Visa Contactless and Card Present PSD2 SCA: A Guide to Implementation

September 2019

Version 2.0
September 2019

Contents

Important Information

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

As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This paper represents Visa's evolving thinking, but it should not be taken as a definitive position or considered as legal advice, and it is subject to change in light of competent authorities' guidance and clarifications. Visa reserves the right to revise this guide pending further regulatory developments. We encourage clients to contact Visa if they experience challenges due to conflicting guidance from local regulators. Where it makes sense, Visa will proactively engage with regulators to try and resolve such issues.

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

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

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

Note on Terminology: the term "Card Present" is used throughout this guide when referring to any electronic transaction that involves a physical payment terminal and a payment card account. This includes:

- Contact and contactless transactions
- Transactions made using cards and payment devices including mobile phones, wearables etc. that are associated with a card payment account
- Transactions at attended and unattended terminals.

Using the 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 6.

This guide covers card present and contactless payments initiated from Issuer provided payment credentials including cards, Issuer provided contactless wearables and mobile single Issuer wallets. The term card is used throughout this document to refer to the Issuer provided contactless payment credential regardless of form factor. Some solutions presented in this guide are only applicable to cards supporting both contact and contactless payments and these are clearly indicated by the text.

Whilst some of the principles covered in this guide are relevant, this guide does not cover Issuer payment credentials enabled by a third party such as tokenised mobile multi-Issuer wallets and third party provided tokenised wearables where consumer authentication is performed by the third party on behalf of the Issuer.

The guide is structured as follows:

Section	Title	Description
1	The requirements of PSD2 Strong Customer Authentication	A high-level summary of the requirements for SCA and the exemptions relevant to card present and contactless transactions as defined in the PSD2 Regulation and the RTS and Visa's interpretation of the requirements and exemptions
2	Visa's PSD2 Contactless Solutions	This section details the tools and services Visa is making available to merchants, Issuers and Acquirers to optimise the application of SCA and allowable exemptions, specifically; the Card Based and Issuer Host Based Solutions. The section also covers unattended terminals and STIP.
3	Guidelines for applying the exemptions and implementing Visa's solutions	Providing information and guidance to help clients to select and effectively implement the most appropriate solutions.

Section	Title	Description
4	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.
5	FAQs	Common questions and answers regarding the application of PSD2 SCA to card present and contactless transactions
6	Bibliography	A list of key additional reference documents.
7	Glossary	A glossary of technical terms used in the guide
A1	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:

Issuer
Merchant
Acquirer

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.

Audience

This guide is intended for anyone involved in the processing of card present and contactless EMV (cEMV) transactions in the Visa Europe region. This may include:

- Issuers, Merchants and their Acquirers and third-party agents and vendors looking for guidance on implementing point of sale 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

1 The requirements of PSD2 Strong Customer Authentication

This section provides a brief summary of Visa's interpretation of the PSD2 Strong Customer Authentication (SCA) requirements in the context of card present and contactless transactions.

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.

1.1 The application of SCA and use of factors

Regulated Payment Service Providers (PSPs) are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) and Acquirers (the payee's PSP). 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 or PIN
Possession	Something only the payer has	A preregistered mobile phone or card
Inherence	Something the payer is	A biometric (facial recognition, fingerprint, voice recognition, behavioural biometric)

Factors must be independent such that if one factor is compromised the reliability of the other factor is not compromised.[1] For card present one factor is always possession evidenced by the cryptogram. The other may be a knowledge or inherence factor, typically one of the example

[1] For more information on the application of factors please refer to Section 2.2 of the Visa paper *"Preparing for PSD2 SCA" November 2018.*

factors shown in Table 1, depending on the type and form factor of the payment credential used.

1.2 Exemptions

The main exemptions to the application of SCA relevant to Visa card present and contactless transactions are summarised below. It should be noted that not all exemptions are available to all PSPs. For more detail on how to practically apply the exemptions please refer to section 3.

1.2.1 Contactless payments at point of sale

SCA is not required for contactless payments at point of sale subject to the following conditions:

- The value of the transaction must not exceed €50; and either
- The cumulative monetary amount of consecutive contactless transactions without application of SCA must not exceed €150 (or the local currency equivalent for non-Euro Zone markets); or
- The number of consecutive contactless transactions since the last application of SCA must not exceed five.

Once the limit for the monetary amount or number of transactions without the application of SCA exceeds the selected limit, SCA must be applied and the count is reset to zero. The cumulative monetary amount and number of transaction limit is counted on the basis of transactions where this particular exemption was applied (i.e. not transactions where a different exemption was applied to avoid applying SCA).

Issuers can select whether to apply the transaction count or cumulative monetary amount limit. Visa recommends the cumulative monetary amount based approach to minimise the impact on customer experience.[2]

Visa's view is that contactless limits should be applied at device/token level rather than account level.[3]

1.2.2 Unattended transport and parking terminals

Article 12 of the SCA RTS states that PSPs shall be allowed not to apply SCA, subject to compliance with the general authentication requirements laid down in Article 2[4], where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

1.3 Out of scope transactions

The following transaction types are out of scope of SCA:

[2] For more information see Question 12 in the FAQ in Section 5

[3] For more information see Question 10 in the FAQ in Section 5

[4] Article 2 states that PSPs shall have transaction monitoring mechanism in place to detect unauthorised or fraudulent payments that take into account a defined set of minimum risk-based factors.

- **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[5]. 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.

These transactions are out of scope regardless of whether they are remote or card present.

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

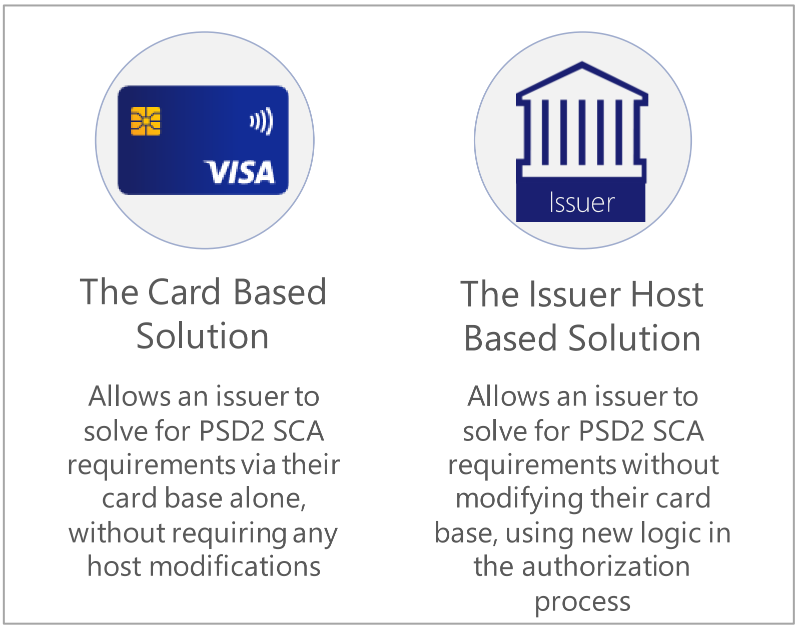
2 Visa's PSD2 Contactless Solutions

2.1 The Visa contactless solutions

Visa is offering two distinct primary solutions to enable Issuers to apply the contactless exemption for card present transactions and to apply SCA when it is required by the regulation. Each of the solutions offers slightly different benefits and implementing each solution implies different considerations. Issuers can select one or more of the solutions based upon their individual requirements. This section provides a summary of each solution along with guidance to Issuers on the points they should consider when deciding whether to adopt each option.

The primary solutions are summarised in Fig. 1 and described in more detail in sections 2.2 and 2.3 .

