestors can provide the merchants with CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA purposes.

Shipment made (Customer no longer available)
3.   The merchant ships the good(s) and **clears** the transaction for the full amount within 7 days.
Order Complete

---

[15] It is permissible for the amount in authentication and authorization to vary within the customer's reasonable expectations. See Section 4.2.3.3, Principle 3

VISA

5.2 Delayed Shipment

5.2.1 Delayed Shipment - expected delay

A merchant receives an order from a customer that they will fulfil in a single shipment, but they know they will not be able to deliver within 7 days. The amount is known and not expected to change other than minimally due to, for example, shipping costs. 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 maximise the opportunity for funds to be available.

Scenario Steps
Customer places an Order
1. The merchant **authenticates** the transaction immediately for the full amount, obtaining a CAVV or CTF 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. The merchant must not authorise the transaction immediately as the authorization 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. If the merchant requires fraud d liability protection, they should not include the CAVV, so that it can be included later in the delayed financial authorization[16]. The merchant must also store the Transaction ID of the account verification for later use. Issuers should not decline an account verification without a CAVV with a response code of 1A (SCA required), since this is not a financial transaction. If a token-based transaction, then the TAVV must be included in the account verification.
Merchant ready to make shipment (Customer no longer available)

3. When the order is ready for shipment, the merchant **authorises** for the full amount. The authorization must include:
     o 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)
     o Either applicable exemption indicators (in Field 34) along with an ECI of 07 or an ECI 05 (or 06) and the CAVV from the authentication.
• The merchant only receives fraud liability protection if authentication was performed or attempted (ECI 05 or 06). In addition, including the CAVV informs the Issuer that authentication has already been performed and so should prevent them responding to the authorization with a response code 1A - SCA required.
• 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 4.2.3.34.2.3.3, Principle 12.

Shipment made

---

[16] Merchants who wish to, can include the CAVV in the account verification. However, such merchants must be aware of the implications of this approach, as described in Principle 1 of Section 4.2.3.3.

VISA

4.   The merchant *clears* the transaction for the full amount.
Order Complete

5.2.2 Delayed Shipment - unexpected delay

Merchants who follow best practice should only perform authorization when they confirm that the goods are available and ready to be shipped (Principle 10). However, if a merchant does authorize before confirming goods are available, Visa recommends they proceed as follows. Merchants in this situation must be aware that 3DS v1.0 does not support 3RI and the ability to obtain a new CAVV required for fraud liability protection.

Scenario Steps
Customer places an Order
1.   The merchant *authenticates* the transaction immediately, obtaining a CAVV or CTF 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.   The merchant immediately *authorizes* the transaction for the full amount[17], including either:
  a.   sufficient information to enable the identification of the transaction as out of scope of PSD2 SCA or;
  b.   applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, or;
  c.   CAVV or CTF TAVV and associated ECI value
If a token-based transaction, then the TAVV must be included.

End of 7 day Authorization validity period (Customer no longer available)
3.   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.   When the order is ready for shipment, the merchant *authorizes* for the full amount. The authorization must include:
  •   A message reason code of 3903 to indicate that the customer is no longer present
  •   the Transaction ID from step 2 (as per MIT framework).
If the original authorization included a CAVV and ECI 05 and 06 then the merchant must be aware that the original CAVV has been used and cannot be stored, therefore the merchant can either:
  •   Submit the authorization with no CAVV and accept that this means no fraud liability protection. Applicable exemption indicators should be populated to help prevent the Issuer responding to the authorization with a response code 1A - SCA required, or;
  •   use 3RI (if available) to obtain a new CAVV for the remaining amount (with ECI 05 or 06) to receive any applicable fraud liability protection and help prevent the Issuer responding to the authorization with a response code 1A - SCA required
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 4.2.3.3, Principle 12.

---

[17] Which may vary from the authenticated amount only within the customer's reasonable expectations.

VISA

Shipment Made
5. The merchant *clears* the transaction for the full amount.
Order Complete

5.3 Split Shipment

5.3.1 Split Shipment - all fulfilled within 7 days

A merchant receives an online order from a customer for multiple items that they are able to fulfil within 7 days, but the goods are delivered in multiple shipments.

Scenario Steps
Customer places an Order
1. The merchant *authenticates* the transaction immediately for the full amount, obtaining a CAVV or CTF 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 4.2.5.2.5.

2. The merchant immediately *authorizes* the transaction for the full amount[18], including either:
    a. sufficient information to enable the identification of the transaction as out of scope or;
    b. applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, or;
    c. CAVV or CTF TAVV and associated ECI value
If a token-based transaction, then the TAVV must be included.

Shipment Made (Customer no longer available)
3. The merchant *clears* for each shipment separately as and when they happen over the next 7 days using multiple clearing sequence numbers[19].
Order Complete

Visa best practice is to use a single authorization with multiple clearing records for split shipment scenarios as defined in Section 4.2.3.3, Principle 10.

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 5.3.3.

---

[18] Which may vary from the authenticated amount only within the customer's reasonable expectations.
[19] For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

VISA

5.3.2 Split Shipment - partially fulfilled within 7 days (unexpected delay)

A merchant receives an order from a customer that they fulfil 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 (Principle 10), will not find themselves in this position. Instead, they will either be able to confirm shipment straight away (refer to Section 5.3.1) or they will identify a delay and therefore the need to perform multiple authorizations (refer to Section 5.3.3).

However, if a merchant does authorize before confirming goods available for shipping and then finds themselves in this situation, Visa recommends they proceed as follows. If a merchant ends up with this scenario, then they must be aware that 3DS v1.0 does not support 3RI and the ability to obtain a new CAVV required for fraud liability protection.

Scenario Steps
Customer places an Order
1. The merchant **authenticates** the transaction immediately for the full amount, obtaining a CAVV or CTF 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. The merchant immediately **authorizes** the transaction for the full amount[20], including either: 　　a. sufficient information to enable the identification of the transaction as out of scope or; 　　b. applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, or; 　　c. CAVV or CTF TAVV and associated ECI value The merchant must also store the Transaction ID for this step for later use. If a token-based transaction, then the TAVV must be included.
Merchant ready to make partial shipment (Customer no longer available)
3. The merchant **clears** for each shipment separately using multiple clearing sequence numbers as and when each shipment occurs over the next 7 days[21] .
End of 7 day Authorization validity period (Customer no longer available)
4. 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)

---

[20] Which may vary from the authenticated amount only within the customer's reasonable expectations.
[21] For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

5. When each subsequent partial order is ready for shipment, the merchant *authorizes* for the amount relating to the goods included in the shipment. The authorization must include:
    o 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)
  • If the original authorization included a CAVV and ECI 05 and 06 then the merchant must be aware that the original CAVV has been used and cannot be stored, therefore the merchant can either:
    o Submit the authorization with no CAVV and accept that this means no fraud liability protection. Applicable exemption indicators should be populated to help prevent the Issuer responding to the authorization with a response code 1A - SCA required, or;
    o use 3RI (if available) to obtain a new CAVV for the remaining amount (with ECI 05 or 06) to receive any applicable fraud liability protection and help prevent the Issuer responding to the authorization with a response code 1A - SCA required
  • 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 4.2.3.3, Principle 12.

