European EMV 3DS 2.2.0 Implementation Guide

October 2019

Version 1.0
30 October 2019

EMV 3DS 2.2.0 optimises the application of PSD2 SCA

3-D Secure is the leading industry standard solution that allows Issuers, Acquirers and merchants to apply Strong Customer Authentication (SCA) as required by PSD2.

The latest version, EMV 3DS 2.2.0, provides critical new functionality that is fundamental to the optimisation of the application of PSD2 SCA and permitted exemptions.

As a result, Visa requires that Issuers support EMV 3DS 2.2.0 by September 14 2020 and strongly encourages merchants and Acquirers to support it as early as possible.

This guide summarises the new SCA functionality that EMV 3DS 2.2.0 offers for e-commerce transactions. It also highlights key implementation considerations relevant to Issuers, Acquirers and merchants.

More information on EMV 3DS, how it works and considerations around implementing and supporting earlier versions of 3-D Secure (3DS 1.0 and EMV 3DS 2.2.1) can be found in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0* and Visa Secure Implementation Guides.

EMV 3DS 2.2.0 Critical New Functionality

- **Optimises** the SCA user experience for biometric and Out of Band (OOB) authentication
- **Maximises** the ability of merchants and Acquirers to take advantage of SCA exemptions
- **Enables** Visa SCA products including Visa Trusted Listing and Visa Delegated Authentication
- **Allows** SCA and exemptions to be applied in complex merchant use cases such as travel

What is new in EMV 3DS 2.2.0:

EMV 3DS 2.2.0 delivers the following key features that are not available in previous versions of 3-D Secure.

Versions compared

Notable Features	3DS 1.0	EMV 3DS 2.1.0	EMV 3DS 2.2.0
Out-of-Band (OOB)/Biometric Mobile banking app integration	N	Basic	Y
3DS Requestor Environment - 3RI[1]			
• Non Payment authentication	N	Y	Y
• Payment authentication with ability to obtain, refresh and regenerate CAVV	N	Y[2]	Y
• Decoupled authentication	N	N	Y
Acquirer Exemption indicators			
• Transaction Risk Analysis (TRA) performed prior to authentication	N	N	Y
• Trusted beneficiaries (whitelisting)	N	N	Y
• Delegated Authentication	N	N	Y
Additional device compatibility e.g. gaming consoles[3]	N	Y	Y

The new indicator fields

New 3DS Requestor Challenge Indicator Field Values Introduced in EMV 3DS 2.2.0	
05	No challenge requested (TRA already performed)
06	No challenge requested (data share only)
07	No challenge requested (SCA is already performed)
08	No challenge requested (utilise trusted beneficiaries exemption of no challenge required)
09	Challenge requested (trusted beneficiaries prompt requested if challenge required)

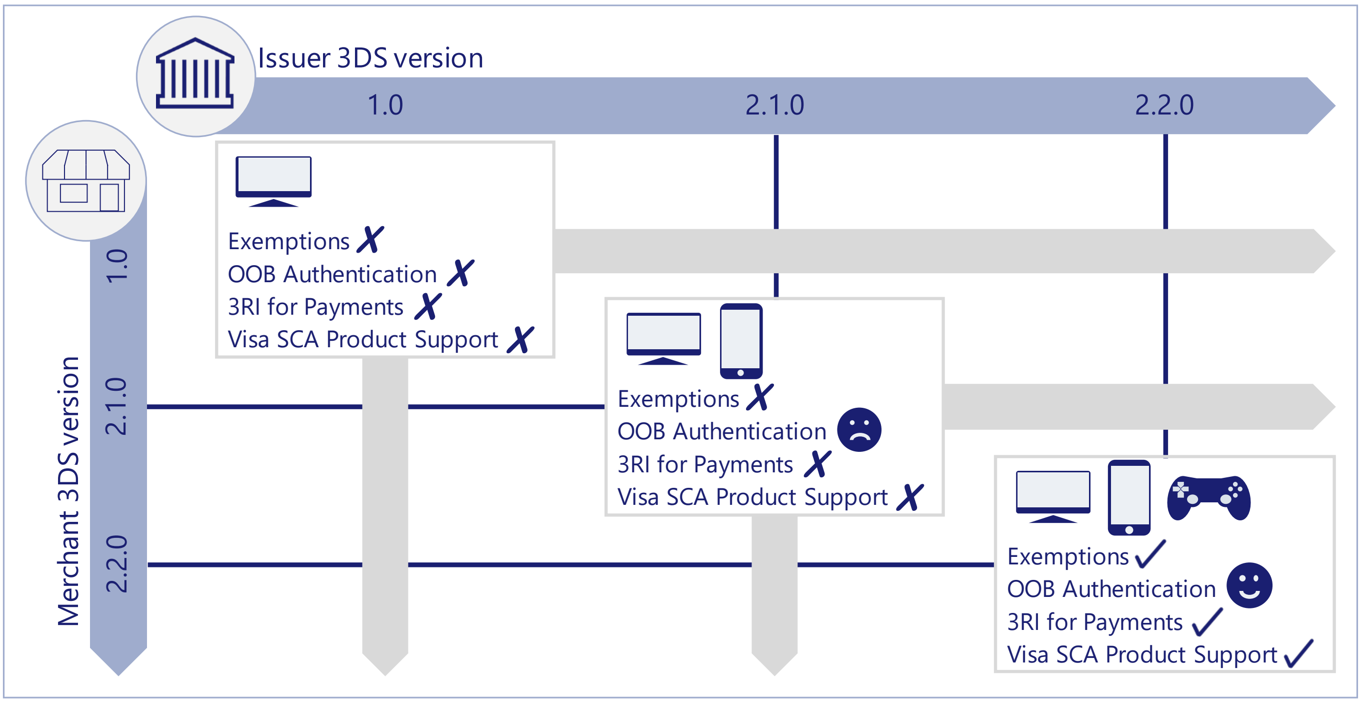
EMV 3DS 2.2.0 introduces five new values for the 3DS Requestor Challenge Indicator field in the Authentication Request message to support application of exemptions and delegated authentication.

