Preparing for PSD2 SCA

November 2018

VISA everywhere you want to be

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. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required.

Note: 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.

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 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.

Contents

Each section in the document has been tagged with the symbols below to help readers quickly identify which are the most relevant to them:


ALL


ISSUER


MERCHANT


ACQUIRER

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 to 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 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.

Visa supports the PSD2 requirements for Strong Customer Authentication (SCA), and Visa's 3D-Secure (3DS) programme supports 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.

Topics for this paper include:

- A summary of PSD2 SCA Regulation
- Visa's vision for SCA
- How to optimize SCA
- Visa's view of other key SCA requirements

This paper represents Visa's evolving thinking on the interpretation and implementation of the PSD2 SCA requirements following extensive consultation with regulators, clients and other industry stakeholders. However, as PSD is a new regulatory framework, this paper does not reflect definitive positions and should not be relied upon as legal advice. 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.

2 Summary of PSD2 SCA Regulation

2.1 The mandate to apply Strong Customer Authentication

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 transaction risk is low. 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). These exemptions are summarised in Table 3 below. The specific rules on SCA come into force on 14th September 2019.

2.2 The Strong Customer Authentication definition

SCA requires that the payer is authenticated by a PSP through at least two factors, each of which must be from a different category as 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 provided it complies with the relevant SCA requirements)

Factors must be independent such that if one factor is compromised, the reliability of the other factor is not compromised. Table 2 summarises common factors and how they may be classified. It should be noted that the choice of factors to use is a decision for individual PSPs.

Table 2: Examples of Categorisation of Strong Customer Authentication Factors

Factor	Knowledge	Possession	Inherence
SMS One-time password (OTP)	√	√	X
Email One-time password (OTP)	√	X	X
*Card Number, Expiry Date and CVV**	*See footnote below*		
Other dynamically generated OTP (e.g. from a banking app or token)	√	√	X
Device ID	X	√	X
Card or device bound Token Cryptogram	X	√	X
Password or PIN	√	X	X
Bank User ID	X	X	X
Fingerprint***	*See footnote below*		
Facial Recognition***	*See footnote below*		
Voice Recognition***	*See footnote below*		
Behavioural Biometric** ***	*See footnote below*		

*Visa believes that card data used alongside another factor is an acceptable form of authentication provided it is used as part of a layered risk-based authentication approach; and that card data could be classified as either knowledge or possession. The use and benefits of Risk Based Authentication (RBA) are discussed in more detail in section 4.1.4.2.
**Provided it complies with the relevant SCA requirements.
*** In most implementations today, biometrics are performed on a user's own mobile phone or other electronic device. The mobile phone or device must be trusted by the Issuer by being associated with the payment user in a secure environment (and where performed remotely, the association of the device with the user must be performed using SCA). The phone or device will often have its own Token Cryptogram, because the device will have been previously tied to a payment card. The overall solution therefore fulfils both the possession and the inherence requirements.

Note: A single factor may be classified in two categories but may not be used on its own to satisfy the SCA requirement on the same transaction.

2.3 Other key requirements of the SCA rules

2.3.1 General authentication requirements

PSPs are also required to have effective transaction monitoring mechanisms in place, to detect unauthorised or fraudulent payment transactions. These mechanisms should allow capturing of the following information:

- lists of compromised or stolen authentication elements;
- the amount of each payment transaction;
- known fraud scenarios;
- signs of malware infection in any sessions of the authentication procedure;
- 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.

2.3.2 SCA exemptions

SCA exemptions are defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment. These exemptions allow PSPs to achieve the right balance between convenience of the payment experience and fraud reduction. The SCA exemptions are available only to PSPs. The SCA exemptions are not available to merchants, unregulated payment gateways or other unregulated entities. The Issuer retains the ability to take the ultimate decision on the application of the exemption.

Merchants should work with their acquirers to develop exemption strategies that respond to their business needs.

The key SCA exemptions are listed in Table 3 below and one only may be applied for each transaction by either the Issuer or the Acquirer.