6. The merchant *clears* each re-authorization as the related shipments are made.
Order Complete

5.3.3   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 minimise 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. The merchant *authenticates* the transaction immediately for the full amount, obtaining a CAVV or CTF 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. Depending on whether the goods for inclusion in the first shipment are immediately available, the merchant must either:
    a. immediately *authorise* the transaction for the value of the goods to be shipped if goods are available, including either:
        i. sufficient information to enable the identification of the transaction as out of scope or;
        ii. applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, or;
        iii. CAVV or CTF TAVV and associated ECI value
    b. perform a zero-value *account verification* if goods to be shipped are not available. This will check that the card is valid and allow the merchant to obtain an "initial" transaction ID. If the merchant requires fraud liability protection, they should not include the CAVV, so that it can be included later

VISA

in the delayed financial authorization[22]. Issuers should not decline an account verification without a CAVV, with a response code of 1A (SCA required) in this scenario. If a token-based transaction, then the TAVV must be included in the account verification. The merchant must store the Transaction ID from this step for use in step 3. If a token-based transaction, then the TAVV must be included.
Merchant ready to make shipments (Customer no longer available)
3. When each of the remaining shipments is ready, the merchant ***authorises*** for the value of goods to be shipped. The authorization must include: o 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)   • If the merchant requires fraud liability protection, they should include the CAVV in this authorization. If the CAVV has already been submitted in the account verification or authorization for a previous shipment, the merchant must be aware that the original CAVV has been used and cannot be stored, therefore the merchant can either: o Submit the authorization with no CAVV and accept that this means no fraud liability protection. Applicable exemption indicators should be populated to help prevent the Issuer responding to the authorization with a response code 1A - SCA required, or;   o use 3RI (if available) to obtain a new CAVV for the remaining amount (with ECI 05 or 06) to receive any applicable fraud liability protection and help prevent the Issuer responding to the authorization with a response code 1A - SCA required   • 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 4.2.3.3, Principle 12.
4. The merchant ***clears*** the amount authorized as the related shipment is made.
Order Complete

---

[22] Merchants who wish to, can include the CAVV in the account verification. However, such merchants must be aware of the implications of this approach, as described in Principle 1 of section 4.2.3.3.

VISA

5.4 Open orders - Unknown amount

The merchant receives an order with an initial amount that they expect to change significantly between now and the time of shipping.

For example, online groceries where the delivery date can be booked several days, weeks or even months in advance. The customer can come back and update the order as often as they like up until the pre-agreed cut-off time. In addition, even after the order is complete, further variance may occur, due to item substitutions, weight etc.

In this scenario, there are different options for the merchant to consider. The best option for a particular merchant will depend upon their preferred business processes.

In all cases, if the final authorization is to take place several weeks/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 maximise chances of funds being available.

5.4.1 Option 1: Delayed authorization, authenticate every order update

Scenario Steps
Customer places an Order
1. The merchant **authenticates** the transaction immediately for the initial order amount, obtaining a CAVV or CTF 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. The merchant must perform a zero-value **account verification** to check that the card is valid, and obtain an "initial" Transaction ID. If the merchant requires fraud liability protection, they should not include the CAVV, so that it can be included later in the authorization[23]. The merchant must store the Transaction ID for possible use in step 4. Issuers should not decline an account verification without a CAVV, with a response code of 1A (SCA required) in this scenario. If a token-based transaction, then the TAVV must be included in the account verification.
Customer updates Order
3. 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 CTF TAVV (and associated ECI value), discarding the initial one and keeping the latest one. Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5. • The merchant may also optionally perform an additional zero-value *account verification* each time to check that the card is valid but if the merchant requires fraud liability protection, they should not include the CAVV from the new authentication in the account verification so that it can be included later in the authorization. If a token-based transaction, then a TAVV must be included in the account verification.
Merchant ready to make shipment (Customer no longer available)
4. At time of shipping, the order is closed. The merchant **authorizes** for the latest authenticated amount. The authorization must include: o 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)

---

[23] Merchants who wish to, can include the CAVV in the account verification. However, such merchants must be aware of the implications of this approach, as described in Principle 1 of Section 4.2.3.3.

	o	The CAVV and ECI value from the latest authentication if it was not included in the account verification and / or any applicable exemption indicators

- 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 4.2.3.3, Principle 12.

5. The merchant **clears** the transaction for the final amount.

<div align="center">Order Complete</div>

5.4.2 Option 2: Authenticate for a maximum estimated amount upfront, delayed authorization

Scenario Steps
Customer places an Order
1. The merchant **authenticates** the transaction immediately for an estimated maximum amount that the basket can have obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization (see best practice below for additional considerations). Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.
2. The merchant must perform a zero-value **account verification** to check that the card is valid, and obtain an "initial" transaction ID. If the merchant requires fraud liability protection, they should not include the CAVV, so that it can be included later in the delayed financial authorization[24]. The merchant must also store the Transaction ID for this step. Issuers should not decline an account verification without a CAVV, with a response code of 1A (SCA required) in this scenario. If a token-based transaction, then the TAVV must be included in the account verification.
Customer increases order value to greater than the authenticated amount
3. 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 CTF TAVV (and associated ECI value), discarding the initial one and keeping this latest one. Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.   - The merchant may also optionally perform an additional zero-value *account verification* each time to check that the card is valid but if the merchant requires fraud liability protection, they should not include the CAVV, from the new authentication so that it can be included later in the authorization. If a token-based transaction, then a TAVV must be included in the account verification.
Merchant ready to make shipment (Customer no longer available)
4. At time of shipping, the order is closed. The merchant **authorizes** for the final amount. The authorization must include:

---

[24] Merchants who wish to, can include the CAVV in the account verification. However, such merchants must be aware of the implications of this approach, as described in Principle 1 of Section 4.2.3.3.

VISA

○   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 CAVV and associated ECI value from the latest authentication if this was not included in the account verification and / or any applicable exemption indicators.
  • 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 4.2.3.3, Principle 12.

5.   The merchant *clears* the transaction for the final amount.
Order Complete

Best Practice

If using this option, clearly communicate to the customer before the authentication step that:

- they are authenticated for a 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

If you have clearly communicated a maximum to your customer at the previous authentication you should authenticate again as soon as that maximum is neared or exceeded. If the customer's reasonable expectations are that the amount authentication could be exceeded, then you can authorize a higher amount within the customer's reasonable expectations (with an upper limit of a 15% variance between authenticated and authorized amount) (see Section 4.2.3, Principle 12)

5.4.3   Option 3: Process using MIT Unscheduled Subscription type (UCOF)[25]

A merchant with an agreement for open orders of this type may choose to process orders as Unscheduled Credential-on-File (UCOF) MITs. For further details see section **Error! Reference s ource not found. Error! Reference source not found.**.

---

[25] Visa reserves the right to revise this guide pending further regulatory developments as set out on page 4.

5.5 Aggregated Payments

Visa rules define an aggregated payment as a single Transaction that combines multiple purchases made by the same cardholder on the 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.

5.5.1 Option 1: Merchant sets up customer agreement to enable payments under MIT Unscheduled Subscription type (UCOF)[26]

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 no longer available for authentication when they are charged for the usage at the end of the day using an MIT UCOF. For further details see Section **Error! Reference source not found.**.

5.5.2 Option 2: Authentication for fraud liability protection

Scenario Steps
Customer makes purchase that triggers a new aggregation series
1. Merchant *informs* 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. Merchant *authenticates* for 15 USD (or local currency equivalent) obtaining a CAVV or CTF TAVV (and associated ECI value). Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.5.
3. Merchant performs a zero-value *account verification* to check that the card is valid and obtain an "initial" Transaction ID. If the merchant requires fraud liability protection, they should not include the CAVV, so that it can be included later in the delayed financial authorization[27]. The merchant must also store the Transaction ID for this step. Issuers should not decline an account

---

[26] Visa reserves the right to revise this guide pending further regulatory developments as set out on page 4.
[27] Merchants who wish to, can include the CAVV in the account verification. However, such merchants must be aware of the implications of this approach, as described in Principle 1 of Section 4.2.3.3.

verification without a CAVV, with a response code of 1A (SCA required) in this scenario. If a token-based transaction, then the TAVV must be included in the account verification.

Aggregated value or time threshold reached (Customer no longer available)

4. When either threshold is reached, the merchant ***authorizes*** for the final amount. The authorization must include:
    o 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)
    o The CAVV and associated ECI value from the authentication if this has not already been used in the account verification. Applicable exemption indicators should be populated.
• If the authorization is declined, as the goods and services have already been provided to the customer, the merchant may attempt to authorize again in the form of a resubmission, as described in Section 5.8 *Resubmission of declined authorization for service already delivered*.