Fig. 1: Summary of the Visa Solutions



The Card Based Solution

Allows an issuer to solve for PSD2 SCA requirements via their card base alone, without requiring any host modifications

The Issuer Host Based Solution

Allows an issuer to solve for PSD2 SCA requirements without modifying their card base, using new logic in the authorization process

In addition to these two primary solutions, Visa is introducing new authorization message response codes. Stand In Processing (STIP) is also important to the application of PSD2 SCA and exemptions in a card present environment. These are covered, along with a summary of SCA options in sections2.4, 2.5 and 2.7.

2.2 The Visa Card Based Solution

2.2.1 Introduction to the Card Based Solution

The solution works on the basis of incorporating the logic required to track transaction count or cumulative monetary amount within the chip on the card. The solution is based on the Visa Contactless Payment Specification Version 2.2 Updates List 3 (VCPS2.2.3) specification whose key features are described below. It allows all of the logic required for application of the contactless payments exemption and of SCA, when required, to be executed in the card chip without the need to contact the Issuer host. The solution requires no upgrade to merchant terminals or Issuer host systems.

2.2.2 The VCPS 2.2.3 chip specification

2.2.2.1 Velocity parameters

The Visa Contactless Payment Specification Version 2.2 Updates List 3 (VCPS2.2.3) introduces two new velocity parameters to assist Issuers in meeting the requirements of the PSD2 regulation and to provide further risk management controls. These parameters are:

1. **Consecutive Transaction Counter – No CVM (CTC-NC) – "The Counter":** This parameter counts the number of consecutive transactions performed since the last successful CVM. It supports application of the transaction count limit.

2. **Cumulative Total Transaction Amount – No CVM (CTTA-NC)- "The Accumulator":** This parameter accumulates the total transaction amount spent on the card since the last successful CVM. It supports the application of the cumulative monetary amount limit.

An Issuer will decide which parameter it wishes to use as the basis for applying SCA. Guidance on selection of the parameter is given in section 3.4.1

2.2.2.2 Country list and currency parameters

In addition, the specification also supports the following parameters:

3. **Cardholder verification country list:** Issuers are required to define the cardholder verification country list. The specification allows configuration of up to 40 countries. This is required for both CTC-NC and CTTA-NC to determine whether the card is within scope of the requirement to apply SCA.

4. **Currency conversion:** The specification allows configuration of up to 20 currencies along with the exchange rate. This is only required if using CTTA-NC. The conversion rate used for determining whether SCA needs to be applied is not the same as the conversion rate used during clearing and settlement transactions. The rate used is a decision for Issuers – see section 3.2.5 below.

The specification also supports no CVM based Card Risk Management. This applies to:

- Transactions in scope of SCA checks (i.e. within the EEA country list defined)
- Both online and offline transactions without SCA

When the parameter limit that the Issuer has selected for the application of SCA (either 5 consecutive transactions or a cumulative limit of €150) is breached, a transaction will require application of Cardholder Verification Method (CVM).

2.2.2.3 Chip and signature support

The specification also has a configurable parameter for signature to allow for circumstances where an Issuer offers Chip and signature for the application of CVM, for example where it is offered to certain customers for inclusivity (for more details see FAQs Section 5 item 6 below) or in markets where it may be allowable. This parameter can be set by the Issuer during card personalisation. Where the parameter is set, the counter or accumulator will be reset for contact chip and signature transactions as well for Chip and PIN.

2.2.3 How the Card Based Solution works

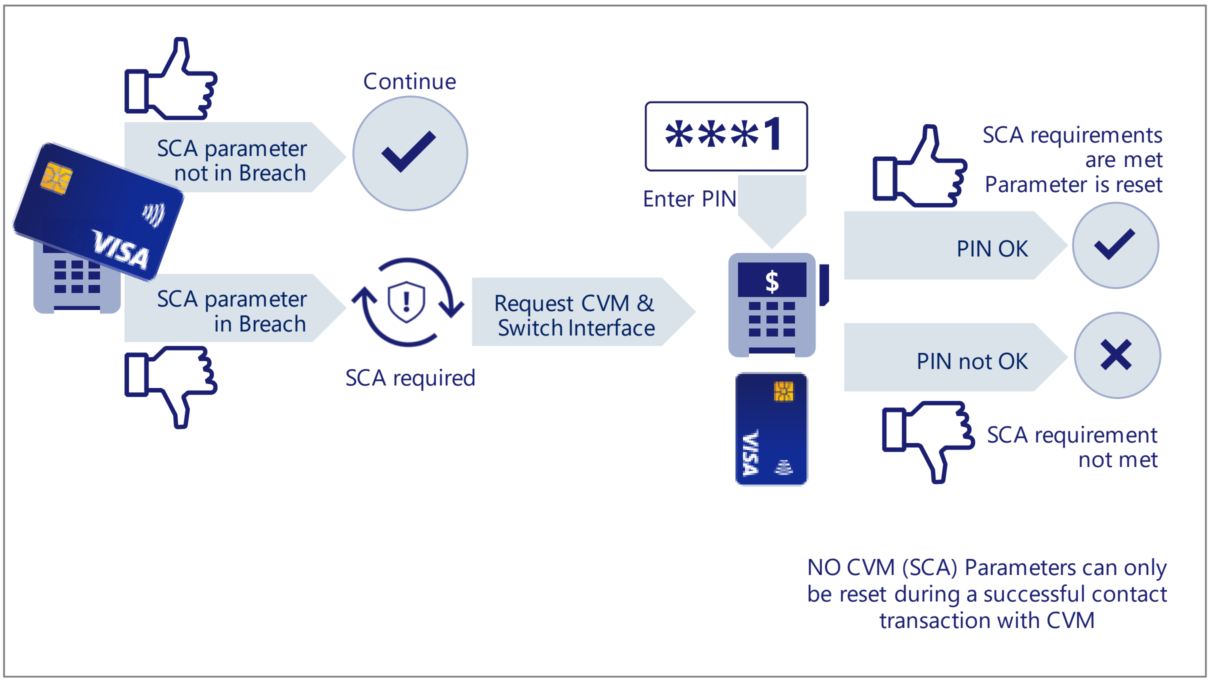
The transaction counter and amount parameters allow the chip on the card to:

- Track and a mass cumulative monetary amount and number of consecutive contactless transactions against the limits for transactions within the European Economic Area (EEA)
- Convert between multiple currencies for transactions that are within Europe, but outside the domestic currency of the issuing country
- Recognise when the pre-set transaction count or cumulative monetary amount threshold is reached and trigger the terminal to request a Chip and PIN transaction to authenticate the customer
- Reset the counters to zero when SCA has successfully been applied through CVM, either as a result of the pre-set contactless limit being reached or another PIN authenticated transaction taking place, such as a higher value Chip and PIN transaction on an ATM withdrawal

The process of incrementing and resetting the counters and accumulators on the card is referred to as Card Risk Management.

The transaction flow is illustrated in Fig 2 below.

Fig. 2: The Card Based Solution transaction flow



Continue
SCA parameter not in Breach
VISA
SCA parameter in Breach
SCA required
Request CVM & Switch Interface
***1
Enter PIN
$
SCA requirements are met Parameter is reset
PIN OK
PIN not OK
SCA requirement not met
NO CVM (SCA) Parameters can only be reset during a successful contact transaction with CVM

2.2.3.1 Incrementing the parameters

The transaction counter or accumulator is only incremented when a contactless transaction carried out without CVM is authorised and approved, either online or offline. This takes place via the contactless interface.

The counter and accumulator are not incremented when a transaction is declined, nor are they incremented when a zero-value transaction is carried out. This means that transactions processed through the mass transit model can be exempted. In this case, a contactless transaction performed at a qualifying unattended ticket gate or parking terminal has no effect on the counter or accumulator for a zero value transaction.

2.2.3.2 Resetting the transaction count and cumulative monetary amount parameters

- Any successful Chip and PIN transaction will reset the counters
- If the counters are breached, the transaction will switch interfaces and a successful transaction will reset the counters.

2.2.3.3 The transaction flow process

When a contactless transaction is attempted, the card chip checks the current status of the counter or accumulator No CVM parameters. If completing the transaction will not breach the transaction count or cumulative monetary amount limit, the transaction can be completed as a normal contactless transaction. If the limit will be breached, CVM needs to be applied.