To ensure that features are fully available, both merchant and Issuer must support EMV 3DS 2.2.0. If the parties support different versions of 3DS, the supported functionality defaults to the lower version, as illustrated overleaf:

[1] 3RI is a 3DS transaction type initiated by a merchant to confirm that an account is still valid or for Cardholder authentication. 3RI supports a number of complex payment use cases. For more information see page 5.

[2] Visa has defined a method for EMV 3DS 2.1 to support 3RI purchase transactions. Please note this approach is specific to Visa cards and is not included in the EMV 3DS specification.

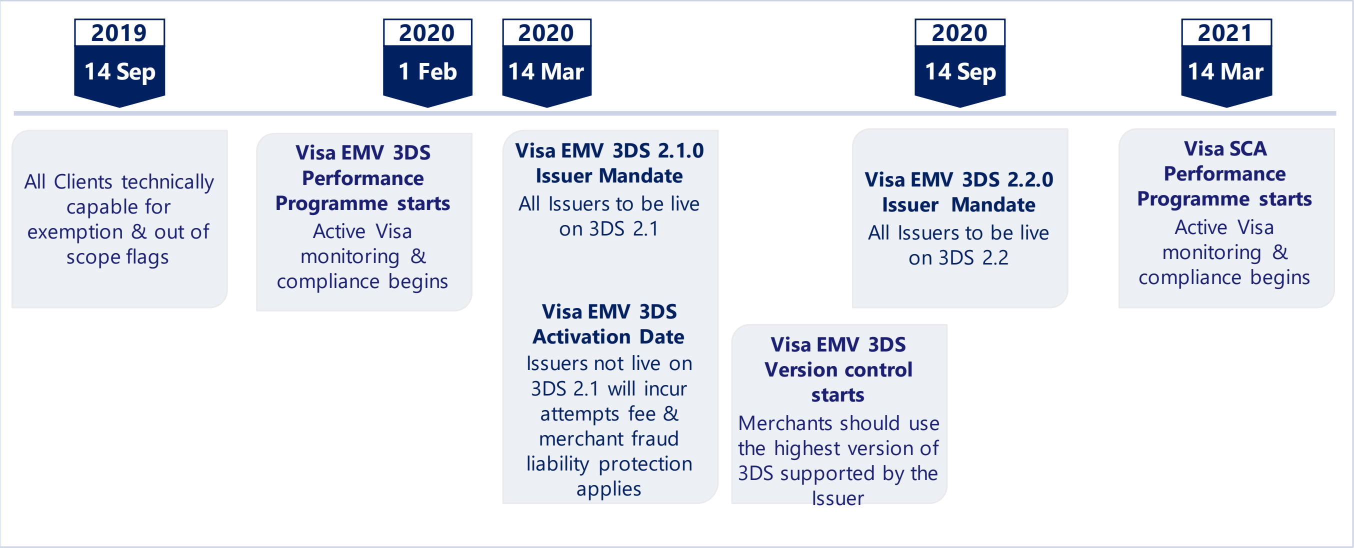
[3] Support of additional device information is outlined the *EMV 3-D Secure SDK—Device Information Data Version 1.3*



Note: Visa SCA products include Visa Trusted Listing and the Visa Delegated Authentication Program

EMV 3DS 2.2.0: Visa implementation timescales

Enablement of EMV 3DS 2.2.0 across the ecosystem is an important step in achieving SCA regulatory compliance. Visa is implementing a technology roadmap to help ensure smooth industry-wide deployment of EMV 3DS.



2019 14 Sep
All Clients technically capable for exemption & out of scope flags

2020 1 Feb
Visa EMV 3DS Performance Programme starts
Active Visa monitoring & compliance begins

2020 14 Mar
Visa EMV 3DS 2.1.0 Issuer Mandate
All Issuers to be live on 3DS 2.1

Visa EMV 3DS Activation Date
Issuers not live on 3DS 2.1 will incur attempts fee & merchant fraud liability protection applies

Visa EMV 3DS Version control starts
Merchants should use the highest version of 3DS supported by the Issuer

2020 14 Sep
Visa EMV 3DS 2.2.0 Issuer Mandate
All Issuers to be live on 3DS 2.2

2021 14 Mar
Visa SCA Performance Programme starts
Active Visa monitoring & compliance begins

Visa expects Issuers in Europe to deploy EMV 3DS 2.1.0 by **14 March 2020** and to deploy EMV 3DS 2.2.0 by **14 September 2020**. We also strongly encourage merchants to support EMV 3DS 2.2.0 as early as possible in order to fully support the SCA exemptions and optimise customer checkout experiences.[4]

[4] For more information see *Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance, Article ID: AI09310, 5 September 2019*

EMV 3DS 2.2.0 Technical Overview

3DS Requestor Initiated (3RI) payments

3DS Requestor Initiated (3RI) is a 3-D Secure transaction initiated by a merchant when the Cardholder is not available, either to confirm that an account is still valid or for Cardholder authentication.