5. The merchant ***clears*** the transaction for the full cumulative amount.

Customer makes purchase that triggers a new aggregation series
6. Restart from step 1

5.5.3   Option 3: Authorize for the maximum amount upfront, authenticate only if required by the Issuer

Whilst it is possible for an Issuer to immediately authorize for the full amount upfront, requesting a suitable SCA exemption and then only authenticating if required by the Issuer, and clear when the 15USD total is reached or at 7 calendar days, this is <u>not</u> 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.

5.6   Real-time service via mobile app with payment after service /completion

In these scenarios, the customer is paying for a service at end of service rendered. Examples include:

- Ordering a car ride via a mobile app
- Opening a fuel pump and buying fuel via a mobile app

In such cases, the amount can be estimated at the start, but the final amount is not known at time of order. Payment is not made on booking, but at service completion.

Note: Unscheduled Credential-on-File (UCOF) MITs are not suitable for this type of scenario, since it involves a merchant/cardholder interaction via the mobile app where authentication is possible.

The example scenarios assume that any variation between the original and final amount is within the customer's reasonable expectations. In the case where the final value of the transaction is outside of the customer's reasonable expectations then additional authentication and authorization may be needed. For more information on reasonable expectations see Section 4.2.3.3, Principle 14.

5.6.1   Option 1: Direct to authorization flow

In this Scenario, if an SCA exemption can be exercised then the Merchant can request it via the direct to authorization flow, in order to enable authentication to be by-passed, unless ultimately required by the Issuer.

Scenario Steps
Customer books service
1. Merchant *authorizes* for 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.) Using an estimated amount is only available to certain merchant types, such as taxis, hotels etc. See Visa Rule # 25596
2. If the transaction is approved, skip to step 3 or 4 as applicable. However, if the Issuer responds with a response code 1A – SCA required then the merchant performs *authentication* for the estimated amount then *authorizes* again, with the CAVV or CTF TAVV and associated ECI value. The estimated indicator must again be populated in the authorization
Final value of service not within reasonable expectations
3. If the final amount is above the customer's reasonable expectations (as described in Principle 14,) compared to the authorized amount, then the Merchant must: • *reverse* the authorization from step 1 or 2 • *authorize* for the final amount using applicable exemption flags in F34. If none possible or Issuer responds with a decline code 1A (SCA required) 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.
Final value of service within reasonable expectations
4. The merchant *clears* the transaction for the final amount (within reasonable customer expectations as described in Principle 14, Section 4.2.3.3). The final amount could include a tip, for example.
Order Complete

5.6.2   Option 2: Perform authentication every time

Scenario Steps
Customer books service
1. Merchant **authenticates** for highest estimated amount at ordering, obtaining a CAVV or CTF TAVV (and associated ECI value).

2. Merchant can either:
 	
    a. **authorise** for highest estimated amount at ordering. Merchant must use the estimated amount indicator (refer to Base I Technical Specification Volume 1 for further details.) Using an estimated amount is only available to certain merchant types, such as taxis, hotels etc. See Visa Rule # 25596, or;
    b. perform an **account verification** at time of ordering to check that the card is valid and obtain an "initial" transaction ID for use in the later authorization. If the merchant requires fraud liability protection, they should not include the CAVV, keeping it for later use in an **authorization** for the actual amount at time of service completion. The authorization must include:
        i.   A message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from the account verification (as per MIT framework)
        ii. The CAVV and associated ECI value from the authentication if this has not already been used in the account verification.
 	
In both cases, the CAVV can be included in the final authorization for fraud liability protection.

Final value of service not within reasonable expectations

3. If the final amount is above the customer's reasonable expectations (as described in Principle 14, Section 4.2.3.3) compared to the authorized amount, then the merchant must:
    • **reverse** the authorization from step 2
    • **authorize** for the final amount using applicable exemption flags in F34. CAVV from step 1 is no longer valid as not covering amount and should not be used in this authorization. If no exemption possible or Issuer responds with a decline code 1A (SCA required) 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 attempt another authorization.

Final value of service within reasonable expectations
4. The merchant **clears** the transaction for the final amount (within reasonable customer expectation).
Order Complete

5.7   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.**

5.7.1   Reserve on-line, pay in store

A customer could make an order via a website or mobile app but 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 transaction at time of collection to meet SCA requirements.

5.7.2   Buy online, pick up in store (BOPIS)

A customer could make an order via a website and complete authentication and authorization online (as per the one-time purchase scenario defined in Section 5.1).

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.

5.7.3   Pay in-app when in store

A customer could use 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 is performed, and therefore the transaction is treated as eCommerce, not face-to-face.

VISA

5.7.4   Pay in store for home delivery

A customer could purchase 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, meeting SCA requirements.

5.8   Resubmission of declined authorization for service already delivered

Resubmissions are a type of transaction whereby the merchant can re-submit a previously declined authorization due to lack of funds in the case where a service has already been delivered. The main use case for this is Mass Transit. For example, if a cardholder taps in to mass transit with their Visa card or token on a mobile device, but the end of day authorization is declined by the Issuer due to lack of funds, the Mass Transit merchant is allowed to resubmit the authorization after an agreed period of time to attempt to claim back the debt they are due for the transit service provided. In this case, the original CIT is exempt from SCA under the transit exemption and the resubmission is simply an attempt to complete that already exempted transaction, so no SCA data needs to be included in the resubmission.

The merchant must identify the resubmission as follows using the Transaction ID from the declined delayed authorization as the original Transaction ID.

Table 25: Resubmission

Description	Transaction Type	POS Entry Mode (PEM) (F22)	POS Environment (F126.13)	Message Reason Code (F126.13)	Transaction ID (F125**)
Resubmission	First Transaction (CIT)	Any valid* (10 if stored credential)	--	--	--
	Subsequent Transactions (MIT)	01 or 10 if stored credential	--	3901	Tran ID of First transaction

VISA

5.9 Establishing a new agreement for future MITs

In most cases, pending further regulatory guidance, SCA is required for establishing new agreements.

5.9.1 SCA is required by Merchant to set up new agreement

Scenario Steps
Customer Signs up to a new agreement for future merchant initiated payments
1. Merchant discloses to 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. Merchant should discuss with their Acquirers to be familiar with the rules associated with their MIT types. For more information, see Appendix A.4: Stored Credential Framework and Appendix A.6: Merchant Initiated Transaction Framework
2. Merchant *authenticates* for amount due immediately only as per Section 4.2.3.3, Principle 17, applying SCA.
3. Merchant *authorizes* for the amount due that day including CAVV and associated ECI value and stores the Transaction ID of this authorization for later use as the Initial Tran ID in future MITs[28]. If no amount due that day, authorize for zero amount as per Section 4.2.3.3, Principle 17. This first authorization is the CIT used to establish the agreement for future MITs and should be flagged as per the key data fields detailed in Table 15. If the authorization is approved, the payment credentials can be stored for future use according to the Stored Credential Framework (see Appendix A.4: Stored Credential Framework)[29]. If the credential is not stored under the SCF, 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. The merchant *authorizes* future MITs, identified as shown in Table 15.   The initial Tran ID to use is the one generated in step 3 unless grandfathering applies. 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. Any amount variance should not be a concern, as the transaction is an MIT and therefore is considered by Visa to be out of scope.   It is important for merchants to be aware, however, that MITs do not have fraud liability protection under the Visa Rules.

5.9.2 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, the initial transaction is a MOTO type transaction. When this is the

---

[28] If the agreement was established prior to 14th September 2019, then Grandfathering applies. See Section 4.2.3.3, Principle 5

[29] The credential must be stored according to the SCF for Standing Instruction MITs. For industry best practice, use of stored credential is optional.

case, it is important for merchants to remember that the subsequent payments made under that agreement are not to be flagged as MOTO. They are MITs:

- When an agreement is initiated via MOTO, this initial CIT is to be indicated as a MOTO and it is out of scope of PSD2, so SCA is not required.

- The ongoing transactions must be flagged with the appropriate MIT type (see Section 3.8) and not as a MOTO transaction. MITs are considered by Visa out of scope of PSD2, so SCA is not required.