Table 3: Summary of Exemptions from SCA

Exemption	Description	Conditions
Contactless payments at point of sale	SCA is not required subject to transaction value and velocity conditions	• The value of the transaction must not exceed €50; and • The cumulative limit of consecutive contactless transactions without application of SCA (PIN entry or Cardholder Card Verification Method (CDCVM)) must not exceed €150; or • The number of consecutive contactless transactions since the last application of SCA (PIN entry or CDCVM) must not exceed five
Unattended transport and parking terminals	Unattended terminals for transport fares (e.g. at transport gates) and parking fees	
Trusted beneficiaries	The payer may add a trusted merchant to a list of trusted beneficiaries held by their Issuer, completing an SCA challenge in the process, to prevent further SCA application on subsequent transactions with the trusted merchant	• The payer may add or remove the merchant to or from the Issuer managed list, or consent to the Issuer's suggestion to add a merchant • The Issuer may also remove a merchant from a list • Enrolment and amendment of the list requires SCA
Recurring transactions	Applies to a series of transactions of the same amount made to the same payee	• SCA must be applied when the series is set up, or to the first transaction in the series (if the first transaction is initiated by the payer)
Low value transactions	Remote transactions less than €30 do not require SCA so long as velocity limits are met	• The value of the transaction must not exceed €30; and • The cumulative limit of consecutive transactions without application of SCA must not exceed €100; or • The number of consecutive transactions since the last application of SCA must not exceed five
Secure corporate payments	Payments made through dedicated corporate processes and protocols (e.g. lodge cards, central travel accounts and virtual cards)	• Payment processes and protocols are only available to corporate payers and not individuals • Some competent authorities may need to confirm the dedicated corporate processes and protocols guarantee levels of security in line with the PSD2 requirements

<table>
<tr>
<td>Transaction Risk Analysis (TRA)</td>
<td>SCA is not mandated where a PSP, having in place effective risk analysis tools, assesses that the fraud risk associated with a remote payment transaction is low (when the requirements are met). The Issuer has the ultimate say on whether SCA needs to apply</td>
<td>

The value of the transaction is below €500
The risk analysis undertaken meets specific requirements
The Issuer or Acquirer applying the TRA exemption has fraud rates below the following defined limits:

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

2.3.3 Transactions out of scope of SCA

The payment card transactions listed in Table 4 are considered to be out of scope of the SCA mandate.

Table 4: Summary of Transactions that are Out of Scope of SCA

Transaction Type	Description
Payee or Merchant Initiated Transactions	A transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. Where the initial mandate is set up through a remote electronic channel, SCA is recommended if there is a risk of fraud but should not be necessary for subsequent payments initiated by the merchant. Applies to all payment instruments including cards
MOTO	Mail Order/Telephone Order transactions are out of scope
One leg out	A transaction where either the Issuer or Acquirer is located outside the EEA
Anonymous transactions	Transactions through anonymous payment instruments are not subject to the SCA mandate

3 Visa's Vision for Strong Customer Authentication

3.1 Visa's principles for SCA

Based on the core tenets the European Commission has detailed for PSD2 SCA, Visa has set out the following guiding principles for PSD2 SCA products, programs and compliance:

- Innovate to give consumers choice and control to make informed decisions

  Consumer-centricity has always been core to Visa's mission. The goal of PSD2 is to strengthen the security of consumer decision-making in payments and beyond. Visa will help facilitate trust and innovation between parties, and the ecosystem, so that consumers are empowered to confidently make decisions about their payments that are both secure and seamless. For example, Visa's new Trusted Listing solution for the application of the trusted beneficiaries exemption will give consumers a clear and simple way to select those trusted merchants that they are confident to pay without completing SCA; and Visa Biometrics will enable consumers to choose their preferred biometric (fingerprint, facial voice). These increased levels of security and control will directly benefit consumers by increasing their trust and confidence when purchasing online; by minimising disruption to the user experience where SCA is required (or by not needing to apply SCA); and by reducing the inconvenience and worry experienced as a result of payment fraud.

- Build trust and security into every payment experience

  It is crucial that we collaborate as an industry to reduce fraud by removing sensitive data in the payments ecosystem, encouraging dynamic forms of authentication, and deploying multiple layers of security with Machine Learning and Artificial Intelligence as foundational components to identify suspicious patterns.

- Expand access to data, while keeping it protected

  Visa is committed to facilitating proof of authentication between parties to enable the ecosystem to monitor performance, identify where improvement is needed, and grant visibility for auditors.

- Foster competition and innovation through open standards

  Harmonization promotes collaboration and participation that endeavours to address the needs of the ecosystem. Alignment from the industry drives down costs and barriers to entry, which in turn, enables a consistent experience across PSPs that benefits cardholders.