Assuming a dual interface terminal, the transaction will continue, or switch interface as follows:

- In the case of an offline PIN transaction, if the card supports it, the terminal will switch to the contact interface and the application of CVM resets the counter and accumulator parameters to zero
- Contact transactions performed at terminals without a PIN entry capability will be sent online to the Issuer and if CVM is not applied, the parameters will not be reset.

For contactless transactions the contactless card specification does not permit this, so the transaction will be declined by the card, unless the terminal has contact capability. Note a transaction processed through the Mass Transit Model will not decline.

2.2.4 Benefits and considerations

The card-based solution offers the following benefits:

- The customer experience is as friction free as possible
- Merchant terminals are unaffected and do not need to be upgraded
- No changes need to be made to the Issuer host system
- No changes need to be made to Acquirer systems
- The solution is able to exclude exempt transactions including unattended transit terminals operating under the Visa Unattended Mass Transit Framework

However, implementation of the card-based solution requires that cards based on VCPS2.2.3 or higher are reissued to all customers.

2.2.5 When Issuers should consider adopting the solution

The Card Based Solution works well in offline PIN markets as follows:

- The solution works in markets with offline PIN support, where Issuers and cards are used to switching interfaces to Chip and PIN.
- The solution works best for offline PIN support, but could be used for online PIN markets, with consideration to customer experience.

2.3 Issuer Host Based Solution

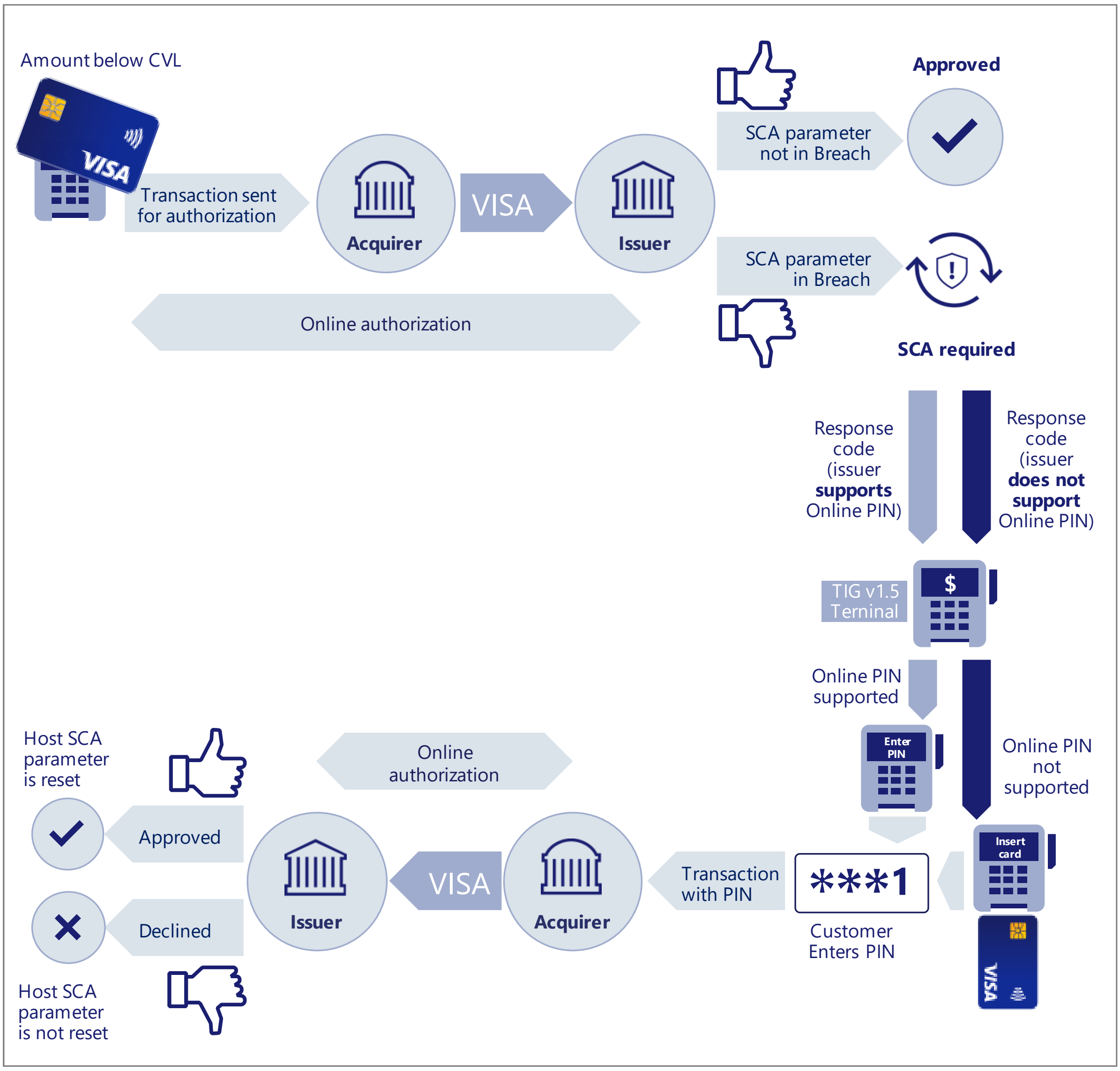
2.3.1 Introduction to the Issuer Host Based Solution

The Issuer Host Based Solution works by executing the logic required to track transaction count or cumulative monetary amount within the Issuer's host system rather than on the card chip. It therefore works for existing cards with no need to reissue and also works for mobiles and wearables. The solution is fully online, based on a contactless zero floor limit and provides the Issuer with the ability to adjust the parameter thresholds as required.

2.3.2 How the solution works

The solution utilises new authorization response codes to request SCA when needed. The transaction flow is summarised in Fig. 3 below:

Fig. 3: The Issuer Host Based Solution transaction flow



When a customer initiates a contactless transaction, the transaction is sent online to the Issuer for Authorization.

The Issuer tracks the number of transactions and the cumulative monetary amount with no cardholder verification based on receiving transaction authorization requests. The Issuer resets the counts every time a transaction with cardholder verification is performed (contact chip with offline or online PIN, contactless with online PIN or CD-CVM). When the Issuer host detects that the pre-set transaction count or cumulative monetary amount threshold has been reached, it returns the appropriate response code back to the merchant terminal.

The Issuer can respond with one of two new response codes depending on whether the Issuer supports online PIN:

- Response code 1A is used to switch interface to contact for offline PIN
- Response code 70 is used for online PIN

This is determined by which market the Issuer is in.

See section 2.4.1 for more information on the response codes. So long as the terminal is compliant with Terminal Implementation Guidelines v1.5 (TIG V1.5), it will recognise the code and prompt the customer to authenticate the transaction.

In markets that do support online PIN as a CVM, the cardholder, mobile and wearable user will just be invited to enter their PIN into the terminal. The Issuer has the choice to use Response code 70 or 1A, but Visa strongly recommends Issuers use Response code 70, as the customer experience is better.

In markets that don’t support online PIN as a CVM, the customer will be invited to insert their card to complete the payment using Chip and PIN. Once the customer has entered the PIN, the terminal returns the authorization message with the PIN to the Issuer for approval. Once the PIN is verified, and if the transaction is approved, the host based counter or amount accumulator resets to zero.

If the transaction is declined, the host SCA parameter is not reset.