> ### Key Point
>
> When setting up an MIT agreement, MOTO is only valid for the initial transaction when an agreement is established. Afterwards, the ongoing payment must not be identified as MOTO, but as an MIT.

5.9.3 Using a stored credential established by MOTO

A merchant may obtain a cardholder's credential for storage and future use via the MOTO channel. It is important for merchants to understand that any subsequent CITs using a stored credential established over MOTO must be flagged according to the circumstances of the current transaction. For example:

- When stored credential is established via MOTO, this initial CIT is to be indicated as a MOTO and it out of scope of PSD2, so SCA is not required.

- Any future CITs initiated using that stored credential must be flagged according to the channel over which that transaction is being performed. For example, if over the phone, the transaction can be flagged as MOTO and is out of scope; if initiated via the merchant website, it must be flagged as eCommerce and SCA, or a suitable exemption is required.

- If the credential is obtained for use in future MITs, refer to Section 5.9.2 above

The fact that a transaction uses a stored credential obtained via MOTO does not mean it can be considered a MOTO transaction for the purposes of SCA. Each transaction 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 obtained via MOTO is not necessarily a MOTO transaction.

5.9.4 Agreements established prior to PSD2 RTS for SCA coming into effect

If a merchant has an agreement in place prior to 14 September 2019 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 recognise 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 14 September 2019 so that it can be used as a proxy for the "initial Tran ID" for all future transactions using the MIT framework. This process is known as "grandfathering".

> ### Best Practice
>
> Merchants who intend to use grandfathering as a means of continuing agreements established prior to 14 September 2019 must plan in advance to capture the Transaction ID of an applicable transaction in the agreement series to use as a proxy for the initial CIT Transaction ID for all future transactions after the 14 September 2019.

5.10 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.

5.10.1 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 covered 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 # 0029844 and 0029267.

5.10.2 Customer driven agreement changes

Examples of customer driven changes to payment terms include:

- Changes to pricing or terms, such as

- o package (e.g. switch from premium to standard or vice versa)
- o change of billing cycle (e.g. from monthly to yearly)
- Pausing or stopping and then restarting a subscription, such as
  - o A subscription is paused by a customer to be restarted at an unknown later date
  - o 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".)
  - o 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 covered 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 establishing a new agreement described in Section **Error! Reference source not found.**.

5.11 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.

VISA

5.11.1 Installments

Installments are payments made in the case where the customer has already received the goods but have established and agreement to pay in installments over an agreed period.

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.

Scenario
Customer agrees installment plan
1. The merchant **sets up a new agreement** in accordance with the options in section 5.9 and using the Installment MIT type "I" in the authorization request.
Customer receives goods
2. Customer takes home goods having agreed to pay remaining balance by installments.
Merchant takes installment
3. The merchant[30] **authorizes** the amount based on the installment agreement and at pre-agreed time as an Installment MIT subsequent transaction (see Section 3.8).
Payment schedule complete

For more information on rules applicable to Installment, see Visa Rule ID # 0029267. Key highlights as of January 2019 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:

- 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

---

[30] It is possible that the merchant processing the installments with which the customer has an agreement and the merchant providing the goods could be different. See Section 0

5.11.2 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. 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

Several rules apply to recurring payments. For more information see Visa Rule ID # 0029844 and 0029267. Key highlights as of January 2019 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.
- 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.
- more than six months have elapsed since the previous transaction in the series

Scenario
Customer signs up for ongoing service or subscription
1. The merchant *sets up a new agreement* in accordance with the options in section 5.9 and using the Recurring MIT type. See additional requirements below
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. The merchant *authorizes* the amount based on the recurring payment agreement at the pre-agreed interval as a Recurring MIT subsequent transaction (see Table 15).
Customer ends agreement

At the same time as providing these notifications, the merchant must advise the Cardholder how to cancel the agreement with the merchant.

VISA

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 it 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

VISA

5.11.3 Signing up for services charged at irregular intervals (usage based)

This is the type of agreement where both the amount and time period between payments is variable and cannot be defined at time of agreement. Payment is usually triggered based on usage. 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 – 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 snow storm in winter months.
- aggregated payments using a stored payment credential (e.g. purchases from a mobile app store)

Scenario
Customer and merchant establish agreement
1. The merchant *sets up a new agreement* in accordance with the options in section 5.9 and using the UCOF MIT type.
Customer consumes goods or service
2. Customer receives goods or consumes service at any time. No further authentication or authorization is required.
Merchant ready to request payment
3. The merchant *authorizes* an amount based on agreed method of calculation in the agreement as a UCOF MIT subsequent transaction (see Table 15).

Several rules apply to Unscheduled Credential on File payments. For more information see Visa Rule ID # 0029844 and 0029267. Key highlights as of January 2019 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.

VISA

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

5.11.4 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

Scenario
Customer checks out and agrees to ongoing payments
1. 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. Applicable exemptions can be exercised which may result in this step being skipped, see Section 2.2. However, the merchant must be aware that if authentication is required for setting up the agreement, exemptions should not be used.

2. The merchant can either:
    a. Perform a single **authorization** for the full amount due that day (with CAVV and associated ECI value and / or applicable exemption indicators)
        • this authorization must be flagged 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.

b. Perform two separate *authorizations* and clear two transactions • one for the purchase (with CAVV and associated ECI value or applicable exemption indicators) and • one for the amount due today related to the agreement – this authorization must be flagged 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. If the transaction is performed with a token, each authorization must contain a separate TAVV.
Customer uses service
3. The merchant *authorizes* future MITs, identified as detailed in (see Table 15). 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.

5.12 Multi-party Commerce

Depending on the scenario, customer interactions could have one or more than one merchant.

5.12.1 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 3rd party credit provider.
- purchase both a mobile phone and a care contract for the phone in-store. The care contract is fulfilled by a 3rd party provider.
- purchase furniture in-store and pay for delivery and installation by a 3rd 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.

Therefore, the Visa authorization system allows the CIT and MIT to originate from different merchants (i.e. merchant descriptor and merchant ID can be different), as long as:

- the customer has been clearly informed who he is transacting with at time of CIT and which merchant he 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);

VISA

- there is a way to prove the relationship between the two merchants (e.g. T&Cs presented to 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 recognised payment model such as Payment Facilitator or Marketplace as defined below.

5.12.2 Marketplaces (single merchant)

As per Visa rule ID# 0030069, Visa define 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 of the sale.

For example:

- 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:
    - o Displayed prominently on the website or mobile application
    - o Displayed more prominently than the name and brands of retailers using the Marketplace
    - o 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.

5.12.3 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.

5.12.4 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 behalf.

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

From an SCA perspective, it is the end merchant that drives requests for authentication and authorization, not the referral service. The referral services is not involved in any way in the payment 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 3rd party agent. Alternatively, they could enhance their offering following the Marketplace construct to aggregate all the payments for their suppliers/retailers.

5.13 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
- Tip or 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 detail on how these industry specific scenarios should be process are provided in an addendum to this document titled "Implementing Strong Customer Authentication for Travel and Hospitality".

5.14 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.

5.14.1 Adding a card to a merchant account/customer profile

Customer requests addition of a card to a merchant account for future customer initiated purchases only. No financial transaction is performed at time of addition. For example, the customer is setting up payment details for a new account.

In this scenario, the payment details must be stored in accordance with the stored credential framework:

Scenario
Customer logs on to merchant and adds a payment credentials to their account
1. Merchant must *disclose* to the customer how the stored credential will be used. For more information about SCF and the requirements a merchant has to meet, see Appendix A.4: Stored Credential Framework.
2. Merchant must *obtain* cardholder consent. Refer to same appendix
3. SCA is required if there is a risk of fraud. A merchant may submit a non-payment *authentication* request to 3DS to confirm the customer's identity. This does not provide fraud liability protection.
4. Merchant must perform a zero value authorization, using indicators according to the SCF, informing the Issuer that the credential is being stored. Note: If a new card is added, go back to step 1
Customer makes future payment using stored credential
5. Future CITs using the stored credential must be *authenticated* unless a valid exemption applies.