3RI can be used to enable merchants to effectively manage some complex payment use cases.

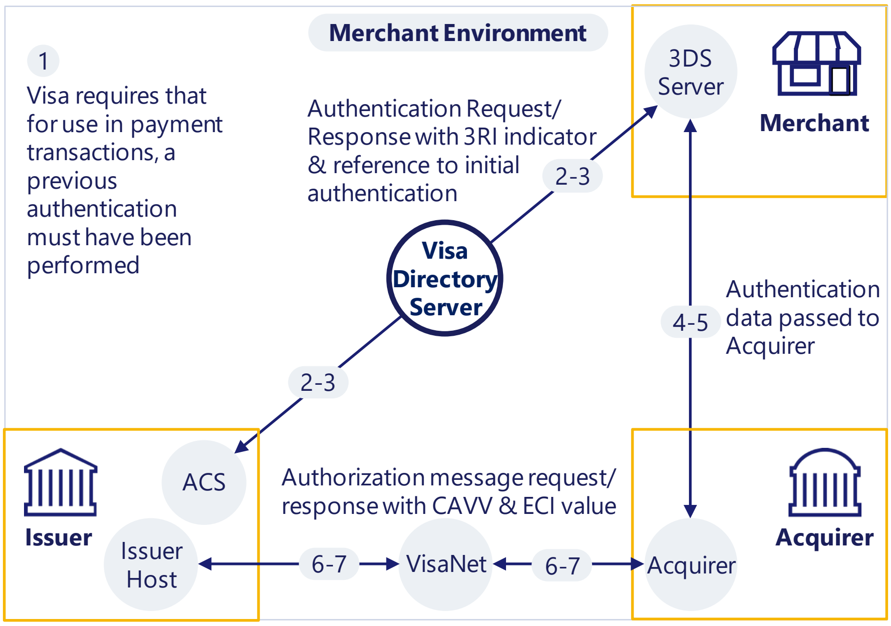
For example, a 3RI transaction enables the merchant to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions previously authenticated.

For Issuers, provision of this prior transaction data improves risk management and provides secondary evaluation on a previously authenticated transaction. This feature allows merchants who have performed authentication for a transaction to maintain their fraud liability protection and provide evidence that SCA has previously taken place - under legitimate circumstances, such as delayed or split shipment.

Example Complex Use Cases Supported by 3RI

- **Allowing** an authorized entity in a Multi-Party Commerce scenario to request a CAVV on behalf of a merchant
- **Allowing** a merchant to obtain a new CAVV in the case of split or delayed shipment when one or more items are not ready for shipment until a much later date
- **Requesting** a new CAVV to maintain liability protection and provide evidence that SCA has previously taken place - when authorization is sought more than 90 days after a transaction has been authenticated

The 3RI process flow


Merchant Environment
1
Visa requires that for use in payment transactions, a previous authentication must have been performed
Authentication Request/ Response with 3RI indicator & reference to initial authentication
2-3
3DS Server
Merchant
Visa Directory Server
4-5
Authentication data passed to Acquirer
2-3
ACS
Issuer
Issuer Host
Authorization message request/ response with CAVV & ECI value
6-7
VisaNet
6-7
Acquirer
Acquirer

The 3DS 3RI flow is shown on the left.

Detailed examples of where this may be used for specific transaction types are included in *PSD2 SCA for Remote Electronic Transactions Implementation Guide* and *Implementing Strong Customer Authentication for Travel and Hospitality*.