2.3.3 Benefits and considerations

The Issuer Host Based Solution offers the following benefits:

- The customer experience is as friction free as possible
- There is no need for card reissuance – the system works with existing cards
- Exempt transactions at unattended transport or parking terminals can be readily supported
- It can improve credit and fraud risk as all in scope transactions are authorised online
- There is no requirement for the customer to either double tap or insert and enter PIN in on-line PIN supported countries

However, the implementation of the Issuer Host Based Solution requires:

- Issuer host authorization systems to be changed to:
    - Manage the SCA cumulative transaction count or cumulative monetary amount accumulator parameters
    - Support the new response codes to request the application of SCA when the selected parameter has been breached

- All in scope transactions need to be authorized online, requiring a zero floor limit across Europe. This will be implemented in October 2019.
- There is an additional authorization processing overhead for the Issuer for transactions that require SCA, but this can be minimised by selecting to use the cumulative monetary amount parameter rather than the transaction count.
- That PoS Terminals are TIG V1.5 compliant to ensure that the new response code is recognised. If a terminal is not upgraded, it will not recognise the response codes sent when SCA is required and the transaction will be declined.
- All Acquirers must support the new Response codes.
- Acquirers and merchants will need to cooperate in terminal upgrade programmes, to minimise potential declines and minimise friction in the customer experience.

2.3.4 Consumer experience considerations

The following table summarises how the customer experience of the Host Based Solution differs under different payment device and Online PIN vs. Offline PIN scenarios.

Table 2: Summary of Issuer Host Based customer SCA experience

Payment Device/ Environment – Contactless	Code used	Online PIN environment – Consumer experience	Offline PIN environment – Consumer experience
Card – Online PIN supported over contactless	70	Requests PIN	Changes interface to Chip
Card – No Online PIN over contactless	1A	Changes interface to Chip	Changes interface to Chip
Card – Chip & signature	1A	Changes interface to Chip	Changes interface to Chip
Mobile - Online PIN supported by Issuer AND device	70	Request PIN	N/A
Mobile – Non online PIN supported by Issuer OR device	1A	Ask to tap again with CDCVM required	Ask to tap again with CDCVM required
Wearable with online PIN	70 & 1A	Requests PIN	Decline

The TIG 1.5 terminal specification does allow the Issuer Host Based Solution to be used for a transaction initiated by a mobile device that does not support online PIN as a CVM method, however it should be noted that if the customer taps again without applying CDVCM the terminal will ask for the device to be tapped again and the customer may experience a “loop” of repeated requests to re tap.

2.3.5 When Issuers should consider adopting the solution

The Issuer Host Based Solution works well in:

- Online PIN markets
- Markets operating zero floor limits

2.4 Authentication and Authorization Message Codes

2.4.1 SCA Required Response Codes

SCA may be required if the applicable monetary amount or number of transactions limit has been exceeded.

The requirement to apply SCA will be communicated to the terminal by way of an appropriate response code as follows:

1. Response code 1A in Field 39 – a new response code that will be available to Issuers to indicate that the transaction cannot be approved until SCA is applied.
    a. Issuers may respond with 1A for both e-commerce and card present contactless point of sale (POS) transactions
    b. For contactless transactions, response code 1A should be used for offline PIN. The terminal will then switch interfaces to contact and request an offline PIN
    c. Issuers should not use response code 1A for One Leg Out transactions
2. Response code 70 in Field 39 should be used effective 3 June 2019, code 70 (PIN data required) that will allow Issuers that support online PINs to request SCA.
    a. The cardholder will then be prompted at the point-of-sale (POS) terminal to enter their PIN if the POS device supports online PIN.
    b. Response code 70 will result in the prior transaction, which triggered the response code, being resubmitted to the Issuer along with an online PIN.
    c. A POS device in an offline PIN country will treat a Response code 70 as a Response code 1A and will switch interface.

3. Response codes 70 is optional from 3 June 2019 and mandatory from 18 October 2019 for Acquirers (alongside 1A). Issuers are mandated to adopt the response code 1A for remote electronic transactions from 18 October 2019.

2.4.2 Terminal support of Response Codes

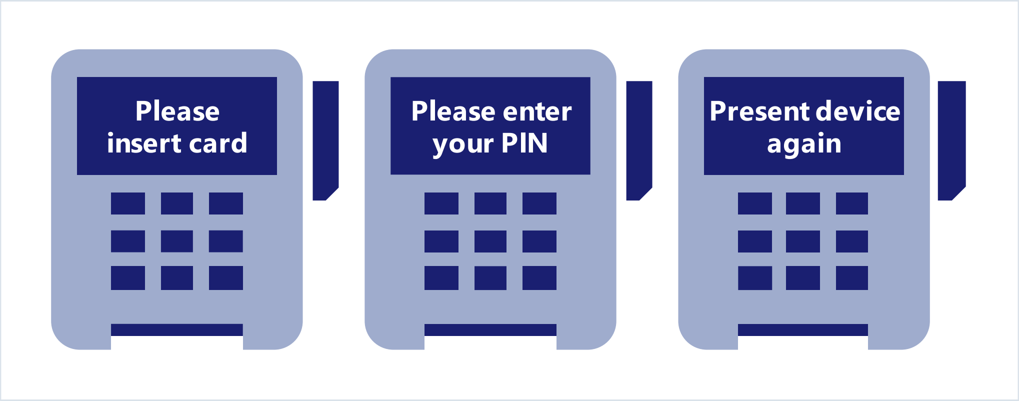
The Visa Europe Contactless Terminal Implementation Guide Version 1.5 (TIG V1.5) requires that the terminal is able to respond to the response code and display the appropriate cardholder prompt message[6].

2.5 Solutions for the application of SCA

The reader may, after the contactless tap and on receipt of the appropriate response code (see section 2.4.1 above), prompt the consumer to undergo SCA. In that case, specific instructions detailing the SCA action required by the POS system are displayed.

Depending on the outcome of the SCA logic, the reader may display a prompt for the cardholder to insert their card in the chip reader, the cardholder may be prompted to enter their PIN, or the cardholder may be prompted to tap their device again, depending on whether the Issuer supports online PIN or not, as per the screens shown in Fig. 5 below.

Fig. 5: Example cardholder prompts



2.5.1 Mobile and wearable authentication

For Visa contactless transactions conducted with a consumer device, such as a mobile phone, the reader may prompt the consumer to follow the instructions on the display of their device, for example when a consumer is required to enter a passcode into their mobile device.

2.5.2 Transaction Declines

If SCA has been requested by the Issuer and the POS system is not able to carry out the SCA, it should decline the transaction and present the cardholder with a “Not Authorised” message.

[6] For more details, please refer to the TIG V1.5 or above

2.6 Transactions at Unattended Terminals

Transactions undertaken at unattended transit and parking terminals, to which the unattended transit and parking terminals exemption applies, will be handled by the Visa contactless solutions as follows:

- Under the Card Based Solution, the card will not add to the No CVM count if it sees a zero amount transaction.
- Under the Issuer Host Based Solution, the transactions will be identified by the MCC codes.

Where the terminal does not have PIN entry capability and the unattended transit and parking terminal exemption does not apply and the SCA limit parameter is breached, there is the chance that some transactions may be declined.

2.7 Stand in Processing – STIP

Stand-in processing (STIP) occurs when Visa acts as a backup processor that approves or declines authorizations on behalf of an Issuer. The VisaNet Integrated Payment (V.I.P.) System determines when a transaction is eligible for STIP based on Issuer availability or participation in various Visa on-behalf-of services. When a transaction is routed to STIP, a series of Issuer-defined parameters and activity limits are used to determine how the transaction should be processed.

2.7.1 Strong Customer Authentication Parameters for STIP[7]

To ensure that STIP transactions support the PSD2 requirement to support Strong Customer Authentication (SCA), **effective with the April 2019 Business Enhancements release**, new SCA STIP parameters will be available for Issuers in the European Economic Area (EEA) in the following scenarios for contactless transactions:

Additional configuration options will be provided for PSD2 SCA STIP for contactless transactions, namely:

- Does the issuing BIN want to decline all unauthenticated contactless transactions in STIP when the Issuer is unavailable?
  - An authenticated contactless (F22.1=07/91) transaction is one where:
    - Offline PIN validation has been successfully performed or
    - Consumer device cardholder verification method (CDCVM) or
    - Online PIN is present in the request and can be validated by the V.I.P. System in STIP

The default value for the question above will be 'No', i.e. an unauthenticated contactless transaction will not be declined in STIP due to lack of SCA. Issuers that choose to participate in the SCA STIP options must submit the SCA Client Implementation Questionnaire (CIQ) to specify their SCA parameters for STIP. The questionnaire will be available to download from the Europe CIQ Forms page at Visa Online shortly.