Solutions that build consumer confidence in security with minimal checkout friction will drive transaction volumes to the benefit of merchants, Issuers and Acquirers. At the same time, these solutions should minimise integration and operational overheads for all stakeholders. Visa aims to deliver these benefits across its authentication solutions portfolio.

3.2 Visa's focus for SCA

The execution of these principles falls under four primary categories:

1. Leadership: We are committed to working with the ecosystem to provide clarity around the regulations, and to deliver the optimum balance between security and convenience for our clients and our consumers. Additionally, we will partner with the ecosystem to prepare consumers for SCA to ensure a smooth transition when the regulation comes into force.
2. Products: Visa is building and evolving products and authorization messages to support clients in complying with the regulation without adding unnecessary friction to the payment experience.
3. Programs: Visa is designing programs and adjusting Visa Rules as needed to support the ecosystem to deliver a seamless SCA experience for consumers.
4. Compliance: Visa will support the ecosystem in providing proof and transparency between parties to monitor performance and support PSD2 compliance.

4 Visa's Recommendation on Optimizing SCA

4.1 When is SCA needed for your business?

This section builds on the above summary of the SCA regulation to provide more clarity on what this means in practice for our clients. To summarise, SCA will differ based on the electronic payment channel and method:

- Remote: SCA is applied to all remote payments unless an exemption is correctly applied or a transaction is considered to be out of scope of the SCA mandate (Refer to Section 2).
- Face-to-Face: SCA must be applied (unless an exemption is applied, or the transaction is out of scope) to a payment made in the face-to-face environment. This will usually be done through either of the following methods:
  - Chip and PIN: Considered to already be two-factor authenticated.
  - Contactless: Contactless transactions are considered exempt from SCA, provided certain parameters are met (Refer to Table 3).

4.1.1 When SCA is needed for electronic transactions

As discussed in Section 2, transactions such as MITs are considered to be out of scope for SCA. This section reviews Visa's position on the common use cases that fall under in-scope and out-of-scope transactions to clarify where SCA is needed in practice.

Electronic transactions can be classified in two categories:

1. Cardholder Initiated Transactions (CIT): cardholder is initiating the transaction.
2. Merchant Initiated Transactions (MIT): a transaction, or a series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once set up, allows the merchant to initiate subsequent payments from the card without any direct involvement of the cardholder.

Table 5 below summarises common use cases for both CIT and MIT transactions, and Visa's recommendation for SCA.

Table 5: Summary of Common CIT and MIT Use Cases

Transaction Type	Use Cases	Recommendation for SCA Requirement
Cardholder Initiated	One-time purchase (includes Card 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 recommended if the amount differs by more than a cardholder reasonably expects*
	Establish agreement for ongoing/future payments (e.g. subscription, no show)	Depending on the circumstances, SCA is recommended when the initial mandate is set up if there is a risk of fraud
Merchant Initiated	Merchant executes payment (e.g. subscriptions, no show)	Out of scope. SCA recommended on the set up of an ongoing subscription service if there is a risk of fraud
	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. VAT)	Not required as long as subsequent events can be linked to the initially authenticated authorization

*What is within 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.

Table 6 below summarises common use cases for non-payment actions, and Visa's recommendation for SCA.

Table 6: Summary of Common Non-Payment Use Cases

Action	Use Cases	Recommendation for SCA Requirement
Loading of Credentials	Adding a card-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 recommended
Card Validity Check	Check validity of PAN and expiry date	Not required when used only to check validity
Trusted Beneficiary	A merchant will send in an enrolment request to the Issuer to be added to a cardholder's trusted beneficiaries list	SCA required on the enrolment

4.1.2 When SCA is needed for contactless transactions

As discussed in Section 2, contactless transactions are exempt from the requirement to apply SCA, provided that the following conditions are met:

- The amount of the contactless transaction does not exceed EUR 50; and
- The cumulative amount of previous contactless transactions since the last application of SCA does not exceed EUR 150; or
- The number of consecutive contactless transactions initiated by the payer since the last application of SCA does not exceed five.

The following three approaches may be used to manage the application of SCA when it is required:

1. Provide proof of SCA on each transaction removing need to track amount and count on card: Contactless transactions can be initiated via either a device or card. If the combination of factors described in a. and b. below are used, Visa's view is that contactless transactions requiring SCA should be compliant with the regulatory requirements.