The TRA exemption indicator

The advantages of flagging the TRA exemption via 3DS

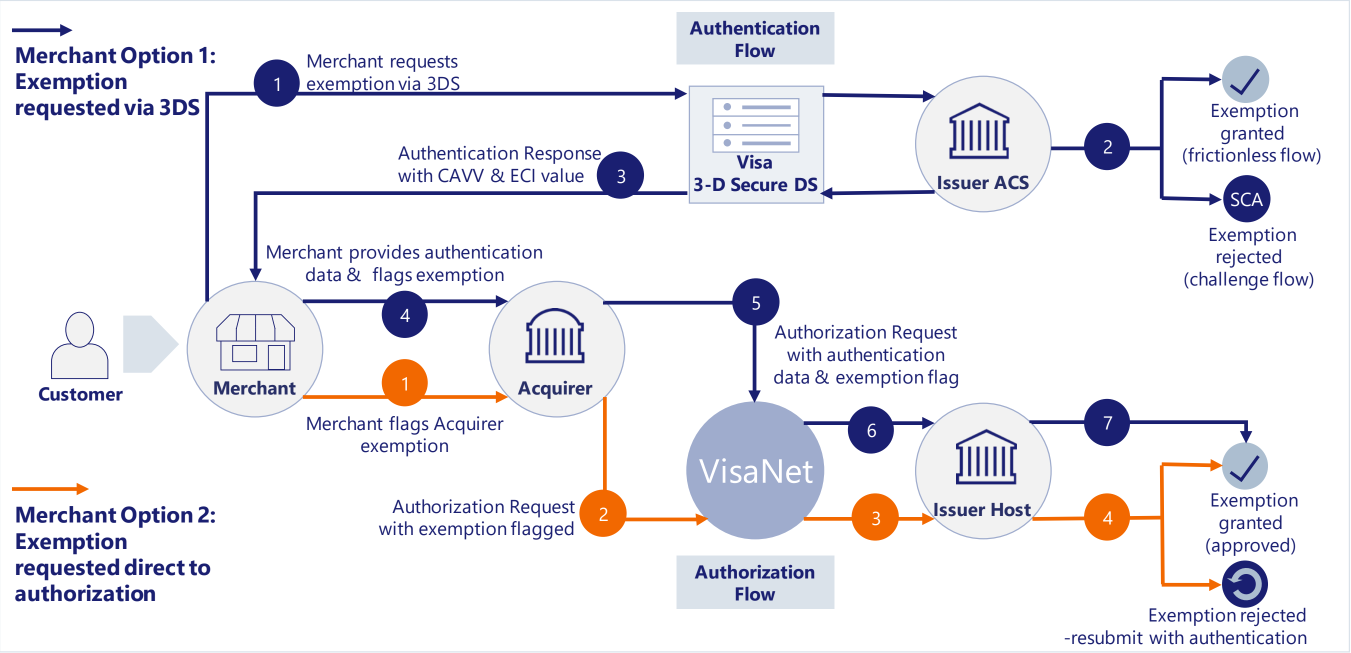
- **Better** approval rates, as the issuer will receive a CAVV – demonstrating that the issuer's Access Control Server (ACS) risk engine has approved the request for frictionless authentication
- **Should** the Issuer determine that SCA is still required (i.e. Transaction considered high risk), following a 3DS TRA exemption request, they can simply initiate a challenge within the 3DS flow.

TRA is key to delivering frictionless payment experiences for low-risk transactions. The TRA exemption may be applied by the Issuer or the Acquirer (who may outsource the application of TRA to the merchant). Use of the Acquirer exemption can allow merchants, with their own risk engines, to assess the risk of the transaction and influence the level of friction applied into their customer's payment journey.

EMV 3DS 2.2.0 includes the following indicator in the 3DS Requestor Challenge Indicator Field within the Authentication Request (AReq) Message[5]:

- **Value 05:** can be set by the merchant to indicate that transaction risk analysis has already been performed and no challenge is requested.

Following a successful application of the TRA exemption via EMV 3DS 2.2.0, the merchant/Acquirer should then use the TRA flag in Field 34 to signal this to the Issuer along with the CAVV. Alternatively, once TRA has been applied, the merchant/Acquirer can submit the transaction straight to authorization (using the appropriate flag in Field 34), as illustrated below.


Merchant Option 1: Exemption requested via 3DS
Authentication Flow
1
Merchant requests exemption via 3DS
Visa 3-D Secure DS
Issuer ACS
2
Exemption granted (frictionless flow)
SCA
Exemption rejected (challenge flow)
Authentication Response with CAVV & ECI value
3
Merchant provides authentication data & flags exemption
4
5
Authorization Request with authentication data & exemption flag
Customer
Merchant
Acquirer
1
Merchant flags Acquirer exemption
VisaNet
6
Issuer Host
7
Exemption granted (approved)
Exemption rejected -resubmit with authentication
Merchant Option 2: Exemption requested direct to authorization
Authorization Request with exemption flagged
2
3
4
Authorization Flow

[5] Refer to the EMVCo 3-D Secure Protocol and Core Functions Specification Version 2.2.0 for more information

The trusted beneficiaries exemption indicators

The trusted beneficiaries exemption allows for the cardholder to add a trusted merchant to a list of trusted beneficiaries held by their Issuer, completing an SCA challenge in the process. Further SCA application on subsequent transactions with the trusted merchant should generally not be required. This allows merchants with low fraud rates to offer a lower friction checkout experience to regular customers.

EMV 3DS 2.2.0 includes two indicator values in the 3DS Requestor Challenge Indicator Field within the Authentication Request (AReq) Message:

- **Value 08:** can be set by the merchant to indicate the customer has added the merchant to his/her list of trusted beneficiaries and no challenge is requested.
- **Value 09:** can be set by a merchant to request that the Issuer applies SCA and presents the customer with the option to add the merchant to their trusted list for future transactions.

These indicators are essential to the application of the trusted beneficiaries exemption.

Visa offers a solution to allow issuers and merchants to use the trusted beneficiaries exemption through its Visa Trusted Listing Program. For more information on how 3DS 2.2.0 supports Visa's Trusted Listing Program please see below.

Delegated Authentication indicator

Under the PSD2 regulation, PSPs can outsource the application of SCA to a qualified third party. EMV 3DS 2.2.0 includes the following indicator in the 3DS Requestor Challenge Indicator Field within the Authentication Request (AReq) Message:

- **Value 07:** can be set by the merchant to indicate that SCA has already been performed and no challenge is requested.