When using a stored credential, a merchant must comply with the relevant disclosure, consent, cancellation procedure and processing rules (see Visa Rule ID # 0029267).

5.14.2 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
2. Merchant must *disclose* to the customer how the stored credential will be used. For more information about SCF and the requirements a merchant has to meet, see Appendix A.4: Stored Credential Framework.
3. Merchant must *obtain* cardholder consent.
4. As this is a financial transaction, *authentication* is required for the amount of the financial transaction unless an exemption applies. In addition, adding the card may require SCA if there is a risk of fraud.
5. Merchant submits an *authorization* for the transaction amount including the CAVV and associated ECI value and / or applicable exemption indicators and the appropriate identifier to indicate that a card is being stored according to the SCF. Merchants must be aware that if the transaction is declined, the credentials cannot be stored.
Customer makes future payment using stored credential
6. Future CITs using the stored credential must be *authenticated* unless a valid exemption applies.

For more information about SCF and the requirements a merchant has to meet, see Appendix A.4.

5.14.3 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 5.9.

5.14.4 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.

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.

VISA

5.14.5 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, then authentication is not required. However, SCA is recommended if the customer changes the card number (PAN or Token).

If only the expiry date is changed and the card number remains the same, authentication is not required.

5.14.6 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.

5.15 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 5.9.

5.16 Mass tokenising existing credential on file

For Bulk tokenisation, 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.

VISA

Section 6

Planning for PSD2 - what you need to do

6. Planning for PSD2 – what you need to do

Visa clients, merchants and other stakeholders need to plan and prepare for the enforcement of PSD2.

This section summarises the key decisions and actions that need to be taken by each stakeholder group and identifies the sections of the guide that provide more detailed guidance:

6.1   Issuer planning checklist

Issuers should ensure they have a PSD2-SCA plan in place that covers at least the following critical decisions and actions:

Table 26: Issuer planning checklist

1 Develop authentication and authorization strategies & policies		
1.1	Get up to speed	• Many transactions may not require Strong Customer Authentication. • So as not to unnecessarily disrupt the customer experience, familiarize yourself with your eligibility for exemptions, the out of scope criteria, and your local competent authority's guidance on the regulation.
1.2	Develop overall policies and systems for application of exemptions	• Develop risk management and exemption prioritisation policies that will minimise the application of SCA challenges for low risk transactions submitted to you for authentication, while maintaining fraud rates within target reference fraud rates and ensuring compliance with Visa rules on transaction abandonment. *For more guidance see section 4.*

1.3	Develop risk policies to optimise application of the TRA exemption	• Define the reference fraud rate band(s) which you intend to comply with in order to apply the exemption
		• Analyse your fraud and risk management data to identify transaction profiles/risk scores for which the exemption can be applied while maintaining fraud rate below the target reference fraud rate threshold
		• Work with your ACS vendor to configure your RBA engine
		• Monitor the effectiveness of your TRA exemption policy in terms of:
		  • Measured fraud rate
		  • Latency
		  • Transaction abandonment

VISA

		• Ensure you are meeting the fraud reporting and notification guidelines published by your local competent authority
1.4	Develop policies for selecting merchants that will qualify for the trusted beneficiaries exemption and evaluate solutions to implement trusted beneficiaries listing. Note: Issuers may choose not to support the trusted beneficiaries exemption.	• The trusted beneficiaries exemption will be beneficial for low risk/fraud merchants with regularly returning customers who are prepared to accept fraud liability under the Visa Rules. • It is recommended that Issuers develop a list of merchants who may be listed as trusted beneficiaries based on these criteria. • For more information on Visa's Trusted Listing solution please consult your Visa Account Executive.

1.5	Create your authorization logic and strategy	• There will be many transactions that will come in without a cryptogram and exemption (notably, out of scope transactions including MITs and one-leg out transactions). If you see this:
		  • First check to see if the transaction is out of scope of the regulation. If this is the case, follow normal authorization processing. (Note: do not use any SCA response codes.)
		  • Use and accept exemptions whenever possible. Your risk-based model will help you identify low risk transactions.
		• Note: If you receive an authorization without a cryptogram or an exemption request:
		  • First check to see if an exemption is applicable using a risk-based model such as Visa Advanced Authorization (e.g. low risk, low value) and apply that during the authorization.
		  • If it doesn't, consider responding with a 1A decline code requesting resubmission for authentication. (note: this should only be the case for a small number of transactions).

2 Ensure you have the latest technology in place to optimize for PSD2	
2.1	Plan to adopt RBA as early as possible.	• All Issuers who do not yet support RBA should consult their ACS vendor to agree on an implementation plan. • Any Issuer whose ACS is unable to offer RBA should consider alternative providers • Visa is able to offer Issuers additional risk management guidance and RBA services. Consult your Account Executive for more information
2.2	Plan to migrate to 3DS 2.2 by September 2019.	• All Issuers should support version 2.2 of the 3DS specification by September 2019 to ensure that exemptions can be fully supported. • Consult your ACS vendor to agree a migration schedule • Visa is able to offer an ACS capability to Issuers whose ACS vendor is unable to migrate them within an acceptable timescale

VISA

2.3	Ensure you can still support legacy 3DS 1.0	• Many merchants around the world will still be on 3DS 1.0. It is important to ensure you still support this version for the foreseeable future.

2.4	Develop an SCA roadmap	• Plan to support and migrate to SCA challenge methods that:
		  • Deliver the simplest user experience
		  • Minimise checkout friction
		  • Minimise security vulnerabilities
		  • Allow consumers to authenticate using technology they can access without reliance on mobile network coverage
		• Note Issuers may need to support more than one method to ensure full inclusivity

2.5	Issuers that use, or plan to use SMS OTP should ensure that they have auditable measures in place to mitigate known risks associated with SMS and should develop a roadmap to migrate customers to more secure authentication methods.	• Given the effectiveness of SMS OTP plus card data in mitigating fraud across Europe, a sudden replacement of this authentication method by September 2019 is both impracticable and potentially disruptive for European cardholders including those who do not own a smartphone. • Visa's position is that card data alongside another factor should be considered a valid SCA method provided a risk-based authentication approach is also taken because the layering of additional security and the generation of a secure cryptogram is sufficient to strengthen the overall solution to meet the requirements of SCA. Visa considers this to be a pragmatic and practical approach and is engaging with regulators on this. • Issuers should aim to migrate customers to more secure solutions including app-based biometrics and push messaging.
2.6	Develop a plan to offer a biometric authentication capability by April 2020.	• Consult your ACS or authentication vendor to develop a plan to adopt a biometric solution • Visa is also able to offer biometric solutions. See section 3.8 and consult your Visa Account Executive for more information
2.7	Provide accessibility options	• Ensure options are available to consumers who cannot or do not wish to use smartphones or other mobile devices • Ensure you can support multiple communication channels to your cardholders, such as WIFI, mobile and email, to minimize abandonment and disruption of service
2.8	Connect with your providers	• Ensure you are aligned with your ACS provider on your authentication strategy and customization • Ensure your processor will support the new PSD2 fields in the authorization message • Note: new fields will be available in April and Summer to be ready by Sep • Ensure your down-stream systems (e.g. fraud and monitoring) can support the new data elements

VISA

2.9	See how Visa can help you	• Visa has solutions that can help you optimize to get you moving quickly (e.g. Visa Advanced Authorization and Visa Risk Manager, Visa Trusted Listing, Visa Delegated Authentication, Visa Transaction Advisor, VCAS). • We will be releasing additional details in the guides, webinars, roadshows, etc. to support you

VISA

6.2 Acquirer planning checklist

Acquirers should ensure they have a PSD2-SCA plan in place that covers at least the following critical decisions and actions:

Table 27: Acquirer planning checklist

1 Develop authentication and authorization strategies & policies		

1.1	Develop policies and systems for application of exemptions	• Develop risk management and exemption prioritisation policies that will minimise the application of SCA challenges for low risk transactions while maintaining fraud rates within target reference fraud rates. *For more guidance see section 4.*
		• Exemption requests can be submitted through 3DS or direct to authorization
		   • Work with merchants to optimize strategies that will optimise user experience while minimising the risk of Issuers requesting resubmission for authentication
		   • Some Issuers want exemption requests to be sent in through 3DS. Identify those Issuers and refine your authorization strategies.