   The regulation outlines that 'Inherence' can be satisfied through the use of a biometric to identify the cardholder. The EBA has said that this can include behavioural biometrics which comply with the relevant requirements. Therefore:

   a. 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).

   b. When using a contactless card, two-factors of authentication can be captured through the card cryptogram coupled with either a behavioural biometric, or online PIN (for markets that offer this functionality). Visa is currently working to establish that real-time predictive models such as Visa Advanced Authorization (VAA) can qualify as a form of behavioural biometrics. VAA is able to identify cardholder behaviour compared to segment, geographic, and transactional normalities to identify unauthorised card use. This is subject to further regulatory guidance.

2. Card-Based Accumulators: Issuers may utilise the new SCA functionalities introduced in *Visa Contactless Payment Specification (VCPS) version 2.2.1* or higher, published in April 2018, to help manage compliance at card-level.

3. Host Accumulators: Issuers in markets operating zero floor limits for contactless may prefer to take a host-based approach with counters introduced in their authorization systems. When a cumulative limit is reached, the Issuer may return an Authorization Response Code indicating additional customer authentication required, which will trigger capture of SCA on terminals compliant with the *Terminal Requirements & Implementation Guidelines (TIG) version 1.4*, published in September 2018.

Issuers may wish to consider a 2-phase approach as follows:

1. Using Visa Advanced Authorization (VAA) real time risk scoring to risk assess transactions.
2. Consider adopting the card-based accumulator approach and introducing the capability progressively through the natural card replacement cycle.

Issuers should consider their policies and approach for application of SCA when contactless count or value limits are reached.

For clarity, "in app" payments using a mobile payment service are not considered as card present transactions (but are a remote electronic payment transaction), even if, for example, the payer and mobile device are physically on a payee's premises when the payment is made.

4.1.3 Changes to the Authorization Messages to Identify Transaction Classifications

We are enhancing our authorization message data to enable our clients to properly identify transactions to provide proof of SCA compliance between parties.

- MIT Framework: This framework, introduced in 2016, is a global standard to identify MITs, which are out of scope of the regulation. This includes requiring the initial authenticated CIT to be linked to subsequent MITs for increased visibility during disputes. If the MIT framework is not used, the Issuer will not be able to correctly identify the transaction and may incorrectly decline and request SCA even though the cardholder is not available. To avoid this experience, the MIT Framework needs to be implemented by the ecosystem.

Merchants with payment models that rely on Merchant Initiated Transactions and all Acquirers should plan to support the MIT framework to avoid transaction declines. Issuers must also ensure they can recognise these transactions and treat them out of scope. For more information on the MIT framework please contact Visa.

- Additional Customer Authentication Required response code: Issuers may use a new Response Code to indicate to the Acquirer that a transaction cannot be approved until SCA is performed.

- Exemption Requests: Visa Issuers and Acquirers will have access to new technology to communicate exemption requests. Exemptions which an Acquirer has a right to apply may be communicated to the Issuer by means of a flag at either authorization or at authentication using 3DS 2.0.

Issuers and Acquirers should start to develop policies and systems for application of exemptions. If you require more guidance please contact your Visa Account Executive.

  - Authorization request: New indicators in the authorization request will be used by Issuers to identify Acquirer-requested exemption requests. If an Acquirer would like to request an exemption but does not flag this in the authorization request, they are likely to receive an 'additional customer authentication required' response 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.

  - 3DS 2.0: An Acquirer may request an exemption via an exemption flag in the 3DS 2.0 protocol. The Acquirer would also have to submit the exemption request with the cryptogram in the authorization request, to be able to link it to the authentication flow. The Issuer may be more likely to approve the transaction, as they will have additional authentication data to identify the cardholder when making their authorization decisions. Additionally, if the Issuer does not accept the exemption request, they can continue immediately with SCA without the risk of additional latency caused by requesting a resubmission via 3DS.

4.1.4 Products and Programs to Optimize SCA

Visa is continuing to build and evolve a suite of products and programs that will enable secure and seamless electronic experiences for consumers while enhancing security.