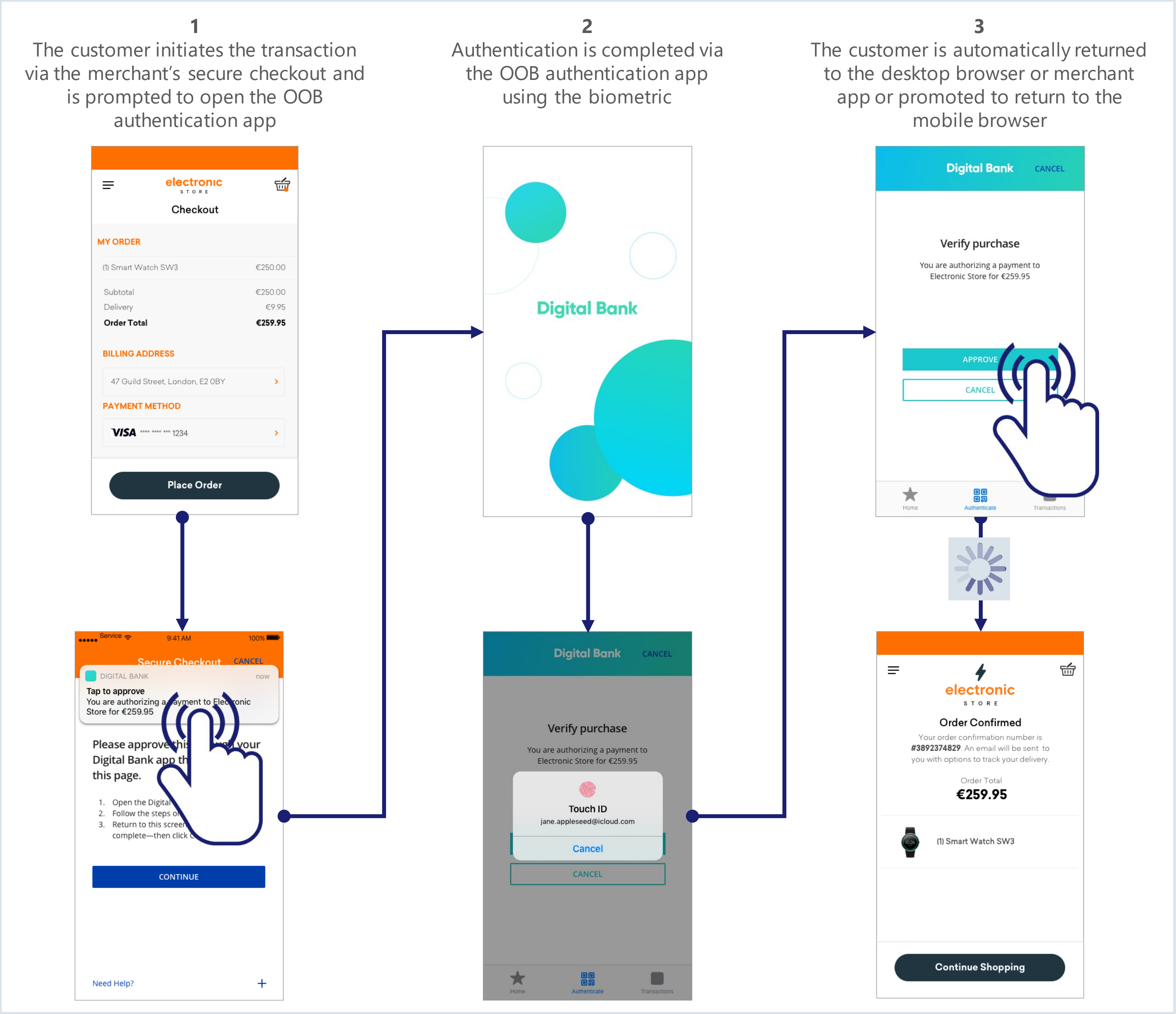
Following a successful application of the Delegated Authentication exemption via EMV 3DS 2.2.0, the merchant/Acquirer should then use the appropriate flag in Field 34 to signal this to the Issuer. Please see the Visa Delegated Authentication Program section on page 11 for an overview of how EMV 3DS 2.2.0 supports the Program.

Support of Out-of-Band (OOB) and biometrics.

OOB allows customers to be authenticated through a separate app, for example their mobile banking app, while making a purchase via a merchant website or app. OOB enables biometric authentication, which is the preferred long term solution for providing a PSD2 compliant authentication factor while minimising customer friction.

EMV 3DS 2.2.0 is the only protocol that provides a useable consumer flow for biometric authentication.

Seamless navigation between the browser or app-based checkout and the OOB authentication app is critical to minimising friction for the customer. EMV 3DS 2.1.0 does not allow a user friendly transfer between the merchant app and the Issuer app for OOB authentication. EMV 3DS 2.2.0 resolves the issue as it supports automatic redirection between the apps in most use cases (except for navigating from the OOB authentication app back to a mobile browser). A typical user experience flow is shown below:



1
The customer initiates the transaction via the merchant's secure checkout and is prompted to open the OOB authentication app

2
Authentication is completed via the OOB authentication app using the biometric

3
The customer is automatically returned to the desktop browser or merchant app or promoted to return to the mobile browser

Tap to approve
You are authorizing a payment to Electronic Store for €259.95

Please approve this through your Digital Bank app then return to this page.