Note:

[7] These requirements are defined in VBN: Changes to Stand-In Processing to Support Strong Customer Authentication Under PSD2 18th April 2019

Issuers can define the response code to be used in SCA STIP in answer to the question above:

- Declined with Response Code 05—Do Not Honour
- Response Code 70: To be used by Issuers from markets supporting online and offline PIN (and therefore online PIN at contactless)
- Response Code 1A: To be used by Issuers from offline PIN markets
- Approved with Response Code 00 (Note: This is the default if the Issuer does not use the STIP option as listed above.)

2.7.2 Scope of SCA / PSD2 for STIP Transactions

PSD2 requires that SCA be performed on transactions where both the Acquirer and Issuer are located in the EEA[8]. Issuers can define certain exemptions[9] to be used in SCA STIP.

SCA STIP is not required to be performed for Contactless transactions at an unattended terminal with the following merchant category codes (MCCs) for the purpose of paying a transport fare or a parking fee:

Transit and Parking MCCs

- MCC 4111—Local and Suburban Commuter Passenger Transportation, Including Ferries
- MCC 4112—Passenger Railways
- MCC 4131—Bus Lines
- MCC 4784—Tolls and Bridge Fees
- MCC 7523—Parking Lots, Parking Meters and Garages

[8] For a list of countries see Appendix A.1

[9] For more detail see section 1.2

3 Guidelines for applying the exemptions and implementing Visa's solutions

3.1 Selecting the optimum solution.

The solution that Issuers select will depend upon a number of factors including the market(s) they are operating in and the practical balance between the potential need to re-issue cards and upgrade merchant terminal and Issuer authorization host systems.

Each of the two solutions and the considerations to take into account is summarised in Table 3 below:

Table 3 Summary of the Visa solutions and considerations

	Card Based Solution	Issuer Host Based Solution
Benefits	• Apply SCA and exemptions for plastic cards in all market conditions in Europe. • No additional transaction processing. Card determines need for, and triggers, SCA (e.g. PIN) capture • Can also improve Issuer control of credit and fraud risk	• Apply SCA and exemptions without requiring re-issuance of card plastics. Existing cards work as usual. • Precise method of accounting for exempted transactions (e.g. unattended transport and parking). • Can improve Issuer control of credit and fraud risk. • Exchange rates can be applied dynamically
Considerations	• Card re-issuance can be expensive, especially within PSD2 timeframe • If parameters are breached, the solution always switches transactions to Chip & PIN to capture SCA • As such, this may hinder growth of contactless • Not suitable for mobile or wearables	• Requires Issuer host changes (new parameters and Response Codes) • Results in additional transaction processing where SCA is required
Dependencies	• Requires card re-issuance based on VCPS 2.2.3 or higher	• Requires all transactions to be processed online (e.g. zero floor limit) • Requires terminals to comply with TIG 1.5 to process new RC

		• Requires Issuer to support new host-based parameters and Response Codes

Issuers may consider adopting more than one solution for PSD2 compliance.

3.2 Implementing the Card Based Solution

3.2.1 Customer experience considerations

Issuers should understand the impact on the customer experience of switching to Chip and PIN when SCA is required. In markets supporting Online PIN, a change of interface is required under the Card Based Solution when SCA limit parameters are breached. It should also be noted that under the card based solution, the counters cannot be reset without using a contact interface.

3.2.2 Card reissuance

The most significant policy decision for Issuers considering implementing the Card Based Solution is the need for card reissuance. Visa recommends that:

- Issuers consider the opinions of local competent authorities in determining their card replacement strategy
- Issuers work with their card vendors ensure that all contactless cards issued after 14th September 2019 are based on VCPS 2.2.3 or higher
- Issuers may wish to consider forced reissuance where appropriate, especially for regular contactless card user customers

Visa is working with regulators to ensure that they are aware of the challenges and disadvantages of large scale forced card reissuance and to promote acceptance of pragmatic card replacement strategies that aim to minimise disruption to customers and fraud risk. Issuers should take their own legal advice and understand the view of their local competent authorities before finalising their strategy.

Visa’s position is that the cumulative counts or amounts requirements should apply, where applicable, to cards issued after the SCA rules enter into force, i.e. 14 September 2019, and that for existing cards in circulation, Issuers should have a card replacement programme in place to achieve compliance with the regulation over a reasonable time period. Issuers should work with their regulators on a smooth glide path. For further details, please refer to our “Preparing for PSD2 SCA” guidance issued in November 2018.

3.2.3 Setting personalisation criteria

Personalisation is managed through the VPA. Visa encourages Issuers to use the simplified profile selection approach within the VPA to take advantage of the predefined best practice personalisation settings and reduce the complexity of card set up for SCA. Refer to the Contactless Best Practice Risk Guide for further details.

The Issuer can set the options at card personalisation, to receive values of the on-card SCA parameters in the authorization request message, the Issuer then has the option to use this information in the authorization process.

3.2.4 Selection of the Velocity Parameters and resetting of counters

The Issuer may select whether to use the consecutive transaction counter parameter or the cumulative monetary amount parameter as the basis for triggering the application of SCA. Issuers may also set the value for which SCA is applied when the parameter is breached. This may be lower than the values defined by the PSD2 SCA RTS (5 consecutive transactions or a cumulative monetary amount of €150 since the last application of SCA), if the Issuer wishes to adopt a more cautious risk strategy.

Visa recommends that Issuers adopt the cumulative monetary amount parameter to minimise the impact of the application of SCA on the customer experience.

Issuers should note that for the Card Based Solution, when the limit is breached, the counter will only be reset if the contact interface is used. Going online and using the contactless interface will not reset the counter.

3.2.5 Setting currency conversion rate parameters

For the Card Based Solution, the conversion rate used is set at personalisation and therefore the rates used will be an approximation of the actual exchange rates at any point in time.

The rate used is a decision for Issuers. Issuers should check the policy of local competent authorities before determining which conversion rates should be used. Refer to the Contactless Best Practice Risk Guide for further details on setting the parameter.

It is possible to update currency conversion parameters via scripting, at the Issuer's discretion.

3.2.6 Contact and contactless interface selection and support of Chip and Signature

Parameters need to be set to ensure selection of the correct interface for application of SCA and resetting of counters. The card needs to be configured to switch to the contact interface in order to reset the counter when a PIN is entered correctly.

The VCPS 2.2.3 specification has a configurable parameter for signature to allow for circumstances where an Issuer offers Chip and signature for the application of CVM. Where the parameter is set, the counter or accumulator will be reset for contact chip and signature transactions as well for Chip and PIN. Please note that the counter will not be reset if the contactless interface is used.

Refer to the Contactless Best Practice Risk Guide for further details on setting these parameters.

3.2.7 Unattended terminals and application of the unattended transit terminals exemption

Issuers need to be aware that under the Card Based Solution:

- When the card is used at an unattended transit or parking terminal and the SCA parameter is breached:
  - If the transaction is zero value, the counter will not be incremented and SCA will not be requested.
  - The card will attempt to switch interface
  - If the terminal is unable to switch interface, then the transaction will be declined.

3.2.8 Availability of the solution

The VCPS 2.2.3 specification governing the solution was published in December 2018 and is now available. The Applet VSDC 2.9.1 required for producing the cards and the testing tools are available.

Visa expects to have products available for use by Issuers from May 2019.

VPA which is used for defining personalisation profiles and simplified profile selection will be updated for SCA related usage from May 2019

Issuers are encouraged to contact their card vendors for further updates.