Visa's core products will be the foundation of new innovative solutions to support SCA compliance. These products include:

- 3-D Secure (3DS): This is an industry protocol that provides the default mechanism for performing strong authentication.
- Predictive Analytics: Visa's real-time predictive modelling technology leverages Visa's global view of payment and fraud data. Our suite of predictive models can be deployed as foundational layers of security to quickly identify when authentication is needed, and to reduce fraud in the ecosystem.
- Tokenization: The Visa Token Service (VTS) enhances security for card payments by: 1) limiting them to a particular device, merchant, transaction type or channel and 2) strongly linking the cardholder and their consumer device and/or merchant account. This provides a strong foundation for PSD2 compliant authentication solutions across multiple use payment cases and platforms.

The following sections give an overview of products and programs that Visa is building and evolving to support the ecosystem's PSD2 SCA readiness.

4.1.4.1 3DS 2.0

Visa's new 3D Secure 2.0 (3DS 2.0) authentication protocol will provide the platform for a new suite of identity and risk solutions all designed to offer a high level of security, support compliance with the SCA requirements and deliver a superior customer purchasing experience.

3DS 2.0 is a fundamental upgrade of the global standard for card 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. This is known as frictionless authentication.
- 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.

4.1.4.2 Risk Based Authentication

Risk Based Authentication has already delivered significant benefits in the markets where it has been deployed. Today, in a UK pre-PSD2 environment, 95%[1] 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 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".

Visa is taking steps 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. Details will be published in Visa's 3-D Secure 2.0 Programme Implementation Guides.

4.1.4.3 Visa Consumer Authentication Service (VCAS)

Visa Consumer Authentication Service (VCAS) is a data-driven hosted 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, while providing enhanced levels of security. To deliver this, VCAS assesses the risk of a transaction in real-time using predictive risk analysis based on enhanced inputs, including device and transaction information and behaviours. This network-wide level of intelligence gives Issuers the ability to decide if and when to apply SCA 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.

[1] Source Visa Risk based authentication case study

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

The VCAS solution has been built in partnership with CardinalCommerce, an industry leader in digital payment authentication that is fully owned by Visa. VCAS will fully support 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.

4.1.4.4 Visa Biometrics

Visa is developing biometric capabilities to provide a consumer-friendly alternative to one-time-passwords at checkout, if 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.

4.1.4.5 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. During checkout, consumers will be asked if they'd like to add a merchant to their trusted list. Once SCA has been completed, the merchant will 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 not require the additional authentication of 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.

If a merchant and its Acquirer participate in Trusted Listing and choose to send the trusted beneficiaries exemption flag, under Visa's Rules, the Issuer will retain chargeback rights, just as they do today, since SCA is not performed on the transaction. If a merchant or Acquirer would like liability protection, they can choose to submit a 3DS authentication request to the Issuer who can then decide to perform SCA or apply an exemption.

4.1.4.6 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 either 3DS or an API.

As a general principle in the Visa Rules, the entity that applies the exemption takes the liability for any resulting fraud. If the Acquirer decides to apply the TRA exemption but the Issuer overrides it and applies an SCA challenge, then under the Visa Rules, the Issuer assumes liability for any resulting fraud.

4.1.4.7 Visa Delegated Authority

The PSD2 regulation allows an Issuer to 'delegate authority' for authentication to a third-party (e.g. wallet provider, merchant). Visa is establishing a Delegated Authority Program whereby clients and third-parties can choose to allow Visa to manage this delegation process.

4.1.4.8 Visa Checkout and Visa Secure Remote Commerce

Visa Checkout (VCO) is an online multi-merchant service that simplifies and streamlines the checkout experience by removing the need for consumers to enter payment and shipping details each time they make a purchase. VCO enhances consumer confidence and trust by displaying card art, increases sales conversion, lowers fraud and works seamlessly with the merchant's existing payment infrastructure.

Visa Secure Remote Commerce (SRC) is an evolution of VCO that leverages Visa tokens for security and harmonises checkout solutions across card payment brands. This has the additional benefits of reducing payment button proliferation, providing greater consistency and confidence for consumers and easier implementations for merchants.

Visa SRC can be configured on a merchant level to achieve the optimum checkout flow. Pre-transaction risk scoring, sanctions screening and contextual consumer authentication can all be used to address the fraud dynamics of the merchant's business to deliver a best in class customer experience. Visa SRC complements the Visa Delegated Authority Program, 3DS and Trusted Listing, enabling merchants to provide their customers with the best possible experience every time they shop.