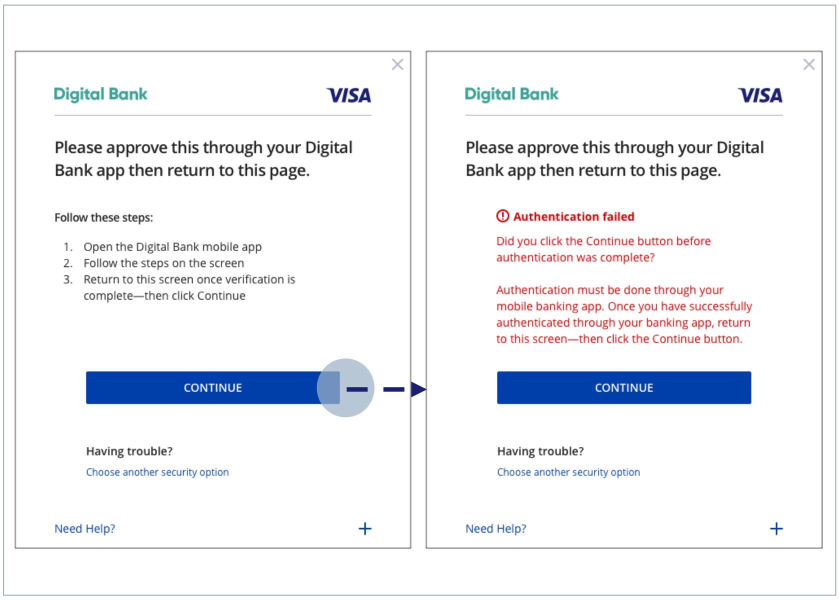
1. Open the Digital
2. Follow the steps o
3. Return to this screen complete—then click C

Verify purchase
You are authorizing a payment to Electronic Store for €259.95

Verify purchase
You are authorizing a payment to Electronic Store for €259.95

Order Confirmed
Your order confirmation number is **#3892374829**. An email will be sent to you with options to track your delivery.

Visa strongly recommends that Issuers and ACS providers implementing biometric OOB authentication, only do so if they support EMV 3DS 2.2.0.



Digital Bank VISA

Please approve this through your Digital Bank app then return to this page.

Follow these steps:

1. Open the Digital Bank mobile app
2. Follow the steps on the screen
3. Return to this screen once verification is complete—then click Continue

Digital Bank VISA

Please approve this through your Digital Bank app then return to this page.

Authentication failed

Did you click the Continue button before authentication was complete?

Authentication must be done through your mobile banking app. Once you have successfully authenticated through your banking app, return to this screen—then click the Continue button.

Note:

There are some significant user experience design shortcomings in the way EMV 3DS 2.1.0 handles the transfer between the apps which results in consumer confusion and high levels of abandonment. The main cause of confusion is the inclusion of a prominent continue button - which should not be clicked until the user has manually opened the Issuer app and authentication is successfully completed:

OOB authentication UX functionality by EMV 3DS version

	Supported by EMV 3DS 2.1.0	Supported by EMV 3DS 2.2.0
Mobile Browser experience		
• Navigating to the OOB Authentication App	Yes	Yes
• Navigating from the OOB Authentication App back to the mobile browser after authentication	No	No[6]
• Automatically proceeding with the purchase flow after OOB authentication	Yes	Yes
App experience		
• Navigating to the OOB Authentication App	Yes	Yes
• Navigating from the OOB Authentication App back to the mobile app after authentication	No	Yes
• Automatically proceeding with the purchase flow after OOB authentication	No	Yes

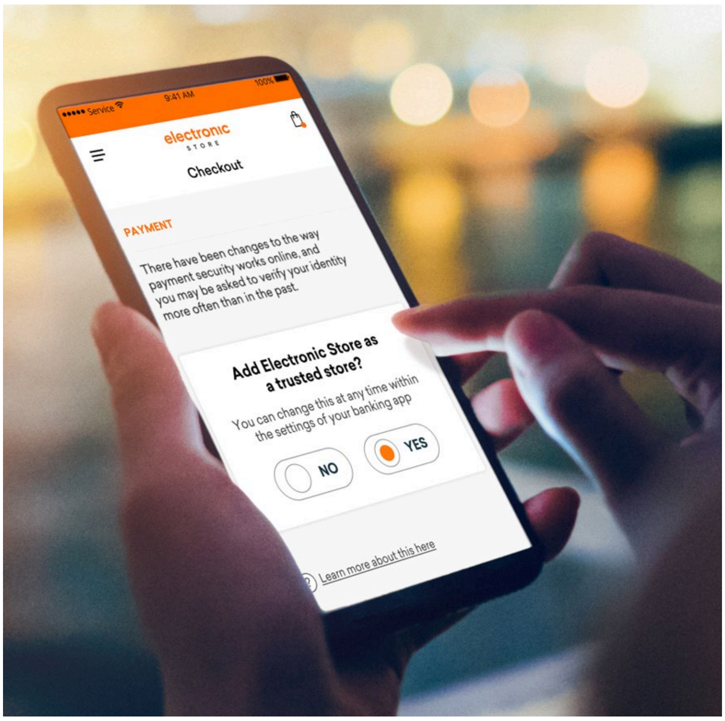
More guidance on optimising the OOB biometric authentication user experience is given in the *PSD2 SCA for Remote Electronic Transactions Implementation Guide.*

[6] Updates to 3DS are being planned that will provide a more streamlined experience

EMV 3DS 2.2.0 and Visa PSD2 SCA solutions

Issuer and merchant support of EMV 3DS 2.2.0 is required in order to implement the following Visa PSD2 SCA solutions.

