PSD2 SCA Challenge Design Best Practice Guide

July 2020

Version 1.0
27 July 2020

VISA

Contents

Important Information

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

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.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers, and Merchants 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.

Note on references to EMV 3DS, 3-D Secure 2.0 and 3DS 2.0: When in this document we refer to 3-D Secure 2.0, 3DS 2.0 or EMV 3DS this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1.0 of the specification is referred to as EMV 3DS 2.1 and version 2.2.0 is referred to as EMV 3DS 2.2. The information in this guide is relevant to EMV 3DS 2.1 and EMV 3DS 2.2.

Purpose of this guide

There are a number of steps that merchants and payment service providers (PSPs) can take to minimise friction experienced by customers making remote electronic payments, while maintaining compliance with PSD2 Strong Customer Authentication (SCA) regulation. These include recognising and flagging out of scope transactions and optimising the application of exemptions to minimise the need for SCA challenges; and optimising the experience of completing an SCA challenge when required. This guide summarises the essential steps that Issuers, merchants, gateways and Acquirers should take to ensure that when customers are required to complete an SCA challenge, the experience is as clear and simple as possible. Guidance on optimising for out of scope transactions and exemptions is given in the companion *PSD2 SCA Optimisation Best Practice Guide*.

PSD2 requires that SCA is applied to many electronic payments

PSD2 requires that Strong Customer Authentication (SCA) is applied to electronic payments within the European Economic Area (EEA) and the UK unless an exemption applies, or the payment falls into one of the out of scope categories.

This requirement has been in place from 14 September 2019. In relation to e-commerce, it will be enforced by regulators from 31 December 2020 in the EEA (subject to guidance or additional conditions imposed by local regulators) and from 14 September 2021 in the UK (subject to compliance with phased implementation plans). These dates are referred to in this guide as "the enforcement dates."

SCA means the payer must be authenticated, normally by their card Issuer, using at least two independent factors, each of which must be from a different category of possession, inherence, or knowledge:

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

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

In Visa's view, the most practical SCA solutions will comprise:

Something only the payer has, for example a:

- Pre-registered mobile phone
- Card reader
- Key generation device

Something the payer is, for example:

- Behavioural biometrics
- A selfie
- A fingerprint
- Voice recognition

Something only the payer knows, for example:

- A password
- A PIN
- Questions whose answers are only known to the payer

Our goal is to minimise friction

Reducing customer friction is essential to minimising customer dissatisfaction and transaction abandonment.

In those cases where it is necessary to apply an SCA challenge, the impact on customer experience will be minimised through:

1. Careful selection and application of SCA factors and elements[1]
2. Optimised design of the challenge process and good communication – ensuring customers are clear on what steps they need to take
3. Proper integration of the challenge screens into the checkout flow

All parties in the e-commerce & payments ecosystem have a role to play

Issuers are responsible for verifying a cardholder's identity, and by default, for the application of SCA challenges, when they are required. In practice this may be done by their ACS or authentication vendor. Application of SCA may also be delegated to qualified third parties, including certain merchants. Visa offers the Visa Delegated Authentication Programme to facilitate delegation. More details on this can be found in the *Visa Delegated Authentication Program Implementation Guide*.

[1] in this document "factor" refers to the category (possession, knowledge, inherence) and "element" refers to the specific implementation within that category (for example: for possession, chip or tokenised device; for inherence, fingerprint, facial recognition or behavioural biometric).

Other parties in the payment and ecommerce ecosystem, including all merchants, gateways, 3-D Secure vendors and Acquirers also need to take steps to ensure that SCA challenge friction is minimised:

All parties have a part to play in reducing friction:

Merchants

- Support EMV 3DS 2.2
- Provide all required 3DS data, ensuring the data is correctly formatted, consistent & of high quality
- Complete testing via the Visa 3DS test platform to ensure everything is working correctly
- Optimise the integration of challenge screens into browser & app checkout outs
- Support SCA based customer enquiries

Gateways, Acquirers & 3DS Server Vendors

- Educate & support merchants in adopting 3DS 2.2
- Support merchants with integration with the 3DS SDK & branding & integration of challenge widows

VISA

- Offers a wide range of authentication & biometric services
- Provides guidance to all parties in the ecosystem
- Monitors performance to ensure ensure the ecosystem delivers best in class experience to consumers while managing risk

Issuers

- Set an inclusive, low friction SCA strategy
- Adopt & incentivise customer usage of biometric based solutions
- Adopt behavioural biometrics
- Minimise steps in the challenge flow & ensure the UI is clear & simple
- Provide effective customer comms & support

ACSs

- Support Visa tools & integrate with the challenge methods required by Issuers
- Ensure system availability & response times exceed Visa minimum requirements

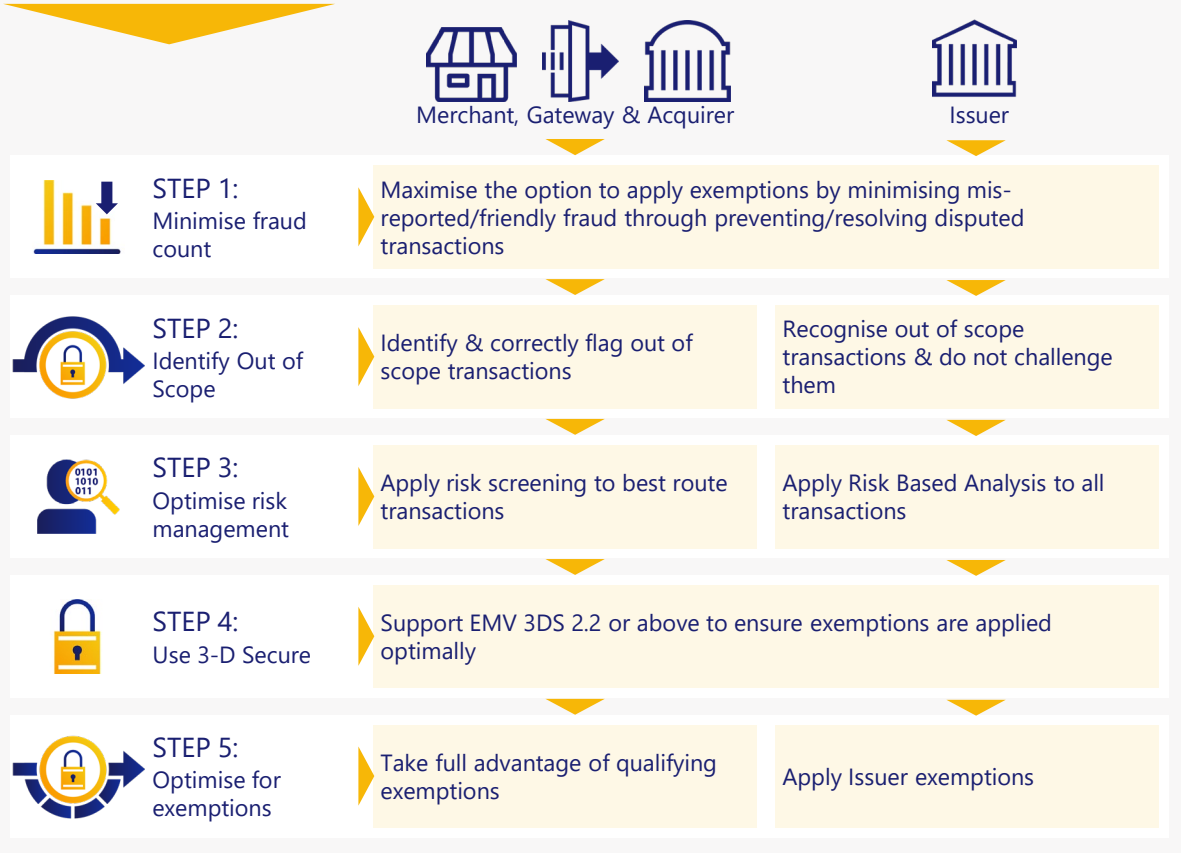
Minimizing friction across the challenge flow

There are two stages to minimising friction:

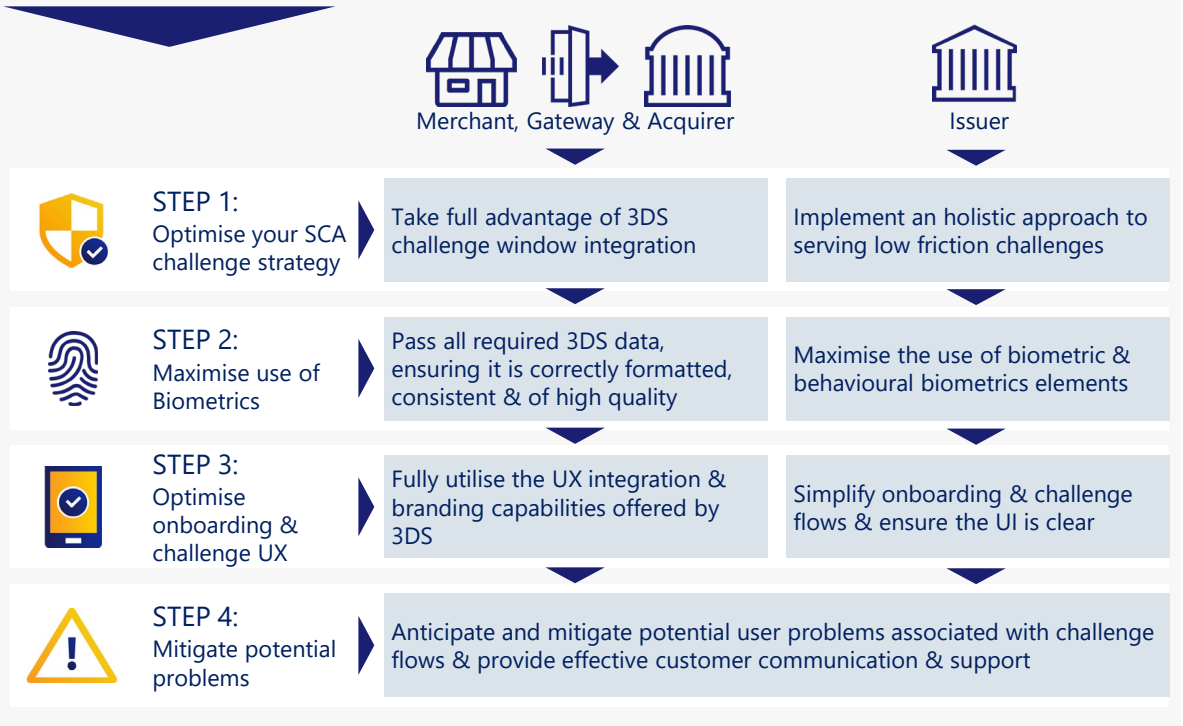
- Stage 1: Minimising the need for SCA challenges
- Stage 2: Creating a great challenge process offering minimal friction when SCA challenges are required

The following sections of this guide describe the key steps stakeholders should take to deliver Stage 2 - creating a great challenge process. See the *PSD2 SCA Optimisation Best Practice Guide* for guidance on Stage 1 and minimising the need for SCA challenges.

Stage 1: Minimising the need for SCA challenges



Stage 2: Minimising friction when SCA is required



Step 1: Optimise your SCA challenge strategy

Issuers should develop a holistic SCA challenge strategy

The optimum SCA challenge solution(s) for an Issuer will depend upon the make-up of their customer base. Issuers, ACS and authentication providers should focus on the following SCA Challenge solution options, targeting them at the appropriate target customer segments:

SCA challenge design – the main solution options:

Recommended solutions:

Description	Solution options	Target Segments*
Secure low friction solutions for the majority of customers in all markets	Out of Band App + Biometric OTP + Behavioural Biometric + 132 978	Browser & non-smartphone users Bank app users Other smart phone users Indicative segment sizes*

Tactical solutions:

Description	Solution option	Target Segment
Inclusive transitional/ back up solution for mainstream customers unable to immediately access recommended solutions	***1 + 132 978 OTP+ Knowledge Factor	Mobile users not accessible through Recommended Solutions by enforcement date Indicative segment size*

Inclusivity solutions:

Description	Example solutions	Target Segment
Solutions for niche segments unable to access recommended or tactical solutions	1234 5678 2 Factor: Card Readers OTP Tokens Browser solutions	Vulnerable & non-mobile phone users Indicative segment size*

*Note – segment sizes will vary by market

SCA challenge strategies should:

1. **Offer to customers a "recommended" authentication solution.** In most cases this will be either an Out of Band app plus biometric, or SMS OTP plus behavioural biometrics solution. In markets where a PSD2 compliant secure national bank or e-ID scheme is widely adopted by consumers this scheme may continue to be used, although whether the scheme achieves low abandonment rates should be taken into account.
2. **Encourage as many customers as possible to adopt the recommended solution** before the enforcement dates (or in the alternative timeframes required by local regulators). Seek to migrate the remaining customers as quickly as possible.
3. **Offer one or more compliant "tactical" authentication solutions where customers cannot access the recommended solution by the enforcement dates.** Tactical solutions may be used where it is not possible to fully implement recommended solutions by the enforcement dates (or the alternative timeframes required by local regulators). In most cases the tactical solution will be based on an OTP or app plus a knowledge factor.
4. **Ensure that a compliant second factor is added to any existing single factor OTP solutions** by the enforcement date, for example upgrading a pre-existing single factor SMS OTP solution by adding a behavioural biometric to provide a second factor.
5. **Offer one or more "inclusivity" solutions** for the minority of vulnerable and/or hard to reach customers who are unable to access mobile phone based authentication. Inclusivity solutions could include, for example, two-factor hardware-based authenticator devices that require input of an assigned password or PIN to operate.
6. **Minimise the barriers to customers adopting an authentication solution,** registering a device and enrolling credentials or devices.
7. **Align authentication solutions across all your service offerings as far as possible.** Providing a common authentication experience across payment authentication, online or mobile banking and other secure services.
8. **Optimise user experience by:**
    - Minimising the complexity of responding to challenges – for example the need to remember complex knowledge factors
    - Minimising the number of steps, keystrokes and latency involved in completing authentication
    - Minimising possible additional barriers to authentication such as the need for app updates during the course of an authentication

9. **Minimise the security risks** associated with storage of inherence and knowledge credentials
10. **Provide seamless fallback elements and customer support processes** when the main SCA solution cannot be used, or a credential needs to be reset
11. **Educate and inform customers** about why they will have to occasionally undertake SCA and how it will work

Merchants can also influence the SCA challenge user experience:

The latest version of 3-D Secure, called EMV 3DS or 3DS 2.0, 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. Merchants have options to:

- Integrate authentication into their checkout process in both app and browser-based implementations
- Brand aspects of the native app 3DS challenge window to provide a consistent look and feel

Merchants should talk to their 3DS server/3DS SDK provider about the best way of optimising 3DS challenge window integration into their checkout experience.

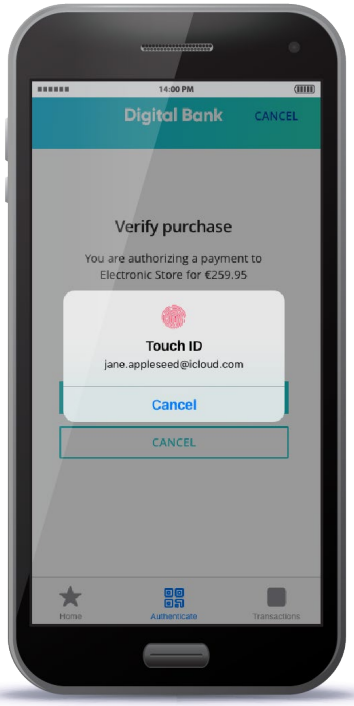
Step 2: Maximise the use of biometrics

Biometrics are the simplest and securest way to apply SCA. They minimise checkout friction and many customers are familiar with them and find them attractive. Both recommended SCA solutions use biometrics to provide an inherence factor.