5 Other key SCA requirements

5.1 The Support and Application of 3D-Secure 1.0 and 2.0

All EEA issuers should plan to migrate to 3DS 2.0 by September 2019.

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. 3DS 2.0 will be deployed across Europe from the end of 2018 and through 2019. The benefits of 3DS 2.0 are summarised in section 4.1.4.

To take advantage of the new services mentioned in Section 4, clients will need to upgrade to 3DS 2.0 by September 2019.

Issuers should plan to adopt RBA as early as possible. Contact your ACS vendor or Visa Account Executive for more guidance.

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. Visa recognises that PSPs may wish to upgrade over time, and Visa recommends that in the meantime, 3DS 1.0 is used with a layered risk-based authentication approach as they move towards 3DS 2.0. Under such an approach, issuers should look to implement RBA as early as possible before upgrading to 3DS 2.0. Issuers should consult their ACS vendor to support and plan for this. Visa is also able to offer an RBA solution that supports both 3DS1.0 and 2.0 (see section 4.1.4.2 for more details) and Issuers who are interested in taking advantage of this should ask their Visa Account Executive for more information.

EEA Acquirers and merchants should be planning to migrate to 3DS 2.0 between April and September 2019 to ensure they can fully benefit from SCA exemptions.

It should be noted that from April 2019, a merchant that has upgraded to 3DS 2.0 will obtain liability protection for an attempted 3DS 2.0 transaction under the Visa Rules if the Issuer does not support 3DS 2.0.

5.2 Dynamic Linking

For remote payment (i.e. online) transactions, where SCA is applied, the payer has to be presented with both the amount of the transaction and the identity of the payee when the payer authenticates the purchase. An authentication code must be generated to link these details to the transaction. The code itself does not need to be visible to the cardholder.

Visa's programmes such as 3DS, Tokenization, and EMV Chip, deliver an authentication code which can link these details 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.

5.3 Specific Strong Authentication Methods

5.3.1 SMS One Time Passwords (OTP)

Visa takes the view that 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.
2. Where SMS OTP is used alongside card data, a "layered" risk-based authentication approach must be deployed (see section 4.1.4.2 for more details).
3. As biometrics are progressively introduced, these will reinforce SCA methods going forward and replace SMS OTP.

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.

Issuers should note that SCA methods that rely upon mobile connectivity will entail some failures where network coverage is limited and should consider offering Wi-Fi based alternatives such as biometrics or mobile-app push notifications for delivering OTPs.

PSPs have an obligation to periodically test, evaluate and have independently audited the security measures they are taking to comply with SCA rules and Visa recommends that Issuers ensure that measures taken to mitigate risks associated with the use of SMS OTP are assessed at minimum as part of this process.

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.

5.3.2 Biometrics

Visa is investing in sophisticated SCA methods leveraging biometric technologies. While these are clearly the preferred long-term SCA methods for Visa, their usage will require Issuers to progressively embrace biometric based SCA solutions, which Visa will require all Issuers to offer as an option for Visa cardholders by April 2020.

Issuers who do not yet support biometric authentication should ensure they have a plan in place to offer the capability by April 2020. To find out more about Visa's biometric solutions contact your Account Executive.

Visa's approach is to provide best in class biometric solutions via the Visa ID Intelligence platform (VIDI) while also supporting Issuers' existing proprietary biometric technologies such as those deployed for Mobile banking log-in authentication.

Visa's biometric solutions will offer support for multiple biometric authentication approaches including fingerprint, facial and voice recognition to allow consumers to select their preferred modality. Support of the FIDO UAF protocol and mobile SDKs will minimise development complexity. This will also enable issuers to customise the consumer experience for different use cases with different risk profiles. For example, a proprietary mobile phone fingerprint authenticator may be sufficient for a medium risk transaction, while an Issuer may decide to use facial recognition controlled and managed by the VIDI SDK and embedded in their own mobile banking application for higher risk transactions.