Visa Trusted Listing Program

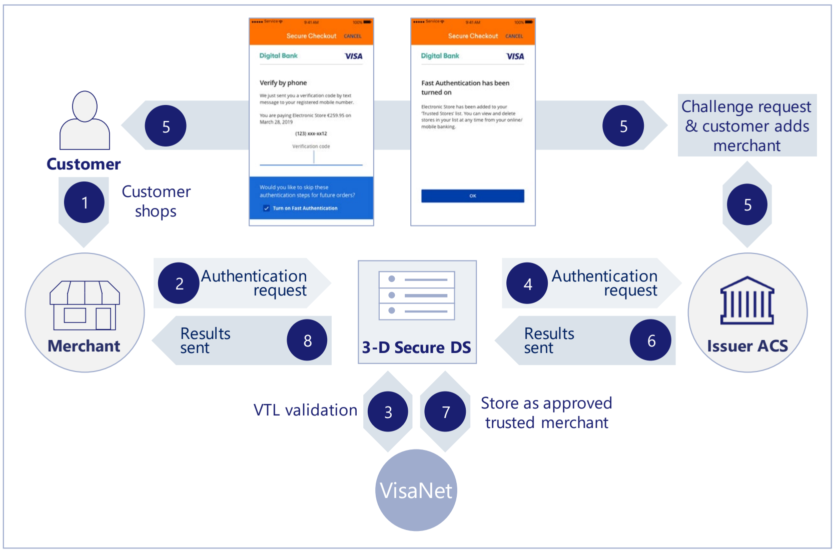


Service
9:41 AM
100%
electronic
STORE
Checkout
PAYMENT
There have been changes to the way payment security works online, and you may be asked to verify your identity more often than in the past.
Add Electronic Store as a trusted store?
You can change this at any time within the settings of your banking app
NO
YES
Learn more about this here

The Visa Trusted Listing (VTL) Program provides an effective framework for enabling the PSD2 trusted beneficiaries exemption.

Once an Issuer and merchant are enrolled in the VTL program, a customer may add a participating merchant to their Trusted List.

The merchant can display a message telling the customer about the option to add them to their Trusted List. This can be done during a purchase, or for example, when a purchase is completed, when a customer is saving a card on file or using a merchant wallet. In each case, the merchant will send a request through an EMV 3DS 2.2.0 Authentication Request requesting the Issuer displays the listing option to the customer. If the Issuer chooses to present the option and the customer agrees that they wish to list the merchant, they will complete a SCA challenge and the merchant will be added to the customer's Trusted List. If the addition takes place during a purchase the SCA challenge also authenticates that purchase transaction. The flow is shown below:



Service
9:41 AM
100%
Secure Checkout
CANCEL
Digital Bank
VISA
Verify by phone
We just sent you a verification code by text message to your registered mobile number.
You are paying Electronic Store €259.95 on March 28, 2019
(123) xxx-xx12
Verification code
Would you like to skip these authentication steps for future orders?
✓ Turn on Fast Authentication
Service
9:41 AM
100%
Secure Checkout
CANCEL
Digital Bank
VISA
Fast Authentication has been turned on
Electronic Store has been added to your 'Trusted Stores' list. You can view and delete stores in your list at any time from your online/ mobile banking.
OK
5
5
Challenge request & customer adds merchant
Customer
1
Customer shops
5
Merchant
2
Authentication request
Results sent
8
3-D Secure DS
4
Authentication request
Results sent
6
Issuer ACS
VTL validation
3
7
Store as approved trusted merchant
VisaNet

In order to support VTL, merchants and their 3DS Servers will need to be enabled for EMV 3DS 2.2.0. Merchants will need to work with their 3DS Server Provider to ensure logic is in place to know when to flag a transaction for Visa Trusted Listing. Note VTL only supports Visa transactions.

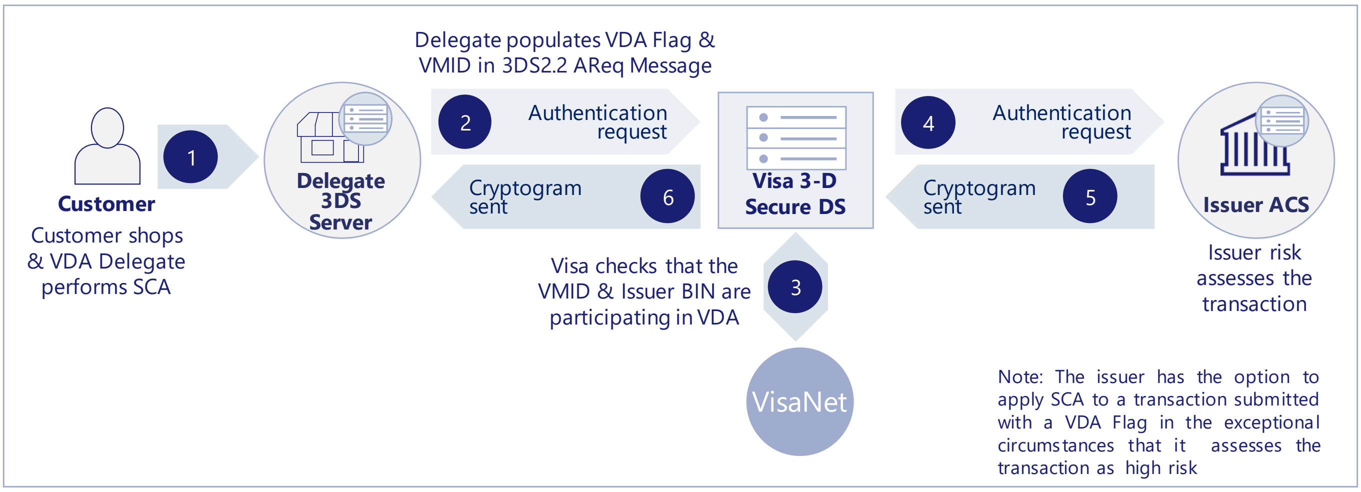
Merchants interested in becoming enrolled in Visa Trusted Listing will also need to submit a registration form through their Acquirer. For more information please refer to the *Visa Trusted Listing Program Implementation Guide.*

Visa Delegated Authentication Program

The Visa Delegated Authentication (VDA) Program allows Payment Service Providers (PSPs) to delegate the authentication process to qualified third parties, or delegates, as permitted under PSD2.