Recommended solution 1: Out of Band app plus biometric

How it works

Out of Band Authentication allows an existing banking app or dedicated authenticator app to be used to apply SCA.



The app is typically "bound" to the device through a secure onboarding process that includes applying SCA. Once it is securely bound, the app facilitates proof of possession without the need for the user to take steps such as entering an OTP. The app also prompts the customer to complete the authentication process by entering the biometric which will typically be a fingerprint, facial or voice recognition or iris scan.

Who should consider it?

All Issuers should consider Out of Band app plus biometric as a strategic, long-term solution:

- Digital and mobile only banks should have a large proportion of their customers already using a mobile banking app. Using this app to authenticate payment transactions should be a relatively straightforward proposition for customers. A knowledge factor may be required for customers without a biometric capable device.
- Established, multichannel banks may already have in excess of 40% of customers using a mobile banking app. Banking app based authentication should be considered as a strategic solution for existing customers and Issuers may wish to encourage more customers to adopt their mobile banking solution to take advantage of simple payment authentication.
- Issuers without a mobile banking app should consider adopting a standalone authenticator app. Please contact your Visa representative if you would like details of Visa's authenticator app solution.

Advantages, disadvantages and options

Out of Band app plus biometric is an established solution offering a reasonable balance between security, user experience, consumer familiarity and acceptance.

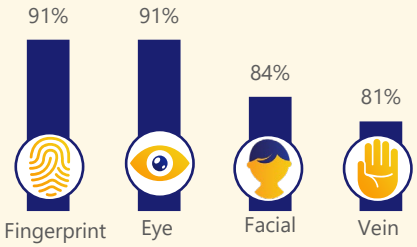
Visa Consumer Research Indicates that Customers are receptive to biometric authentication

66% Believe biometrics are easier than passwords

66% of credit card holders are familiar with biometric authentication – rising to 83% in 30-39 age group.

36% had used biometrics to make a payment in the previous week

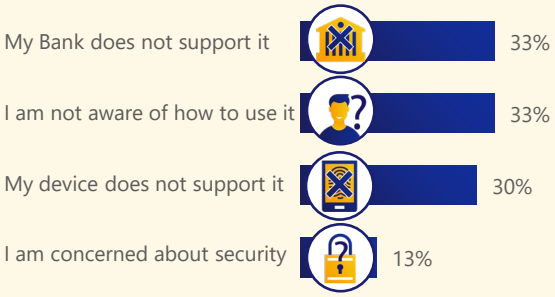
Over 80% perceive biometric methods to be secure



53% Would likely switch away from banks and payment cards that don't offer biometrics

Few are turning away from biometric authentication for security or technical failure reasons:

Reasons customer's have not used biometric authentication in the last 7 days:



Source: Consumer research undertaken on behalf of Visa with a sample of 1,000 UK credit card holders in April 2019

The solution has a number of advantages but also some disadvantages:

Out of Band app plus biometric advantages and disadvantages

Advantages

- Familiar experience for existing bank app users
- Relatively low friction experience
- No knowledge factor to memorise
- Well integrated with app based commerce
- Simple & cost effective to distribute

Disadvantages

- Compatible smartphone required
- Customer onboarding can be complex
- Some user experience friction
- Some consumers resistant to app adoption/ biometric usage

Issuers should ensure they follow the user experience optimisation advice given later in this guide and clearly explain to customers the benefits and data protection measures inherent in their solutions to maximise the benefits.

Recommended solution 2: OTP plus behavioural biometrics

How it works

Behavioural biometrics uses physical behaviour indicators that are unique to an individual customer. These can include the angle at which a device is held, the way keystrokes are entered, gesture analysis and swiping speed.

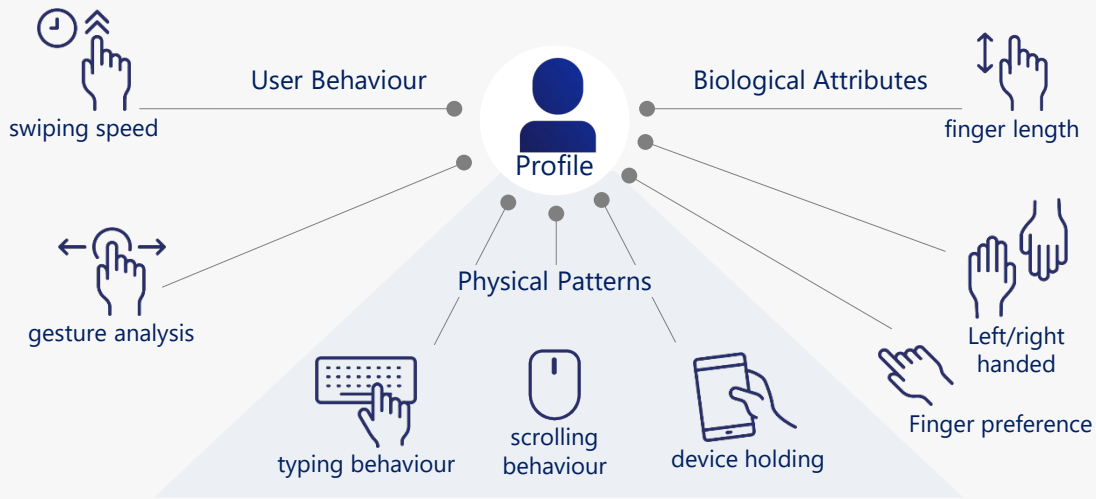
Indicators are analysed and used to build user profiles and authenticate users.

With all data points taken together, a customer's digital footprint is very hard for a fraudster to replicate.

The use of behavioural biometrics is in line with the European Banking Authority opinion on elements for SCA which identifies inherence elements such as keystroke dynamics (identifying a user by the way they **type and swipe**) and the **angle** at which the user holds the device.

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

Behavioural biometrics solutions combine various physical behaviour indicators to deliver an effective inherence factor:



The benefits of behavioural biometrics

Behavioural biometrics offers a number of benefits:

Behavioural biometrics benefits

Supporting SCA
Use of behavioural biometrics to prove inherence is permitted by the regulation

Secure & reliable
Behavioural Biometrics helps to protect against SMS OTP fraud and supplements existing data shared through 3DS

Low friction user experience
The customer does not have to do anything to generate the inherence factor

Inclusive
Behavioural biometrics does not require the customer to have a smartphone or app

Proven, available technology
Behavioural biometrics are widely and successfully deployed in other fraud prevention use cases

Practical considerations of implementing behavioural biometrics

The main practical consideration concerning behavioural biometrics as a standalone solution is that it can take several transactions or interactions with the customer to capture the behavioural characteristics required to build a strong biometric profile.

Options for managing the initial profile building period can include:

- Putting in place an onboarding process during which the customer enters information into their device in a way that allows sufficient behavioural characteristics to be captured
- Utilising a supplementary knowledge factor during the initial stages of development of a customer's behavioural biometric profile
- If the Issuer is prepared not to adopt either approach, taking a layered approach that uses EMV 3DS data in addition to the behavioural biometric to assess the risk profile of transactions

If an Issuer does not choose to use a compliant second factor while the biometric profile is being built, the risks of such an approach could be mitigated through supplementing the behavioural biometrics with additional fraud profiling using EMV 3DS data and by appropriately managing the initial profile building process and period.

If the Issuer decides to take this third approach, fraud protection can be maximised by combining the behavioural biometric indicators with EMV 3DS data, which include device, location and purchase history data, and provides a proven, accurate basis for assessing fraud risk. Issuers should therefore work with behavioural biometric solution

vendors and their ACS vendor to ensure that the solutions they deploy make full use of all available data to minimise user experience friction and fraud. Where adopted, it should be maintained to maximise the effectiveness of risk analysis even when the behavioural biometric profile is compiled.

We plan to seek clarity from the EBA as to whether EMV 3DS data can be used to manage the initial profile building, as well as maximising the effectiveness of risk analysis even when the behavioural profile is compiled. This would offer the lowest friction customer experience while providing effective fraud detection.