5.4 Transaction Risk Analysis (TRA)

The TRA exemption allows for certain 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 transactions. Visa's view on the application of TRA is as follows:

1. Issuers and Acquirers can both apply the TRA exemption so long as their fraud to sales rates are maintained within the specific fraud thresholds for card payments, namely:

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

2. The party using the TRA exemption is liable under the Visa Rules should the transaction be fraudulent.
3. Provided the Issuer is made aware that the Acquirer has performed the transaction risk assessment, the Issuer is not mandated to require SCA and can accept the TRA exemption request.
4. Issuers have the final say when a payment is submitted via 3-D secure or for authorization with an Acquirer exemption request flag and may apply SCA or decline the transaction if they do not wish to honour the Acquirer's TRA exemption request.
5. If the Issuer declines the Acquirer's exemption request and requires SCA to be applied, the Acquirer must resubmit the transaction for authentication, so the Issuer can apply SCA and in this case the Issuer assumes liability for the transaction under the Visa Rules.

Issuers, acquirers and merchants should work to develop risk policies to optimise application of the TRA exemption and monitor its effectiveness from the perspectives of both fraud prevention and minimisation of cart abandonment. Merchants and acquirers should also take account of the balance between control offered by requesting the exemption and liability protection.

6. In the case that one of the PSPs (the Issuer or the Acquirer) applies the TRA exemption, Visa's view is that any fraud from that given 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.

5.5 Trusted Beneficiaries Exemption

5.5.1 Principles

Visa supports the use of the trusted beneficiaries exemption for card payments. It should be noted that in order to be compliant with SCA provisions:

1. Only Issuers can create/maintain lists of trusted beneficiaries on behalf of cardholders and use the trusted beneficiaries exemption, although Issuers are allowed to outsource or delegate this solution (such as through Visa Trusted Listing).

2. 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.
3. Acquirers cannot apply this exemption and a merchant cannot set up the list for the purpose of the SCA exemption.

5.5.2 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.

Issuers should develop policies for selecting merchants that will qualify for the trusted beneficiaries exemption and should evaluate solutions to implement trusted beneficiaries listing. For more information on the Visa Trusted Listing Solution contact your Account Executive.

5.5.3 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 enrolment process through:

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

Merchants with low fraud profiles and regular customers should consider how they can explain the benefits of trusted beneficiaries listing to their customers and encourage those whose issuers support it to enrol their trusted merchants.

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.

5.6 Low Value Transactions

SCA is not mandated for remote electronic low value transactions provided that the following conditions are met:

- The amount of the remote electronic payment transaction does not exceed EUR 30; and
- The cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of SCA does not, exceed EUR 100; or

- The number of previous remote electronic payment transactions initiated by the payer since the last application of SCA does not exceed 5 consecutive electronic payment transactions.

For sake of clarity, the limits (EUR 100 or five transactions) apply separately. Issuers may choose which metric to apply and SCA must be applied as soon as the selected threshold is reached. In practice, because Acquirers typically have no visibility of the cumulative transaction value and volume counts, application of this exemption will be available to Issuers only.

5.7 IoT Payments

Visa expects that transactions will increasingly be triggered through a range of connected or "IoT" devices. These can include for example smart speakers, smart TVs, connected appliances, connected vehicles and in car infotainment systems. In the short to medium term future these transactions will be predominantly initiated by a consumer, but it is expected that in future an increasing number will be triggered automatically by the connected device. For example, a printer may be programmed to automatically trigger a payment to reorder ink when its ink levels run low.

In the case of customer initiated transactions made through these devices, there will be a need to ensure that SCA can be applied when required. Initially this is likely to be through an "out of band" authentication approach delivered via a separate device (which will typically need to be bound to the user using SCA). In the longer term, "native solutions" comprising, for example a voice biometric coupled with the device ID of a trusted, pre-registered IoT device will provide consumers with more convenient authentication experiences. The Visa 3DS 2.0 protocol has been designed to support omni-channel commerce, and solution providers can develop 3DS 2.0 SDKs for any device operating system and user interface, ensuring an optimal customer experience independently of the device.

We expect that it may be possible to treat device-initiated transactions as Merchant Initiated Transactions, so long as these payments are made to a merchant with whom the customer has an agreement.

5.8 Corporate payments

Corporate payments initiated by business entities through dedicated processes or protocols which are not available to consumers and which already offer high levels of protection from fraud may be exempt from SCA.

Commercial cards are issued to business customers. Certain widely used products such as Lodge Cards, Central Travel Accounts, and Virtual Cards are not associated with an individual cardholder; they are used only by the company. Accordingly, because the payment initiation takes place in a corporate environment, their exposure to fraud is very limited. Furthermore,

Virtual Cards can be deployed using single use card numbers or tokens, and usage restrictions on merchant categories and values, and are therefore inherently secure.