3.2.9 Certification

Standard processes will apply for the certification of new VCPS 2.2.3 compliant cards. Visa is making tools available for Issuers to self-certify according to their own timescales. Issuers should contact the Visa Client Implementation team to initiate a certification project. Issuers who do not yet have Client Implementation Team contact should contact Visa customer services.

3.3 Implementing the Issuer Host Based Solution

3.3.1 Availability of the Solution

3.3.1.1 New Response Codes

The Response Code 1A is available in the VisaNet Integrated Payment (V.I.P) System as of April 2019. Acquirers and Issuers must be able to process this code (for remote as well as card present transactions) by October 2019. Processing of the code is optional from April 2019.

Response code 70 is effective from 3 June 2019.

Acquirers are Mandated to support response codes 1A and 70 across the EEA from October 2019. Issuers are mandated to support response code 1A for remote electronic transactions from October 2019

3.3.1.2 Contactless Terminal Requirements and Implementation Guide

The Contactless Terminal Implementation Guide version 1.5 (TIG 1.5) that defines the requirements on terminal to support the new response codes is available as of February 2019.

Acquirers & Merchants are already able to upgrade their terminals to ensure they comply

3.3.2 Use of the new response codes in field 39

3.3.2.1 Response code 1A

Response code 1A should be used by Issuers from offline PIN countries

3.3.2.2 Response code 70

Response code 70 should be used by Issuers from online PIN countries

The response code used is determined by whether the Issuer supports online PIN, not whether the transaction is undertaken in an online or off-line PIN market. The TIG 1.5 compliant terminal will respond appropriately.

Issuers should note that when using a Response code 70 to request CVM, the second authentication request submitted after CVM is applied will have the same chip data as the first, along with the CVM data (the PIN) and the transaction should not be declined.

3.3.2.3 Implementation of the response codes

The new response codes will be implemented through the standard scheme changes process.

Further detailed information on the response codes and their implementation is provided in the appropriate Visa technical letters[10].

3.3.3 Reliance on terminal upgrades

The Issuer Host Based Solution requires that all terminals are upgraded to comply with the TIG 1.5 specification. Acquirers and Merchants should ensure that terminals are upgraded in time, as transactions from non-compliant terminals that require SCA to be applied due to breaching of the cumulative velocity limit will be declined.

3.3.4 Use of the Issuer Host Based Solution outside the EEA

Issuers should not use these Response codes for transactions outside the EAA as they are likely to lead to declines.

3.3.5 Other Issuer implementation considerations

3.3.5.1 Not all transactions will be online

The Issuer Host Based Solution requires transactions to come online for authorization. While zero floor limits will apply on all countries from October 2019, not all transactions will come online. For example:

- Deferred authorization
- Merchant stand-in
- Some low value and transit

transactions will be authorized offline.

3.3.5.2 ATC checking processes

Where ATC checking processes are used a part of Risk management they need to be reviewed as:

- Transactions may be received out of sequence
- Two identical transactions may be received with the same chip data. The second transaction should include the PIN block and should not be declined as a duplicated transaction due to ATC checking rules.

3.3.5.3 Use of the Issuer Host Based Solution for Mobile and wearables

Issuers should also avoid using response code 1A for transactions initiated from wearable devices.

[10] Further details on Response Code 1A are provided in Global Technical Letter and Implementation Guides published October 2018: and April 2019 and July 2019 VisaNet Business Enhancements published March 2019. Details on response code 70 are included in Global Technical Letter and Implementation Guide Version 1 Published April 2019.

For mobile, and wearables, the terminal will need to use the Form Factor Indicator (FFI) to flag to the Issuer that the device is a mobile or wearable.

3.3.6 Terminal upgrade and certification process

Upgrading terminal software in line with the latest version of the TIG will constitute a significant change to the payment functionality. This will necessitate retesting of the terminal according to Visa's standard terminal testing processes. For the contactless interface this means testing with a VpTT (Visa payWave Test Tool) and submitting reports on the CCRT (Chip Compliance Reporting Tool) on VOL. No retesting of the contact interface should be necessary.

Queries relating to terminal testing should be addressed to: iTest@visa.com.

3.4 Optimising application of the contactless exemption

3.4.1 How to select which cumulative limit to apply (preference for value-based approach)

Visa recommends that Issuers use the cumulative amount-based limit rather than the count based limit as this will minimise the frequency with which SCA needs to be applied and minimise impact on customer experience.

In the case that the Issuer is using the host-based solution, selection of the cumulative monetary amount limit also reduces the authorization processing overhead.

3.5 Liability and disputes

There are no changes to liability for card present transactions as a result of PSD2.

3.6 Practical guidelines on applying the transport and parking exemption

Transport and parking transactions are identified from the following MCC codes:

- 4111 (Local and Suburban Commuter Passenger Transportation, including Ferries)
- 4112 (Passenger Railways)
- 4131 (Bus Lines)
- 4784 (Tolls and Bridge Fees)
- 7523 (Parking Lots, Parking Meters and Garages)

3.7 Practical guidelines for supporting non-card payment devices

When using a device (e.g. paying via a mobile phone or wearable device), Visa's view is that two-factors of authentication can be captured through Possession using the token cryptogram (requires prior device linking), and either Inherence using a biometric or Knowledge using a passcode, or online PIN (for markets that offer this functionality). This applies to all mobiles and wearables with a linked mobile application.

3.8 Education of Merchants and Consumers

Visa recommends that:

- Issuers put in place communications programmes to educate customers about the changes they can expect to the contactless transaction experience as a result of the PSD2 requirements for SCA and the reasons for these changes being implemented.
- Acquirers put in place communications programmes to educate merchants about the changes their customers will experience to the contactless transaction experience, so that they can effectively manage the transaction when CVM is requested for a contactless transaction.

4 Planning for PSD2 - what you need to do

Visa clients, merchants and other stakeholders need to plan and prepare for the application of SCA.

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:

4.1 Issuer planning checklist

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

Table 4 Issuer planning checklist

Solution Selection		
1.1	Select Visa solution to for managing the contactless exemption and application of SCA	• Review each of Visa solutions available and the benefits and considerations and guidance provided in this guide • Consider which solution or combination of solutions is the best fit for your market and for your portfolio •
1.2	Develop a plan for implementation of the solution(s)	This should include as appropriate: • Timings for implementation • Issuer host upgrades • Card procurement (VCPS2.23 complaint) • Card reissuance • For more details see below
Card Based Solution Implementation (if applicable)		
2.1	Contact your vendor for information on the availability of the VCPS2.2.3 compliant cards	• Your vendor should be able to advise on timescales • Put a certification project in place
2.2	Develop a plan for reissuance	• Which portfolios the Card Based Solution will apply to • Whether you are going to reissue based on the natural card replacement cycle or an adopt an accelerated programme
Issuer Host Based Solution Implementation (if applicable)		
3.1	Ensure that the new response codes will be supported in time	• Issuers will need to support Response code 1A for offline PIN markets and 70 for online PIN markets
3.2	Scope and plan the required changes to the host authorization	• Evaluate solutions and decide on whether to utilise this solution

	system to support the counter and accumulator parameter logic	• Build counts in Host systems • Review impacts of Article 12 in counts – Transit and Parking
Customer Communications		
5.1	Develop a customer communications plan	• Customers will need to be made aware that their contactless experience will change and why that is the case

4.2 Acquirer planning checklist

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

Infrastructure upgrade		
1.1	Develop a plan for upgrading terminal estate to TIG 1.5	• Issuers in many markets will adopt the Issuer Host Based Solution that requires terminal upgrade • Terminals in your own estate and those managed by ISVs, merchants and other third parties will need to be upgraded • Ensure that a certification project is in place
1.2	Ensure the new response codes are supported	• All Issuers and Acquirers need to support the new response codes (1A and 70) by Oct 2019 • Terminal retesting with VpTT will be needed.
Merchant Communication		
2.1	Develop a plan to prepare merchants for PSD2 and the application of SCA to contactless transactions	This should cover • The need and plans for terminal upgrades • The changes to the customer experience so that staff can be trained to deal with issues appropriately

4.3 Merchant planning checklist

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

Merchants with Acquirer owned terminal estate		
1.1	Familiarise yourself with the PSD2 requirement	• Read the relevant sections of this guide to understanding of the changes to card present and contactless transaction authentication that will take place to ensure compliance with PSD2
1.2	Contact your Acquirer for details on whether and when terminal upgrades will take place.	