1.2	Develop risk policies to optimise application of the TRA exemption	• Define the reference fraud rate band(s) which you intend to comply with in order to apply the exemption
		• Analyse your fraud and risk management data to identify transaction profiles/risk scores for which the exemption can be applied while maintaining fraud rate below the target reference fraud rate threshold
		• Develop policies for selection of merchants for which you will offer to apply the TRA exemption taking account of:
		   • Merchant fraud rates and the impact on liability and fraud count
		   • Merchant ability to apply transaction risk monitoring and assessment
		• Monitor the effectiveness of your TRA exemption policy in terms of measured. This includes fraud rate
		• Ensure you are meeting the fraud reporting and notification guidelines published by your local competent authority

2 Educate and support your merchants		
2.1	Ensure all your merchants are enabled for 3DS	• Put in place a campaign to communicate the requirements of the PSD2 SCA regulation and the need to support 3DS in order to apply SCA • Ensure merchants understand the requirements on them including having a 3DS Server provider, supporting the SDK and providing data elements

VISA

2.2	Ensure your merchants understand the exemptions and the role they can play in optimising the application of exemptions	• Work with merchants with sophisticated risk assessment capabilities to outsource the application of TRA and optimization the application of the exemption • Ensure relevant merchants are aware of the potential of the trusted beneficiaries exemption and the need to educate their customers on enrollment
2.3	Ensure merchants who submit out of scope transactions are able to flag them	• Merchants submitting MITs will need to support the MIT framework
2.4	Ensure merchants are aware of the processing options and understand their obligations	• Proactively brief your merchant customers so that they understand the options available to them for applying exemptions and managing out of scope transactions via both 3DS and authorization flows
3 Ensure you and your merchants have the latest technology in place to optimize for PSD2		
3.1	Plan to migrate to supporting 3DS 2.2 between April and September 2019 to ensure merchants can fully benefit from SCA exemptions	• All Acquirers should support version 2.2 of the 3DS specification by September 2019 to ensure that exemptions can be fully supported. • Acquirers should guide their merchants to migrate to the latest version of 3DS in order to fully benefit from the support it provides in application of exemptions.
3.2	Ensure you support the latest authorization field values	• Make sure you have coded to the new authorization fields and keep development open to code late spring/summer for new ones ahead of September 2019 • If an Issuer responds with a value 1A, pass this to the gateway/merchant to have them trigger 3DS to retry the transaction • Ensure gateways are aware of the new fields • Look for abuse from merchants and monitor them / work with them

VISA

6.3   Merchant planning checklist

All merchants with EEA Acquirers that take card payments will need to ensure that they can support 3-D Secure 2.0 by September 2019. This includes merchants who have not previously used 3-D Secure. Key actions merchants need to take are as follows:

Table 28: Merchant planning checklist

Action		Applies to	How to
1	Plan to adopt or migrate to 3DS 2.2 between April and September 2019 to ensure you can fully benefit from SCA exemptions	All merchants	• See steps below for more detailed guidance on key steps
2	Implement a 3DS Server	All merchants	• If you already support 3-D Secure, consult your MPI vendor and/or payment service provider to agree an upgrade path to 3DS 2.0 • If your current MPI vendor is unable to offer a 3DS Server capability you will need to select a new vendor with a certified 3DS Server product. Consult the Visa 3-D Secure Vendor list • If you do not yet support 3-D Secure, you will need a 3DS Server vendor. If your e-commerce checkout functionality is hosted by a payment service provider on your behalf, you should consult your provider. • Visa is able to offer a 3DS Server capability to merchants and Acquirers
3	Ensure that mobile app-based checkouts support the 3DS 2.0 SDK	All merchants with mobile apps	• Consult the EMVCo 3-D Secure specification for more details on the SDK • Identify a certified 3DS SDK vendor
4	Ensure that you can provide all required data elements	All merchants	• Refer to section 3.3.7 and Appendix A.1 for more details on the data elements • Consult your 3DS server vendor or payment service provider to identify what action you need to take to ensure that data elements can be provided
5	Ensure that you can support the Visa MIT framework	All merchants with subscription or other MIT payment business models	• Refer to section 3.8 for more information on the MIT Framework and managing MITs • Ensure procedures/systems are in place as soon as possible to store the transaction ID of a previous CIT or MIT to benefit from grandfathering of existing customer

			agreements already in place prior to 14 September 2019 • Consult your Acquirer if required for additional detailed guidance
6	Work with your Acquirer to develop exemption strategies that respond to your business needs	Merchants who take a sophisticated approach to risk management and checkout user experience optimisation	• Consider whether you would benefit from your Acquirer applying the TRA exemption and/or the trusted beneficiaries exemption. • Agree with your Acquirer that they are prepared to apply the TRA exemption on your behalf and whether you will undertake • Refer to section 4.3.1 for more guidance on considerations to take into account
7	Plan to make use of the trusted beneficiaries exemption	Merchants with regular returning customers who are able to demonstrate a low fraud rate.	• Consider whether to participate in the Visa Trusted Listing programme (for more details refer to section 3.4) • Consider how to explain the benefits of trusted beneficiaries listing to your customers and encourage those whose Issuers support it to enrol you
8	Determine which version of 3DS 2.0 to support initially	All merchants	• All merchants should support 3DS version 2.1 or higher. Version 2.2 will be required to fully benefit from all exemptions • Merchants with more complex requirements should consider supporting at least version 2.1 initially and should plan to upgrade to 2.2 to take full advantage of the features it offers • See section 3.3.14 for more detailed guidance

VISA

Section 7

Bibliography

7. Bibliography

The following documents provide additional detailed guidance as described in the text of this guide.

Table 29: Bibliography

Document/Resource	Version/Date	Description
Preparing for PSD2 SCA	November 2018	A summary of the PSD2 SCA regulation, Visa's evolving interpretation of it and recommendations for optimizing SCA.
Implementing Strong Customer Authentication for Travel and Hospitality	February 2019	An addendum to this implementation guide whichprovides merchants and Acquirers with examples of performing SCA across common payment use cases common in the travel and hospitality sectors.
Merchant/Acquirer Implementation Guide for Visa's 3-D Secure 2.0 Program	V1.1 24th December 2017	The Merchant/Acquirer Implementation Guide for Visa's 3-D Secure 2.0 Program contains information about: • Visa's 3-D Secure (3DS) 2.0 Program • Program Rules • Implementation Details for a Merchant and Acquirer
Issuer Implementation Guide for Visa's 3-D Secure 2.0 Program	V1.2 15th October 2018	Contains detailed information for Issuers on: • Visa's 3-D Secure (3DS) 2.0 Program • Program Rules • Implementation Details for a merchant and Acquirer
VisaNet Business Enhancements Global Technical Letter and Implementation Guide.	TBA	TBA
Visa Technology Partner Portal	N/A	Portal with additional resources including details on 3DS 2.0 available at: https://technologypartner.visa.com/Library/3DSecure2.aspx
Visa 3DS 2.0 Performance Program Rules	VBN 25th October 2018	Summary of Visa requirements and rules on Issuers, Acquirers and merchants for implementation of 3DS 2.0

3DS Performance Rules FAQ		Summarises Visa Performance Program rules for Issuers and Acquirers
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/

Version 1.1
11 th March 2019

Appendices

A Appendices

A.1 Appendix 1 3DS 2.0 Data Elements

Merchants must provide the data elements in 3DS 2.0 authentication message as follows: 1) required always and 2) required if available. Merchants are also required to use the 3DS Method if the Method URL is provided by the Issuer. Providing 3DS 2.0 data is subject to regional and country regulations.