Issuers implementing a behavioural biometrics based solution should also note that it may be necessary to gain customer consent to collect and process behavioural biometric data. Advice should be sought from a qualified advisor.

Using alternatives to biometric based solutions

While Out of Band app plus biometric and OTP plus behavioural biometrics are recommended as the primary SCA solutions for the majority of customers, alternatives may be considered in the following circumstances:

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

The main solutions relevant in each these cases are summarised below:

Tactical Solution 1: OTP plus knowledge factor

How it works

An OTP is sent to the customer, normally via SMS, to prove possession. This is entered into the 3DS challenge window along with a compliant knowledge credential such as a dedicated password or PIN.

When to consider it

OTP plus knowledge-based solutions may be considered in the following circumstances:

- As a supplement to a behavioural biometric during the early stages of development of a customer's behavioural biometric profile. Issuers may consider this depending upon their risk strategy, but should consider the potential negative impacts on user experience and customer security summarised below.
- As an interim solution if an Issuer is unable to implement a behavioural biometrics based solution before the enforcement date.

Advantages, disadvantages and options

OTP plus knowledge factor is considered compliant with the regulatory requirements for PSD2 SCA. However, it is inconvenient for customers and provides a poor user experience. Use of a knowledge factor is associated with high transaction abandonment rates, increased overheads managing the resetting of forgotten credentials and increased security risks.

More guidance on selection of knowledge credentials is given in the section on Selecting knowledge factors (Out of Band and OTP based Solutions) later in this guide.

Tactical Solution 2: Out of Band app plus knowledge factor

How it works

A device bound banking or authenticator app is used to prove possession. This is coupled with a knowledge factor rather than a biometric.

Who should consider it?

Issuers who have an existing banking app that is accessed via a knowledge factor could consider using it as an SCA solution, so long as it is well established, regularly used by customers and transaction abandonment rates are monitored. Use of a knowledge factor is not recommended for a new app or one that is only used occasionally by customers.

Inclusivity solutions

Why inclusivity solutions are required

While Issuers need to focus on serving the majority of customers with the recommended SCA solutions, inclusivity solutions should also be made available for limited deployment to those customers unable to access or use mobile phones for authentication. A number of two-factor options are available including:

Hardware solutions

- PIN activated card readers: Prove possession through checking the card chip when the card is entered in the reader and knowledge through entry of the card PIN. On successful completion of the challenge, the reader displays a unique numerical code which the customer enters via the 3DS challenge window to prove that authentication has been completed.
- OTP generator tokens: The token, which must initially be securely provisioned to and associated with the customer, proves possession and knowledge or inherence is proved through entering a PIN or biometric, typically via a fingerprint reader built into the token. As with the card reader, the customer enters a code generate by the token to prove that authentication has been completed

- USB authenticator keys (for example FIDO roaming authenticators): Once securely provisioned, these can be plugged into a USB port on the customers computer. Possession is proven by the authenticator returning a cryptographically signed authentication message to the Issuer. The second factor may be a biometric (inherence) or password/PIN (knowledge).

Software solutions

- A device bound browser or software authenticator running on a customer's computer proves possession using a cryptographic exchange. This may be used with either a computer embedded fingerprint reader to prove inherence or a password entered into the 3DS challenge window to prove knowledge.

Issuers should select appropriate solutions based upon a balance between:

- The size and needs of their customer base,
- Simplicity of the onboarding and user authentication experience
- Ease and cost of deployment and management

Issuers should also note that the process of associating the 'possession' device and the user and activation of the device by means of a remote channel requires SCA.

Guidance to merchants on ensuring quality of 3DS data

Merchants must support 3DS to facilitate the application of SCA which is required under PSD2 and Visa strongly encourages merchants and to support EMV 3DS 2.2 as early as possible.

EMV 3DS also requires that merchants submit additional transaction data[2] with the authentication request message. This data is used by Issuer's ACS providers to analyse the risk of the transaction and can reduce the number of transactions for which SCA is applied. It is critical that this data is correctly formatted, consistent and of high quality in order to avoid Issuers having to apply SCA just because they have insufficient data to risk assess a transaction. Merchants should pay particular attention to the Browser IP, Shipping Address Postal code, Billing Address Postal code, and Address match indicator as key fields. However, in general, the more quality data that the merchant is able to supply over time (regardless if it is optional or required), the more it can assist in the risk analysis of the transaction.[3] A further critical factor in the gathering of data is the use of the 3DS Method URL. If a 3DS Method URL is specified, then merchants should be using this for the appropriate flows.

[2] Merchants should refer to the PSD2 SCA for Remote Electronic Transactions Implementation Guide for detailed information of 3DS data requirements

[3] Also see https://www.ukfinance.org.uk/system/files/Strong%20Customer%20Authentication%20-%20Communication%20on%20improving%20outcomes%20from%203DSecure%20–%20Data%20Consistency_1.pdf

Step 3: Optimise the onboarding & challenge UX

The following guidance aims to help Issuers select the best deployment options for each solution to optimise the balance between user experience and security while taking account of practical deployment considerations.

Optimising Out of Band app plus biometric solutions

Issuers implementing Out of Band app plus biometric solutions can choose from the following implementation options:

1. Using the mobile banking app or a dedicated authenticator app
2. Different methods for proving possession via the app
3. Using the native device biometric capability provided by the manufacturer or a third party biometric service enabled via the app

In each case Issuers considering how to implement a solution should consider the following:

Mobile banking app vs. a dedicated authenticator app

The relative advantages and disadvantages of using a mobile banking app vs. a dedicated authenticator app are summarised below:

Mobile Banking App	Vs.	Dedicated Authenticator App
• Easier for customers to discover • App secures multiple Issuer services • Familiar to existing mobile banking customers		• Does not require Issuer to have suitable banking app • Decouples PSD 2 SCA authentication from bank app development • Provides the basis for a single multi-channel authentication solution where the app can be used to authenticate other services
• Issuers must have a suitable app • Development backlogs may delay authentication implementation • Banking apps that are slow to open will adversely impact abandonment.		• Customers need to discover, install and use another single purpose app • May confuse customers

The preferred solution for Issuers that have a mobile banking app is to use the banking app as the authenticator. This is the simplest solution for customers as it does not require them to discover, install, onboard or use a separate app and minimises the potential confusion associated with a customer having to use different Issuer branded apps for banking and payment authentication.

Issuers may consider a standalone authenticator app if:

- They do not offer a mobile banking app
- They want to implement a single centralised authentication solution for all authentication requirements across all digital channels and services
- They are unable to schedule SCA support into the development backlog for the mobile banking app without putting the SCA or app development program at risk

If a standalone app is adopted Issuers need to clearly communicate to customers the need for the app, and the steps in the discovery, downloading, onboarding and authentication process.

Visa Biometric Authenticator App

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

Selection of method for proving possession

The European Banking Authority (EBA) has confirmed that approaches relying on mobile apps, (and also web browsers), or the exchange of public and private keys may be used to prove evidence of possession, provided that they include a device-binding process that ensures a unique connection between the app, browser or key and the device. This may, for instance, be through hardware crypto-security, web-browser and mobile-device registration, or keys stored in the secure element of a device. The regulation requires that such device-binding (if it is performed remotely) is undertaken in a secure environment and by applying SCA. This is likely to require the Issuer to initially rely on factors which can already be deployed, such as SMS OTP (possession) and the login credentials used for online banking (knowledge).

Selection of the biometric

The preferred solution for capturing the biometric will normally be to use native biometric capabilities of the device, for example the inbuilt fingerprint reader.