Where the national competent authorities establish that those corporate payment processes and protocols, which are only made available to payers who are not consumers, meet the PSD2 security requirements, PSPs are allowed to exempt these transactions from SCA. The requirements that national competent authorities impose before a PSP may rely on this exemption may differ between EEA countries.

It should be noted that PSD2 requires PSPs to provide competent authorities with regular, updated and comprehensive assessments of the operational and security risks relating to the payment services it provides, and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks. Competent authorities may specify that PSPs not applying SCA under the corporate payments exemption must ensure the processes and protocols not subject to SCA are specifically included in this assessment.

Where a physical corporate card is issued to an individual named employee and is used by that cardholder employee to manually initiate a payment, for example for directly booking a flight on an airline's website, the SCA requirement applies. However, where the same card details are embedded and used in a secure corporate purchasing process (e.g. with a corporate appointed Travel Management Company), Visa's position is that these transactions should be considered as exempt from SCA, as the process being used is akin to a Lodge or Virtual Card and will be equally secure, and only available for Corporate transactions.

All corporate cards are exclusively offered to customers on the basis of corporate pay and liability. Accordingly, the relevant corporate entity is always responsible for settling payments made using these products and ultimately remains liable for settlement in any event.

5.9 Contactless Payments

5.9.1 Cumulative Limits and the Resetting of Counters

Visa's view is that the following details are relevant if using the card based or host-based accumulator approaches.

For sake of clarity, the cumulative limits (EUR 150 or five transactions) apply separately, however Visa recommends the value-based approach (EUR 150) to minimise impact on cardholder 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 reached.

Visa has already clarified to European supervisors how the same payment account may be associated with several payment devices, for example: a payment card, a mobile phone supporting a service (e.g. Apple Pay), and a wearable device and thus should be perceived as payment instruments being entitled to SCA application.

Visa's view is that:

1. Cumulative counts should be applied at the payment device level, not the payment account level
2. Counter resets should happen when the payment device is authenticated using SCA.

Contactless cards currently in circulation are not necessarily personalised with counters supporting the cumulative count or amount requirements specified in the SCA rules. Visa has created a contactless specification, *VCPS version 2.2.1 (or higher)*, that will allow compliance with the required cumulative counts and amounts for those Issuers preferring to solve SCA at card-level. Similarly, those Issuers wishing to take a host-based approach to managing the SCA rule will need to implement changes to their authorization systems and Acquirers would be required to ensure all terminals comply with *TIG version 1.4*.

Issuers & Acquirers should put in place plans to ensure that cards issued after 14th Sept 2019 and POS terminals are compliant with the new specification

Compliance with these requirements means either complete reissuance of payment cards in Europe or upgrades to POS terminals in Europe. This is neither logistically possible nor desirable from a fraud prevention perspective. Furthermore, upgrades to all POS terminals would create significant overhead and disruption to merchants and widespread card reissuance will be disruptive to cardholder experience.

Visa's position is that the requirement 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.

5.9.2 Contactless Payments at Point of Sale where there is no facility to capture SCA

There are at least two use cases where contactless payments are made but there may be no physical facility for applying SCA. These are:

1. Unattended contactless payment terminals without a PIN Entry Device, for example ticket machines or vending machines. The SCA rules include an exemption for "Unattended terminals for transport fares and parking fees". This allows PSPs not to apply SCA for transactions initiated at these terminals.

2. Card-based payment instruments associated with devices that can support contactless payments but do not have the facility to support SCA. These will typically be unsophisticated wearable devices such as fitness bands, payment wristbands, or jewellery.

Visa's position is that:

1. Transactions attempted at Contactless-Only Unattended Acceptance Terminals (UATs), i.e. ones that do not support a PIN Entry Device and cannot therefore perform SCA, will be sent online for the Issuer to determine whether to approve or decline the transaction. In most cases, such transaction are likely to be very low in value.
2. There is no general exemption from non-card form factors that do not support SCA. As noted above, behavioural biometrics may offer one way to support SCA. Transactions from non-card 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.

For more information

As part of an ongoing programme, Visa will be publishing new implementation guidelines and more detailed information for clients. Please contact your Visa Account Executive to hear more about these new developments.

VISA everywhere you want to be