The merchant data has been categorized into seven groups.

Table 30: Transactional and checkout page information

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
3DS Method Completion Indicator	●		
3DS Requestor Authentication Indicator		●	
3DS Challenge Indicator	●		
3DS Requestor ID	●		
3DS Requestor Name	●		
3DS Requestor URL	●		
3DS Server Operator ID	●		
3DS Server Reference Number	●		
3DS Server Transaction ID	●		
3DS Server URL	●		
3RI Indicator		●	
Account Type		●	
Acquirer BIN	●		
Acquirer Merchant ID	●		
Address Match Indicator		●	
Broadcast Information		●	
Browser Accept Headers	●		
Browser IP Address		●	B

Browser Java Enabled	●		B
Browser Language	●		B
Browser Screen Color Depth	●		B
Browser Screen Height	●		B
Browser Screen Width	●		B
Browser Time Zone	●		B
Browser User-Agent	●		B
Card/Token Expiry Date	●		
Cardholder Account Identifier		●	
Cardholder Account Number	●		
Cardholder Billing Address City	●		
Cardholder Billing Address Country	●		
Cardholder Billing Address Line 1	●		
Cardholder Billing Address Line 2	●		
Cardholder Billing Address Line 3	●		
Cardholder Billing Address Postal Code	●		
Cardholder Billing Address State	●		
Cardholder Email Address	●		
Cardholder Home Phone Number		●	
Cardholder Mobile Phone Number		●	
Cardholder Name	●		
Cardholder Shipping Address City		●	
Cardholder Address Country		●	
Cardholder Shipping Address Line 1		●	
Cardholder Shipping Address Line 2		●	
Cardholder Shipping Address Postal Code		●	
Cardholder Shipping Address State		●	
Cardholder Work Phone Number		●	

Device Channel	●		
Device Rendering Options Supported	●		S
EMV Payment Token Indicator		●	
Installment Payment Data		●	
Merchant Category Code	●		
Merchant Country Code	●		
Merchant Name	●		
Message Category	●		
Message Extension		●	
Message Type	●		
Message Version Number	●		
Notification URL	●		
Purchase Amount	●		B
Purchase Currency	●		
Purchase Currency Exponent	●		
Purchase Date & Time	●		
Recurring Expiry		●	
Recurring Frequency		●	
SDK App ID	●		S
SDK Encrypted Data	●		S
SDK Ephemeral Public Key (Qc)	●		S
SDK Maximum Timeout	●		S
SDK Reference Number	●		S
SDK Transaction ID	●		S
Transaction Type	●		

VISA

For more information on 3DS Server Identifiers listed in the above table see section 4.2.2 of the Visa Acquirer and Merchant Implementation Guide for Visa's 3-D Secure 2.0 Program.

Table 31: 3DS Requestor authentication information

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
3DS Requestor Authentication Method	●		
3DS Requestor Authentication Timestamp		●	
3DS Requestor Authentication Data		●	

Table 32: 3DS Requestor prior transaction authentication information

Data Element (3DS Requestor Prior Transaction:)	Required Always	Required if Available	Browser only (B) or SDK only (S)
Reference		●	
Authentication Method		●	
Authentication Timestamp		●	
Authentication Data		●	

Table 33: Merchant risk indicator

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
Shipping Indicator		●	
Delivery Timeframe		●	
Delivery Email Address		●	
Reorder Items Indicator		●	
Pre-Order Purchase Indicator		●	
Pre-Order Date		●	
Gift Card Amount		●	

Gift Card Currency		●	
Gift Card Count		●	

Table 34: Cardholder account information

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
Cardholder Account Age Indicator		●	
Cardholder Account Date		●	
Cardholder Account Change Indicator		●	
Cardholder Account Change		●	
Cardholder Account Password Change Indicator		●	
Cardholder Account Password Change		●	
Shipping Address Usage Indicator		●	
Number of Transactions Day		●	
Number of Transactions Year		●	
Number of Provisioning Attempts Day		●	
Cardholder Account Purchase Count		●	
Suspicious Account Activity		●	
Shipping Name Indicator		●	
Payment Account Age Indicator		●	
Payment Account Age		●	

VISA

Device information (required for mobile app)

Device information must be provided if a mobile app is being used by the cardholder.

3DS Method

The merchant checkout page must load the ACS 3DS Method URL, if the 3DS Method URL is present, which allows the ACS to obtain additional browser information for risk-based decision making.

A.2 Appendix 2 Authorization Message Fields

Table 35: Visa Authorization messages, message values and how they are used.

Message Type	Message Response Data			
Message	Transaction Status	Transaction Status Description	ECI	CAVV
Authentication Request /Response (AReq/ARes) The 3DS Server[31] sends the AReq through the Visa DS to the Issuer ACS or Attempts ACS Upon receipt, the Issuer ACS or Attempts ACS performs risk-based authentication and provides the results of authentication to the 3DS Server in the Ares	Y	Authentication Successful	05	CAVV Present
	A	Attempts Processing Performed	06	
	N	Authentication Failed; Not Authenticated; Transaction Denied	07	No CAVV
	U	Authentication Could Not Be Performed; Technical or Other Problem		
	C	Challenge Required to authenticate the cardholder		
	R	Authentication Rejected		
Challenge Request/Response (CReq/CRes)	Y	Authentication Successful		Results of the challenge are sent in the Results Request (RReq) message by the ACS to the 3DS Server.

---

[31] A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa's 3DS 2.0 program authentication processing.

VISA

The 3DS Server (or 3DS SDK) sends the CReq to the Issuer ACS Upon receipt, the Issuer ACS challenges the cardholder through an authentication method such as OTP and responds to the 3DS Server or 3DS SDK with the Cres	N	Not Authenticated; Transaction Denied
Results Request/Response (RReq/RRes) The Issuer ACS sends the RReq to the 3DS Server to provide the results of the challenge authentication The 3DS Server acknowledges the RReq by responding with the RRes	Same set of values as AReq/Ares • A successful challenge is an ECI 05 with a CAVV • An unsuccessful challenge is an ECI 07 with no CAVV	

For more details on how these messages are used in the Frictionless and Challenges authentication flows, please refer to Visa Merchant/Acquirer Implementation Guide for Visa's 3-D Secure 2.0 Program section 1.4.

Flags may also be set in AReq message to indicate the application of exemptions. These are summarised in table 36 below.

VISA

Table 36: Flags Set in AReq Message to indicate the application of exemptions

3DS Field	Purpose	Value
Challenge Indicator Field Name: threeDSRequestorChallengeInd	Indicates whether a challenge is requested for this transaction. For example: • For 01-PA, a 3DS Requestor may have concerns about the transaction, and request a challenge. • For 02-NPA, a challenge may be necessary when adding	01 = No preference 02 = No challenge requested 03 = Challenge requested (3DS Requestor preference) 04 = Challenge requested (Mandate) 05 = No challenge requested (transactional risk analysis is already performed) 06 = No challenge requested (Data share only) 07 = No challenge requested (strong customer authentication is already performed) 08 = No challenge requested (utilise whitelist exemption if no challenge required) 09 = Challenge requested (whitelist prompt requested if challenge required)
3DS Requestor Authentication Indicator Field Name: threeDSRequestorAuthenticationInd	Indicates the type of Authentication request. This data element provides additional information to the ACS to determine the best approach for handing an authentication request.	01 = Payment transaction 02 = Recurring transaction 03 = Installment transaction 04 = Add card 05 = Maintain card 06 = Cardholder verification as part of EMV token ID&V 07–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) 80–99 = Reserved for DS use