This offers a number of advantages including:

- Familiar & simple authentication process for the customer consistent with other apps
- Secure on device storage/protection of customer biometric data
- Does not require mobile network coverage

Issuers using native device biometrics need to bear in mind the following considerations:

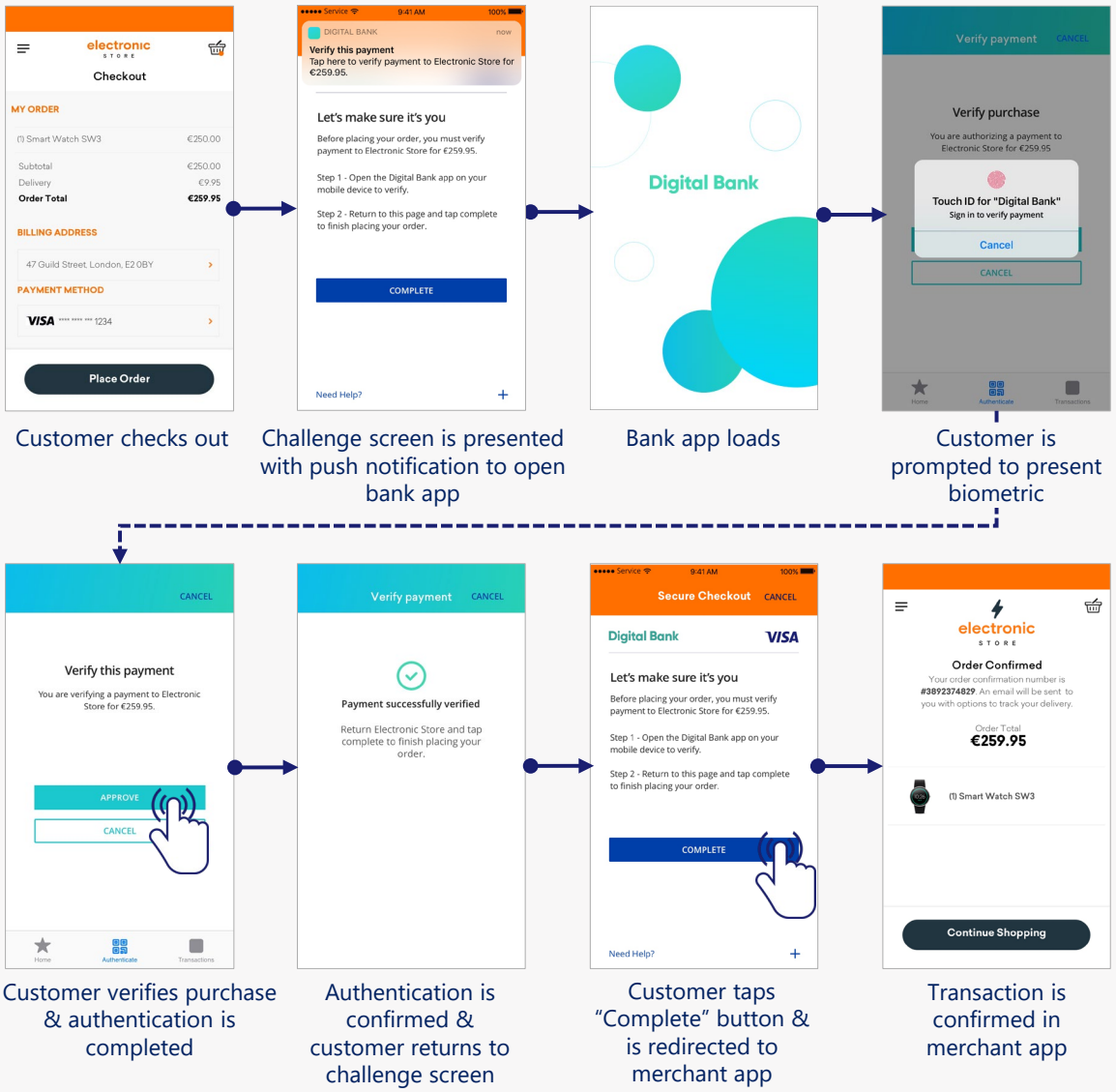
- The need to validate/support multiple device vendor biometric solutions

- Any applicable regulatory requirements are met, e.g. for a commercial agreement between Issuer & device vendor, or for regular auditing of the solution
- There may be issues differentiating between users of shared devices
- Issuers will depend upon the security of the device manufacturer's solution and need to take responsibility for complying with regulatory requirements and take steps to ensure the security of the solution

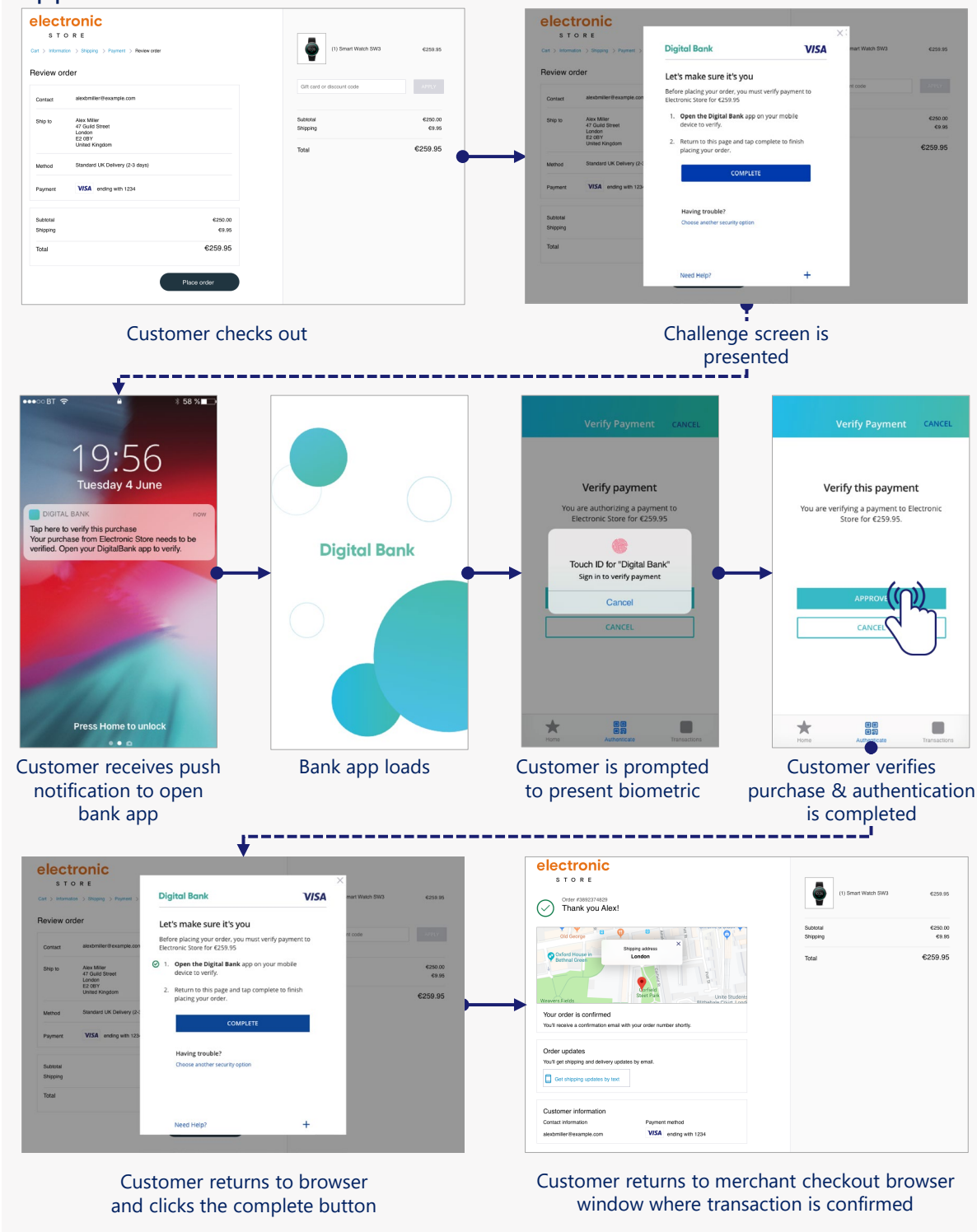
Optimising the Out of Band user experience flow

Example user experience flows for app and browser based purchases are shown below:

Example user experience flow – native app-based purchase with bank app + biometric authentication



Example user experience flow - browser-based purchase with bank app + biometric authentication



Out of Band authentication flows require the customer to move from the merchant's browser or app based checkout to the mobile banking or authenticator app in order to authenticate, and back again once authentication is complete.