Merchants with owned payment terminal estate		
2.1	Identify whether you will need to update your terminals to TIG 1.5	• Merchants in markets where Issuers are adopting the Host Based solution who own their terminals will need to ensure these terminals are updated to TIG 1.5 by Sept 2019
2.2	Develop a plan for terminal upgrades	• Work with your vendor to develop an upgrade and certification plan
All Merchants		
2.1	Train staff	Staff will need to be aware that customers making contactless transactions will be challenged to authenticate themselves on amore regular basis than to date. Staff should understand and be able to explain to customers why this is and that it is not due to a problem with the customer’s card, the payment terminal or processing systems.

5 FAQ

Question		Answer
1	What is the impact of PSD2 SCA regulation on contactless?	New regulatory requirements on Strong Customer Authentication (SCA) will make two-factor authentication a key requirement for the provision of electronic payment services. The new requirements are outlined in the final Regulatory Technical Standards (RTS) on Strong Customer Authentication and secure communications (published 27 November 2017), hereinafter "PSD2 SCA", which will apply from 14 September 2019[11].
2	What is Strong Customer Authentication?	Strong Customer Authentication (SCA) means an authentication based on the use of two or more elements categorised as: • Knowledge (something only the user knows), • Possession (something only the user possesses), and • Inherence (something only the user is), that are independent, in that the breach of one does not compromise the reliability of the other(s).
3	When does SCA apply?	Strong Customer Authentication should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction, or carries out an action through a remote channel which may imply a risk of payment fraud or other abuses. There are certain exceptions detailed in Chapter III of the RTS. The ones most relevant to card present transactions are: • Article 11 – Contactless Payments at Point of Sale • Article 12 – Unattended terminals for transport fares and parking fees. In addition, some transactions are out of scope of the SCA requirements. For more information refer to section 1 of this guide

[11] For further information, please refer to "Preparing for PSD2 SCA", November 2018.

Question		Answer
4	Do PSD2 SCA requirements apply to cards that are issued outside of the EEA (when purchasing in the EEA)? Does this requirement apply when EEA cardholders make purchases where the Acquirer is outside the EEA?	• A transaction from an EEA (the European Economic Area) issued card at an EEA acquired terminal is considered a "two-legged" transaction – and this is in-scope of the PSD2 regulation. • However, a transaction from an EEA issued card at a terminal acquired outside the EEA is considered a "one-legged" transaction – the EBA expects SCA to be applied on a 'best-effort' basis. • Also, a transaction from a non-EEA issued card at an EEA acquired terminal is considered a "one-legged" transaction –the EBA expects SCA to be applied on a 'best-effort' basis.
5	What countries does this apply to?	PSD2 legislation will apply to all countries within the European Economic Area.
6	Are Chip and Signature transactions compliant with PSD2 SCA?	Chip and paper-based signature is not an alternative to Chip & PIN for the purposes of SCA and should only be used for financial inclusion purposes, subject to local competent authorities' views. Visa will process transactions that are authenticated using Chip and signature, but the decision on whether to authorize these transactions should be made by the Issuer based on their risk strategy.
7	Are Magnetic Stripe and Signature transactions compliant with PSD2 SCA?	Magnetic stripe transactions are not compliant with SCA according to the EBA, even as a fall-back.
8	Is there a time limit regarding the 5 consecutive transactions or €150 cumulative contactless spend limits?	No. There is no time period.
9	Do all cards need to be compliant from 14th September 2019 or can we issue rollout on a replacement cycle only?	This is a matter for Issuers. However, Visa's position is that the cumulative counts or amounts requirements should apply, where applicable, to cards issued after the SCA rules enter into force, i.e. 14 September 2019, and that for existing cards in circulation, Issuers should have a card replacement programme in place to achieve compliance with the regulation over a reasonable time period. Issuers should work with their regulators on a smooth glide path. For further details, please refer to our "Preparing for PSD2 SCA" guidance issued in November 2018.

Question		Answer
10	Do the cumulative number of transactions and transaction amount limits apply to the Payment Account or Payment Device?	Visa's view is that contactless limits should be applied at device/token level rather than account level. If the limits were to be managed at the account level, this would not adequately take into account that the same payment card can be used as a plastic card or it can be registered in one or more digital/mobile wallet(s) and/or devices (e.g. smartwatches and wristbands). The application of the limits at account level implies that performing SCA on any device would reset the counter/accumulator. This would have the effect of allowing lost or stolen devices to be used if the owner is not aware of the loss and continues to use other devices and perform SCA.
11	Has an updated contactless risk guide been produced?	Yes, "Contactless Best Practice Risk Guide" issued in September 2018. Please contact your Account Executive for further details.
12	Does Visa recommend a value based or volume based count?	Visa recommends the value based approach to minimise the impact on customer experience. This recommendation reflects the fact that in markets with high levels of contactless usage, consumers now view contactless as a highly convenient way of making low value payments and often make multiple transactions in the course of a day. Fraud rates on contactless transactions are also very low, typically less than 2 basis points. Enforcing SCA via PIN entry every five transactions will be disruptive and inconvenient for consumers and will offer little benefit in terms of fraud reduction. Issuers may choose which metric to apply and SCA must be applied as soon as the selected metric is breached.
13	Does PSD2/SCA have any implications on liability?	PSD2 sets out regulatory liability rules. The current Visa rules around liability and disputes remain in place.
14	What solutions has Visa developed to support compliance with PDS2 SCA requirements?	Visa has designed the following solutions to provide choice for our clients in achieving compliance with PSD2 SCA requirements: • Card Based Solution - allows an Issuer to apply SCA or exemptions via their card base alone; • Issuer Host Based Solution - allows an Issuer to apply SCA or exemptions without modifying their card base, using new logic in the authorization process; and

Question		Answer
		These solutions have been developed to allow for authentication whilst providing minimum friction to the customer at the point of sale. All with the goal of maintaining the positive customer experience millions of cardholders expect from contactless payments. For more information see Section 2 of this guide
15	What are the new Parameters being introduced into the new card specification?	Visa Contactless Payment specification (v2.2.3) has introduced two new parameters namely • CTC- NC – A counter which counts the number of consecutive contactless transactions performed without CVM • CTTA – NC – An accumulator that accumulates the amount of contactless transaction without CVM.
16	How does the card handle different currencies?	The card can be personalised for 40 countries and 20 different currencies. The exchange rate is set at the time of the personalisation of the card.
17	When will the Card Based Solution be ready?	Updated "Visa Contactless Payment Specification", (v2.2 updates list 3) has been issued. The new applet (v2.9.1) has been developed, testing tools are being developed and will be available in spring 2019.
18	Does the Card Based Solution reflect Article 12 re the Transit transactions?	Any transaction that is processed with a zero value, such as transactions processed through the Mass Transit model, for example at London's tube gates, will not count towards the accumulator.
19	When will the Host Based Solution be available?	The "Contactless Terminal Requirements and Implementation Guide", version 1.5, and authorization messages to request for SCA, was published in February 2019. The general principal is that the Issuer counts the PSD2 SCA parameters in their own host. Once the SCA threshold is breached they can issue a response code that will indicate to the terminal that they wish to step up authentication (e.g. request a PIN transaction). For further information, please refer to Technical Guidelines.
20	What is Visa's view on Non Card Form Factors?	There is no general exemption from non-card form factors that do not support SCA. Behavioural biometrics may offer one way to support SCA. Transactions from non-card