VISA

A.3   Appendix 3 Rules detail

Table 37: Rules detail

Rule	Entity	Description / Thresholds	Impact	Enforcement	Effective Date
DECISIONING INTELLIGENCE					
Minimum Data Requirements	Merchant	All merchant data is required for 3DS 2.0 Two sub-categories of required: 1) required always; 2) required if data is available Merchants required to use 3DS method if provided by Issuer	Merchants may need to make enhancements to their checkout process to include additional data elements & support for the Issuer 3DS Method URL	DS will check for "required always" data elements and reject transactions with missing data	April 2019
RBA Enablement	Issuer	Issuer required to support RBA for 3DS 2.0	Issuers will need to develop RBA capabilities or engage an ACS provider who support RBA Several global ACS providers offer RBA capabilities	Transaction monitoring Standard non-compliance assessments may apply	October 2019 – CA, EU, LAC, US; April 2020 – CEMEA October 2020 - AP
USER EXPERIENCE					
Abandoned Transaction Threshold	Issuer	Cardholder authentication abandoned rate threshold of 5% on 3DS 2.0 transactions	3DS 1.0 abandonment rate in NA averaged 3.4% 3DS 1.0 abandonment rate for large US VCAS = 4.8%	Targeting Issuer early warning program to start 2Q 2019 Non-compliance assessments may apply starting month five	October 2019
Maximum latency for RBA	Issuer	Issuer must provide response to initial 3DS 2.0 authentication request within 5 seconds Only allow one Issuer ACS URL in DS Visa Attempts ACS URL will be loaded in the DS Attempts URL	The total weighted average median response time = 0.78 seconds The total weighted average response time = 0.83 seconds 5 NA ACS's average or median response time exceeded 4 seconds, representing: • 1.4% of the total ACS hosts • 0.05% of the total transactions	Visa will stand-in with an attempts response (ECI 06 & CAVV) Issuer retains fraud liability	October 2019
ACS Availability	Issuer	Issuer's ACS must be available 99% of the time	Issuers will need to ensure their ACS's are available 99% of the time	Transaction monitoring Standard non-compliance	October 2019

VISA

		Availability will be measured by: 1 – (# of AReq timeouts / total # of AReqs)		assessments may apply	
PROCESSING					
ECI Consistency (applies to both 3DS 1.0 & 3DS 2.0)	Merchant / Acquirer	For a 3DS transaction, an Acquirer / merchant must submit the same ECI value in clearing that was submitted in authorization Applies to 3DS 1.0 & 3DS 2.0	Acquirer must submit the same ECI value for 3DS transactions in both authorization and clearing to obtain fraud liability protection (i.e. ECI 05 or ECI 06)	Acquirer / merchant will not receive fraud liability protection	Effective Now

VISA

A.4   Appendix 4 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:

- Obtain cardholder consent through SCA for initial storage of credentials
- Utilize appropriate data values to inform the Issuer of consent and identify initial storage and usage of stored payment credentials

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 flagged accordingly.

Table 38: 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.

VISA

Figure 20: STIP SCA flowchart
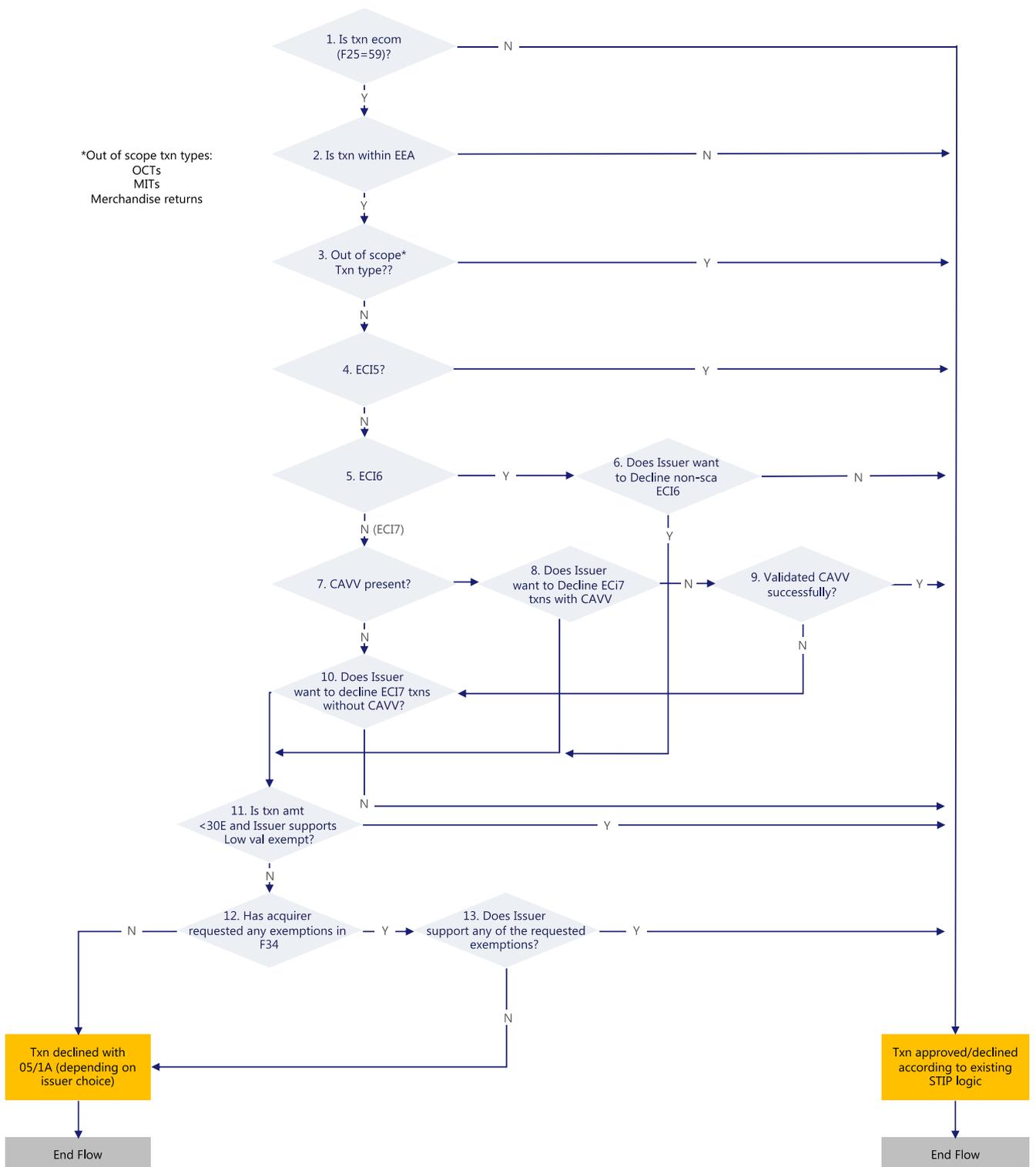
A.6   Appendix 6 Merchant Initiated Transactions

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 standing 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

Digital payment made via an app to purchase goods or order services at the customer's request, such as ordering a ride via an app or buying train tickets, are not MITs but are considered CITs as the cardholder actively participates in the transactions.

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.6.1   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
- Prepayment Transaction

A.6.2 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 represent 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	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.6.3 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.

VISA

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.6.4 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.6.5 Reauthorization Transaction—Message Reason Code 3903 in Field 63.3—Message Reason Code

Description	A merchant initiates a reauthorization when the completion or fulfillment 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 eCommerce retailers. A split shipment occurs when not all of the goods ordered are available for shipment at the time of purchase. If the fulfillment of the goods takes place after the authorization validity limit set by Visa, eCommerce 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 eCommerce retail, lodging, car rental, and cruise lines.
Examples	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in eCommerce retail, lodging, car rental, and cruise lines.

A.6.6 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.

VISA

A.6.7   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.6.8   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.6.9 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.6.10 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.

VISA

A.7 Appendix 7 EEA Countries in scope of PSD2 SCA

The countries below represent those participating in the European Economic Area and therefore subject to PSD 2 regulation

Table 39 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
GIBRALTAR GI 292	SLOVAKIA SK 703
GREECE GR 300	SLOVENIA SI 705
HUNGARY HU 348	SPAIN ES 724
ICELAND IS 352	SWEDEN SE 752
IRELAND IE 372	UNITED_KINGDOM GB 826