This process can be confusing for customers and this, along with poor app performance, may result in authentication failures or transaction abandonment. The risk of problems arising can be minimised by taking account of the following points:

Minimise the risk of customer error

In order to minimise customer error, it is strongly recommended that Issuers carefully design and test user challenge and "unhappy path" instructions, taking account of at least the following points:

- The 3DS challenge screen needs to include clear instructions on opening the mobile banking or authenticator app and using it to complete authentication
- Use of push notifications that direct customers to their mobile banking or authenticator app can help guide customers through the authentication flow
- EMV 3DS 2.2 supports the capability of an Issuer Out of Band app to automatically route the customer back to the merchant app upon completion of the authentication challenge.
- With EMV 3DS 2.1 the customer has to navigate back to the merchant app manually after completion of the Out of Band authentication challenge

For the latest, detailed guidance on optimising the design of the Out of Band user experience please visit the Visa Developer Center at https://developer.visa.com/pages/visa-3d-secure.

Minimise app latency

Issuers should ensure that banking apps used to apply SCA load as quickly as possible to minimise friction and customer abandonment. Ideally the delay between triggering the loading of the app and the customer being able to authenticate should be less than 5 seconds.

Managing app updates

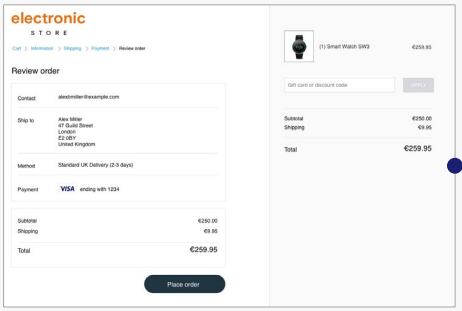
It is important to avoid the customer having to apply app updates during the checkout and transaction authentication flow in order to authenticate a transaction. Issuers should ensure that they implement strategies to minimise the impact of app updates. These strategies should include:

- Ensuring that all customers are migrated to the version of the app that supports SCA before the regulatory enforcement dates
- Communicating the need to update the app to customers
- Ensuring that app updates do not require customers to re-register for mobile banking

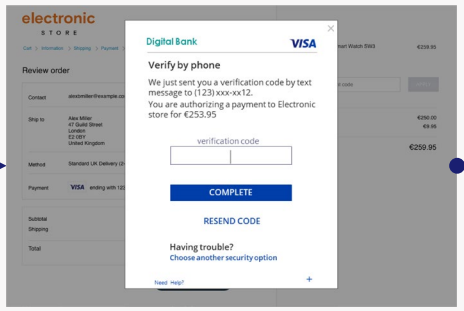
Optimising SMS OTP plus behavioural biometrics user journey

The user journey for SMS OTP plus behavioural biometrics just requires the customer to receive and enter the SMS OTP. The behavioural biometric information is collected without any additional customer action. The design of the user experience needs to focus on providing clear instructions in the 3DS challenge window. Example user journeys for both browser and app based purchase are shown below:

Example user experience flow – browser-based purchase with SMS OTP plus behavioural biometrics authentication



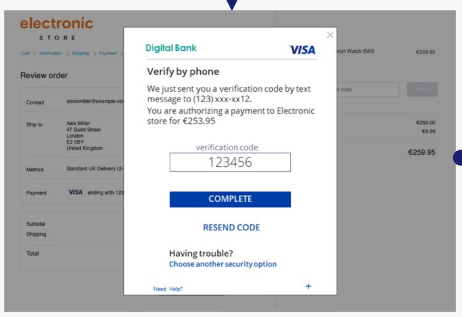
Customer checks out



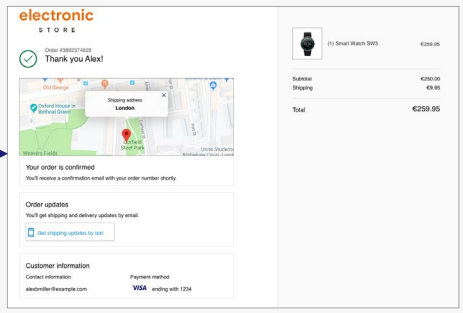
Challenge screen is presented

SMS OTP is received

Behavioural biometrics information is collected without action from the customer.

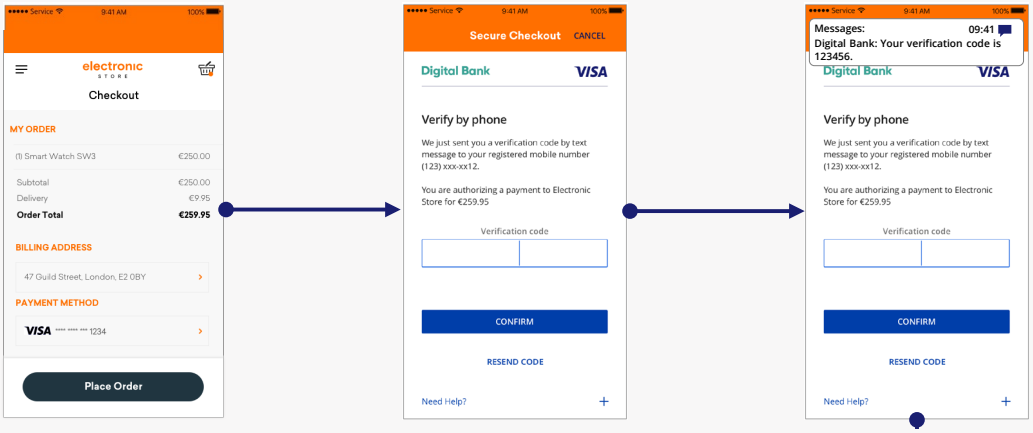


Customer enters verification code and is authenticated using both OTP & behavioural biometric factors



Transaction is confirmed via merchant checkout

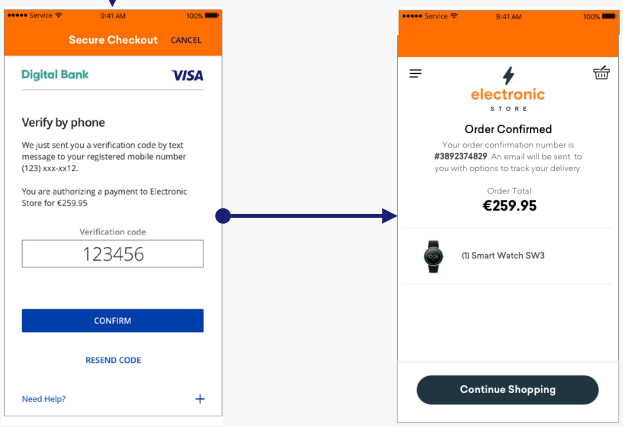
Example user experience flow – app-based purchase with SMS OTP plus behavioural biometrics authentication



Customer checks out

Challenge screen is presented

Customer receives verification code & behavioural biometrics information is collected without action from the customer.