Question		Answer
		form-factors, such as wearable devices, based on the Visa Contactless Payment Specification (VCPS), where CDCVM is not supported by the device, may also be able to perform SCA if the device and terminal support Online PIN.
21	Will STIP provide additional configuration to cater for PSD2 SCA?	Additional configuration options will be provided for PSD2 SCA STIP for contactless transactions, namely: • Does the issuing BIN want to decline all unauthenticated contactless transactions in STIP when the Issuer is unavailable? • Issuers can define the response code to be used in SCA STIP in answer to the question above: ◦ Declined with Response Code 05—Do Not Honor ◦ Response Code 70: To be used by Issuers from markets supporting online and offline PIN (and therefore online PIN at contactless) ◦ Response Code 1A: To be used by Issuers from offline PIN markets ◦ Approved with Response Code 00 (Note: This is the default if the Issuer does not use the STIP option as listed above.) • SCA STIP is not required to be performed for Contactless transactions at an unattended terminal with defined merchant category codes (MCCs) for the purpose of paying a transport fare or a parking fee For more information please refer to section 2.7.
22	Can the solutions for contactless and PSD2 SCA be combined?	The two solutions (Card Based and Issuer Host Based) can be combined in some cases to create additional value, and/or used in concert with other Visa services, such as Stand-In Processing (STIP), for example: • Issuers opting for a Card Based Solution may also implement Issuer Host Based accumulators which could operate in concert; • Regardless of the solution opted for, Issuers may choose to implement Visa Stand-In Processing.
23	If an Issuer chooses to go with the Card Based Solution, does it have to ensure that all card portfolios are upgraded and reissued by September 2019?	This is a matter for Issuers. However, Visa's position is that the cumulative transaction count or monetary amounts requirements should apply, where applicable, to cards issued after the SCA rules enter into force, i.e. 14 September 2019, and that for existing cards in circulation, Issuers should have a card replacement programme in place to achieve compliance with the regulation over a reasonable time period. Issuers should work with their regulators on a smooth glide path. For further details,

Question		Answer
		please refer to our “Preparing for PSD2 SCA” guidance issued in November 2018.
24	Will support be given to Acquirers to update terminals to TIG 1.5?	There is currently no mandate on updating to TIG 1.5, however Visa would like to see TIG1.5 adopted as widely as possible.
25	What Visa MCC’s are covered by the transit and unattended parking machine exemption	The following Visa MCC’s are relevant to the PSD2 Article 12 exemption: • 4111 (Local and Suburban Commuter Passenger Transportation, including Ferries) • 4112 (Passenger Railways) • 4131 (Bus Lines) • 4784 (Tolls and Bridge Fees) • 7523 (Parking Lots, Parking Meters and Garages)

6 Bibliography

No	Document/Resource	Version/Date	Type	Description
1	Authorization Changes to Support Strong Customer Authentication VBN ID: AI07809	31 May 2018	VBN	Authorization changes required to support PSD2 SCA
2	Update on Authorization Changes to Support PSD2 Strong Customer Authentication VBN ID: AI08011	16 August 2018	VBN	Updated authorization changes required to support PSD2 SCA
3	Europe Contactless Terminal Implementation Guidelines Updated to Support Compliance with SCA Requirements Under the PSD2, VBN ID: AI08745	16 August 2018	VBN	European contactless terminal guidelines on how to support PSD2 SCA requirements
4	Contactless Best Practice Risk Guide	September 2018	Guide	Best practice risk guide for contactless
5	Global Technical Letter and Implementation Guide	October 2018	Technical Letter	Providing details of Response Code 1A
6	Preparing for PSD2 SCA	November 2018	Guide	A summary of the PSD2 SCA regulation, Visa's evolving interpretation of it and recommendations for optimizing SCA.
7	Visa Contactless Payment Specification VERSION 2.2 Updates List 3 (VCPS 2.2.3)	December 2018	Specification	Specification for the card-based solution defining chip parameters

No	Document/Resource	Version/Date	Type	Description
8	Visa Card Based Solution Video	28 January 2019	Video	https://www.youtube.com/watch?v=BQvdddVaW9k&feature=youtu.be
9	Visa PSD2 Contactless Host Solution	28 January 2019	Video	https://www.youtube.com/watch?v=fB7EWLHvPvs&feature=youtu.be
10	Contactless and PSD2 SCA Q&As	February 2019	Guides	Series of Questions and Answers on contactless PSD2 SCA related questions
11	Contactless and PSD2 Webinar Presentations and Videos	February 2019	Guides	Video recording of contactless PSD2 SCA Visa webinars and presentations
12	Contactless Terminal Requirements and Implementation Guide Version 1.5 (TIG 1.5)	February 2019	Guide	. Specification of Visa contactless terminal requirements, incorporating SCA-related Response Code processing
13	Floor Limits Will Be Updated for Countries in the Europe Region Article ID AI08738	14 March 2019	Guide	Updated Europe region floor limits
14	Europe Contactless Terminal Implementation Guidelines Updated to Support Compliance with SCA Requirements Under the PSD2 Article ID AI08745	14 March 2019	Guide	Updated terminal guidelines to support PSD2 SCA requirements
15	Floor Limits Will Be Updated for Countries in the Europe Region, VBN ID: AI08738	14 March 2019	VBN	Floor limits update to changes to floor limits in multiple markets in the Europe region, effective 18 October 2019. Expanding zero floor limits to more countries in the Europe region providing Issuers better visibility into transaction counts and amounts, which are not transparent in an offline environment.

No	Document/Resource	Version/Date	Type	Description
16	April 2019 and July 2019 VisaNet Business Enhancements	March 2019	Technical Letter	Providing further detail and enhancements of Response Code 1A
17	PSD2 - Strong Customer Authentication (SCA) STIP, VBN ID AI08851	18 April 2019	VBN	Changes to Stand-In Processing (STIP) to support SCA under PSD2
18	Global Technical Letter and Implementation Guide, Version 1	April 2019	Technical Letter	Providing details of Response Code 70
19	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

7 Glossary

Term	Description
A	
Application Transaction Counter (ATC)	A counter within the application on a contact Chip or Contactless Card that tracks the number of times the Chip is read and that is used by the Issuer during the Authorization process.
C	
Card Present Transaction	Any electronic transaction that involves a physical payment terminal and a payment card account. This includes: • Contact and contactless transactions • Transactions made using cards and payment devices including mobile phones, wearables etc. that are associated with a card payment account • Transactions at attended and unattended terminals.
P	
PSD2	The Second European Payment Services Directive whose requirements include that Strong Customer Authentication is applied to all electronic payments within the European Economic Area (EEA). This requirement is effective as of 14th September 2019.
R	
Regulatory Technical Standards (RTS)	An RTS is a standard that is developed for the European Commission, by in the case of PSD2 SCA by the European Banking Authority (EBA), that is then the regulatory technical standards (RTS), which are then adopted by the Commission by means of a delegated act.

Term	Description
P	
Payment Service Provider (PSP)	In the context of PSD2, Regulated PSPs are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP).
S	
Strong Customer Authentication (SCA)	SCA, as defined by PSD2 Strong Customer Authentication Regulatory Technical Standards (RTS), requires that the payer is authenticated by a PSP through at least two factors, from the categories of knowledge, possession and inherence, each of which must be from a different category.
V	
Visa Payment Application (VPA)	A software application contained within a Chip or payment data encoded on a Magnetic Stripe that defines the parameters for processing a Visa Transaction and meets the minimum requirements of the Visa Program.

A Appendices

A.1 Appendix 1 Visa EEA Countries

The countries below represent those participating in the European Economic Area (EEA) and therefore subject to PSD2 regulation:

Table xx 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

Although not part of the European Economic Area (EEA), based on local law, strong customer authentication may apply to transactions in regions that are associated with countries within the EEA. Examples include micro-states and city-states in Europe, along with territories of EEA Countries outside of Europe. Clients in those regions should contact their local regulator and Visa representative to determine if SCA applies and if so how to comply and optimize.