Customer enters verification code is authenticated using both OTP & behavioural biometric factors

Transaction is confirmed via merchant checkout

Selecting knowledge factors (Out of Band and OTP based Solutions)

While knowledge factors are compliant from a regulatory perspective, they have a number of significant disadvantages including:

- Inconvenience to the consumer of remembering and entering a credential
- The high level of user friction involved in entering the credential for example if the customer has to enter selected characters or a code derived from a knowledge credential
- High levels of abandonment and increased customer service overhead for Issuers and merchants resulting from forgotten or mis-entered credentials
- Putting the customer at higher risk of social engineering attacks
- The security risk associated with customers using weak credentials and/or writing them down or storing them insecurely

Knowledge factors should be avoided wherever possible, however where an inherence factor cannot be used, and an Issuer needs to select a knowledge factor, the following considerations should be taken into account:

Potential Knowledge Factor	Implementation considerations		Use Case Recommendations
	Advantages	Disadvantages	
Full existing On-line / Mobile banking credential	• Familiar to customer	• Increases social engineering attack risk • Security risk of re-using a credential across different channel • Not all customers have online or mobile banking	• Out of Band solution using banking app plus knowledge factor
New E-commerce only credential (full or partially entered)	• Removes risk of compromise of banking credential • Does not require an on-line or mobile banking credential	• Additional credential(s) for the customer to remember • Returns to high friction static passwords previously used for 3DS 1.0	• As a knowledge factor with SMS OTP
Full Card PIN	• Familiar to customer	• Security concerns over entering PIN into a browser • May conflict with PIN security messaging to customers • May create additional PCI DSS requirements	• Only with a card reader used as an inclusivity solution
Randomised characters from card PIN	• Familiar to customer	• May conflict with PIN security messaging to customers	• Not recommended
Randomised characters from on-line/mobile banking credential	• Familiar to customer • Reduces malware compromise risk • Could be long enough to protect against fraud	• Not all customers have online or mobile banking • Difficult for customers to recall partial characters and likely to increase abandonment	• Not recommended
Existing Bank ID or National e-ID credential	• Familiar to customer • Already used for multiple authentication use cases	• Only applicable in markets where such schemes are widely adopted	• National Bank ID scheme

Optimising the design and integration of 3DS challenge windows

EMV 3DS allows for better integration of authentication challenge windows into the checkout process flow for both browser and app based implementations.

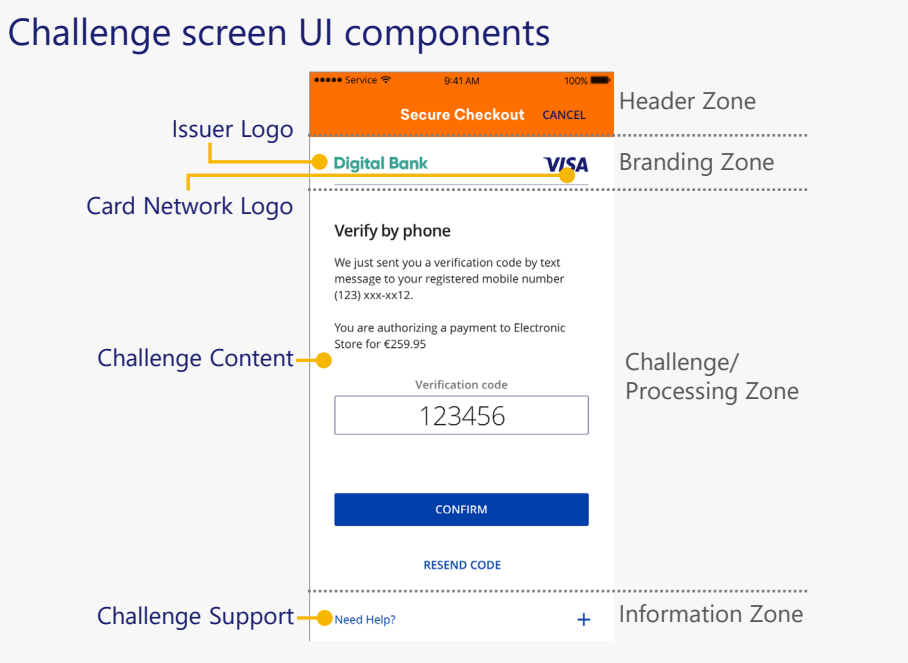
For browser based checkout implementations, the Issuer/ACS controls the content and branding of the 3DS challenge window, providing a consistent Issuer brand experience across all merchant websites. However, the merchant determines the size and placement of the window in relation to content in its checkout page.

For app-based implementations, the merchant app and the 3DS SDK control the rendering of the UI and native and HTML formats are supported. The customer device determines the format used.

For native app formats the merchant is able to customise colours and fonts used in certain components of the challenge window, notably the header zone and confirm button, to provide brand consistency with the merchant app checkout screens. For HTML formants, the branding is defined by the Issuer, providing an Issuer consistent experience across devices that are able to render HTML.

In all implementations and formats the authentication content is provided by the Issuer/ACS.

The 3DS challenge window and flow follows a consistent hierarchy defined by the EMVCo specification. Challenge windows are divided into zones with defined content components some of which can be Issuer customized.



In order to meet the requirements of the PSD2 SCA regulation:

- Visa expects the challenge window to include the merchant name and amount and clearly show the card payment details.
- Where a customer is asked to enter a knowledge factor the knowledge factor must be masked. It is possible to show individual characters as they are entered but the factor must not be shown in full.

More detailed information on 3DS UI challenge screen can be found in section 4 of the EMVCo *3-D Secure Protocol and Core Functions Specification Version 2.2.0* and additional Visa guidelines for Issuers, ACSs and merchants are available on the Visa Developer Center at https://developer.visa.com/pages/visa-3d-secure.

Merchants need to support JavaScript to enable solutions that minimise check out friction

Merchants should allow JavaScripts to run in the 3DS challenge window to allow the collection of device data by the Issuer's ACS. Device information has a strong influence on the risk score and as such will help minimise the need for high friction SCA challenges.

Behavioural biometrics solutions will also require JavaScript integration between the ACS and the behavioural biometrics solution provider for 3-D Secure browser-based authentication challenge flows.

Therefore, merchants are encouraged not to implement restrictions on their websites that could interfere with such scripts. Possible restrictions could be related to the inclusion of third-party content, CORS restrictions, or similar.

Merchants are also encouraged to ensure that when enabling JavaScripts they do so in a safe manner so as to allow the usage of behavioural biometrics for web browser shopping whilst providing customers with a convenient way of authenticating. This in turn will avoid the unwelcomed need to use other authentication solutions which could add friction to the customer's online check out experience.

Step 4: Anticipate & mitigate potential problems

Issuers will need to put in place proactive customer communications, support an increase in customer service requests and provide fall back processes when authentication fails. Such processes must be designed to prevent possible exploitation by fraudsters. They should take account of at least the following:

Issue	Issuer/delegate Response	Additional Guidance points
General failure of authentication	Communicate to the customer to contact the bank and provide a process to securely diagnose the cause of the failure	• Provide advice to the customer on rectifying the problem

Incorrect challenge response from the customer (e.g. OTP or knowledge factor is entered incorrectly or biometric is not recognised)	Visa requires that the customer should be given a maximum of three attempts to enter a factor and then the transaction should be declined	• After each of the first two attempts provide clear messaging that:
		  • Provides advice on correct entry of the factor
		  • States remaining attempts
		  • States that the transaction will be declined in some cases
		  • Offers an alternative where this is possible – for example entering a back-up knowledge factor if a biometric fails
		• For detailed guidance on presentation of this messaging see the user experience guidelines at: https://developer.visa.com/pages/visa-3d-secure

Customer using an app based solution changes their mobile phone	Provide clear communications to customers on the need to enroll any new device or bank/authenticator app and a seamless, self-service process for doing this	• Ensure customers using Out of Band app-based authentication understand how it works and that they need the authenticator app to be installed and provisioned on a new device before they can authenticate e-commerce transactions
Updating of Apps	Adopt app update workflows that minimise the risk that a user will need to manually update an app during the	• Ensure all customers are migrated to the SCA version of the app that before the regulatory enforcement dates • Communicate the need to update the app to customers

	purchase flow to complete authentication	• Ensure that app updates do not require customers to re-register
Customer using SMS OTP changes mobile number.	Ensure a process is in place to manage number updates	• Clearly communicate the need to always register a changed number • Provide a secure process for registering a change of number, which will need to comply with the SCA regulatory requirements if performed online
Customer using a mobile phone based authentication has no mobile or data coverage	Consider offering backup authentication options	• See the guidance at https://developer.visa.com/pages/visa-3d-secure for more information on presenting backup options
Ease of customer contact	Provide alternative customer contact options	• Put in place a social media support contact strategy in addition to traditional customer support channels to ensure customers can easily receive advice in case of authentication problems

Mitigation of potential challenges associated SMS OTP

Continued use of solutions using SMS OTP as a possession factor raises specific challenges. Issuers should consider the following points to mitigate potential problems

Migration to a compliant second factor for SMS OTP

SMS OTP has already been widely deployed by Issuers, but in most cases as a single factor solution alongside card details.

Issuers that use or plan to use SMS OTP as an SCA method beyond the enforcement date should develop a plan to ensure that it is implemented in an SCA-compliant way. Considerations should include:

- Ensuring two compliant factors are used
- Designing the challenge experience to minimize friction, and to provide a more seamless long term compliance option, preferably using behavioural biometrics as an inherence factor or, if this is not possible, a compliant knowledge factor.
- Implementing a test programme, prior to SCA enforcement, that ensures an authentication message can be successfully sent to and received by every registered customer
- Secure processes for collection, registration & maintenance of user mobile numbers, including:
    - Checking numbers are up to date on an ongoing basis

    - Changing mobile numbers associated with an account (ensuring that where changes can be made online, SCA is performed)
    - Ensuring that an authentication message can be received by more than one authorised number when there is a legitimate need[4]
- A process for handling authentication message failures that:
    - Tracks failures, identifies and updates non-working numbers
    - Provides appropriate messaging and prompts to the customer
- Mitigation of security risks associated with the use of SMS
- Development of a customer and stakeholder communications plan
- Development of an inclusion and fall-back strategy for those customers who are unwilling or unable to utilize SMS OTP or do not provide a valid mobile phone number

Mitigation of risks associated with SMS OTP

SMS has inherent security vulnerabilities. These do not preclude its use as an element to prove possession, however Issuers should take steps to mitigate risks including:

- Man in the middle attacks
- SIM swap fraud

For example, commercially available SIM swap fraud detection solutions may be deployed. These identify instances where a new SIM has recently been issued by a Mobile Network Operator and identify suspicious SIM swaps through risk scoring based on location, device type and customer behaviour provided by mobile networks. Use of behavioural biometrics also helps to mitigate the risks associated with SMS OTP through validating the device, location and customer behaviour patterns.

[4] Notes:

1) Where more than one number is registered to a card, the cardholder is responsible for all numbers registered and ensuring that payments authenticated using the numbers are correctly authorised
2) Issuers will need to ensure that risk rules take account of likely legitimate and non-legitimate transaction behaviours and contexts where more than one number is registered to a card

Summary of Visa SCA products

Visa offers a number of products that can help Issuers and ACSs to ensure that SCA can be applied with minimal friction in cases where it is required.

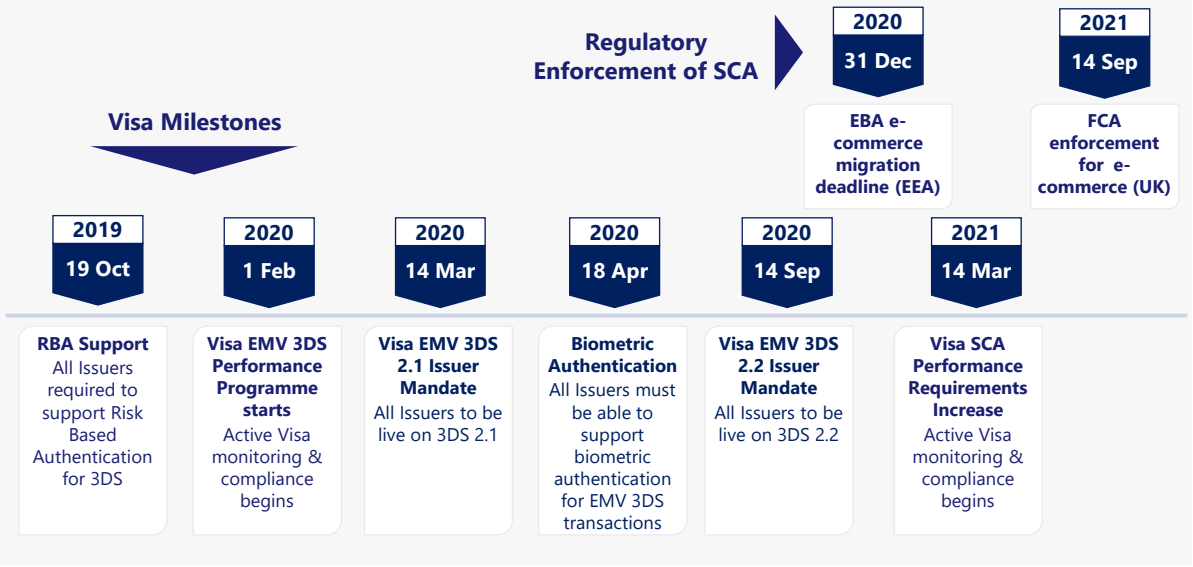
Visa also offers a number of solutions to help clients and merchants minimise the application of SCA challenges. These are summarised in the Visa *PSD2 SCA Optimisation Guide*.

Timescales and Mandates

The requirement to apply SCA came into force on 14 September 2019. In relation to e-commerce transactions, the European Banking Authority (EBA) has recognized the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement SCA and has set a deadline of 31 December 2020 (subject to guidance or additional conditions imposed by local regulators) by which time the period of supervisory flexibility should end. Please note that in the UK the FCA will start to enforce the regulation from 14 September 2021 (subject to compliance with phased implementation plans). The migration plans of PSPs, including the implementation and testing by merchants should also be completed by 31 December 2020.

Visa has put in place a set of rules and mandates for Issuers to support EMV 3DS 2.1, and EMV 3DS 2.2, biometric authentication solutions and Risk Based Authentication. The key timescales are:

Key SCA implementation milestones



Useful References

Document/Resource	Version/Date	Description
PSD2 SCA for Remote Electronic Transactions Implementation Guide	Version 2.0 November 2019	Detailed Guide covering all aspects of planning for and managing the implementation and application of PSD2 SCA for remote electronic transactions. Available at: https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html
EMVCo 3-D Secure Protocol and Core Functions Specification	V2.2.0 December 2018	Specification for the core 3DS technology that describes how 3DS works in detail. Available at: https://www.emvco.com/emv-technologies/3d-secure/
EMVCo 3-D Secure SDK Specification	V2.2.0 December 2018	Specification and information on the operation of the 3-D Secure SDK. Available at: https://www.emvco.com/emv-technologies/3d-secure/
Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure. This version has been updated specifically to cover EMV 3DS 2.2.
Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure. This version has been updated specifically to cover EMV 3DS 2.2.
Visa Secure Program Guide – Visa Supplemental Requirements	Version 1.1 8th August 2019	This document is for Visa Secure and its use to support authentication of payment transactions
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 1.0 October 2019	Guide summarising Visa rules relevant to the application of PSD2 SCA.
Visa Biometrics information on the Visa Developer Center	N/A	Additional information on the service and the API https://developer.visa.com/capabilities/biometrics
Visa Technology Partner Portal	N/A	Portal with additional resources including details on EMV 3DS available at: https://technologypartner.visa.com/Library/3DSecure2.aspx
Visa Secure using EMV 3DS User Experience Guidelines	N/A	User experience guidelines for design and implementation of 3DS challenge screens available at: https://developer.visa.com/pages/visa-3d-secure
Visa 3DS 2.0 Performance Program Rules	VBN 25 October 2018	Summary of Visa requirements and rules on Issuers, Acquirers and merchants for implementation of EMV 3DS

Document/Resource	Version/Date	Description
3DS Performance Rules FAQ		Summarises Visa Performance Program rules for Issuers and Acquirers
Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance	5 September 2019	VBN stating Visa requirements for the implementation of EMV 3DS.
European Banking Authority: Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication	13 March 2018	Regulatory Technical Standards document (RTS) that describes the regulatory requirement to apply SCA under PSD2 and the requirements for factors and elements. Available at: https://eur-lex.europa.eu/eli/reg_del/2018/389/oj
Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2	21 June 2019	EBA Opinion paper that defines in more detail what may or may not constitute a compliant element in each factor category according to the PSD2 SCA regulation. Available at: https://ec.europa.eu/info/publications/190621-eba-opinion-strong-customer-authentication_en

Visa documents available via Visa Online unless otherwise stated.