This allows delegates, such as merchants, who have invested in risk engine technologies to define a consistent consumer payment experience in cases where SCA is required. Issuers may also benefit from higher sales conversions with minimal incremental investment.

The authentication flow for VDA enabled by EMV 3DS 2.2.0 is shown below.



For detail on the EMV 3DS 2.2.0 fields used to flag a Visa Delegated Authentication transaction please refer to the *Visa Delegated Authentication Program Implementation Guide*.

Delegates using EMV 3DS 2.2.0 to indicate a VDA transaction will need to work with their 3DS Server Provider to ensure logic is in place to know when to flag a transaction as VDA eligible. Note VDA only supports Visa transactions.

Delegates interested in participating in VDA should work with their Acquirer to complete a Readiness Questionnaire.

Issuers do not need to be EMV 3DS 2.2.0 ready to accept these requests. However, Issuers will need to work with their ACS Providers to have the right logic for VDA transactions[7].

[7] For more information on the required logic for VDA transactions when the Issuer is not EMV 3DS 2.2.0 ready, refer to *Visa's 3-D Secure Programs' Cardholder Authentication Verification Value (CAVV) Guide Version 3.0.*

Implementing EMV 3DS 2.2.0

Visa strongly advises merchants and clients to adopt EMV 3DS 2.2.0 as early as possible.

Merchants and clients who are unable to immediately adopt EMV 3DS 2.2.0 should initially adopt version 2.1.0 and then quickly transition to version 2.2.0 once they are able to do so.

Issuers should consider the following when upgrading to EMV 3DS 2.2.0:

Issuer Checklist	
✓	Check that your ACS or ACS vendor has passed all required EMV 3DS 2.2.0 certification (EMVCo and Visa)
✓	If you do not operate your own ACS, ensure you are using either of the following to operate the ACS or Directory Server (DS): • The Visa Consumer Authentication Service (VCAS) • An ACS or DS service provider listed on the Visa Global Registry of Service Providers
✓	Agree an upgrade plan with your ACS vendor. The ACS vendor will take care of the majority of the technical work
✓	Ensure you are able to process the new exemption indicators. Your ACS vendor will handle this step in the authentication flow
✓	Take a risk based approach to transactions flagged with exemptions. Do not routinely apply SCA challenges to transactions that are flagged for the TRA or trusted beneficiaries exemptions - unless your ACS risk engine identifies a transaction as high risk
✓	Ensure SCA challenges are applied when a merchant/acquirer requests application of SCA, for example when setting up a Merchant Initiated Transaction (MIT) agreement
✓	Ensure compliance with Visa's rules for application of PSD2 SCA and 3DS. Notably the requirements to support Risk Based Authentication and biometric authentication, responding to an authentication request within 5 seconds, and maintaining authentication abandonment rates below 5%[8, 9]

[8] For more information on Visa rules relevant to PSD2 and 3DS see *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*

[9] Performance rules apply to all versions of EMV 3DS

Merchants should consider the following when upgrading to EMV 3DS 2.2.0:

Merchant Checklist	
✓	Check that your 3DS Server/SDK vendor has passed all required EMV 3DS 2.2.0 certification (EMVCo and Visa)
✓	If you would like to take advantage of the Acquirer TRA exemption, the trusted beneficiaries exemption and/or delegated authentication, ensure you/your vendor can support the 3DS requestor challenge field indicators
✓	If you would like to take advantage of the trusted beneficiaries exemption and/or delegated authentication consider enrolling in the Visa Trusted Listing Program and/or the Visa Delegated Authentication Program[10]

EMV 3DS 2.2.0 3DS Server and ACS Vendors must ensure that they undertake the following before licensing their software or implementing their products and/or services with merchants and/or Issuers:

3DS Vendor Checklist	
✓	**Prerequisites:** Vendors must ensure that they have completed EMVCo testing, and have, where required, signed a Visa EMV 3DS Product Provider Agreement and have a Visa Business ID
✓	**Visa Security Requirements:** Vendors must ensure that, where required, they complete PCI DSS assessment and enrol in Visa's 3rd Party Agent Program
✓	**Visa Product Testing:** Vendors must ensure that they complete the Visa EMV 3DS product testing and approval process
✓	**Digital Certificates:** Vendors that are required to do so must ensure, pre-implementation, that they have requested Visa digital certificates
✓	**Use of Directory Servers**: Vendors must ensure that they only use Directory Servers listed on the *Visa Global Registry of Service Providers* if they are not using the Visa Directory Server

The Visa certification process allows for certification of both EMV 3DS 2.1.0 and 3DS 2.2.0 at the same time, subject to prior EMVCo certification for both 3DS versions. For more information on the applicability and completion for these requirements please refer to *Visa 3-D Secure (3DS) 2.0 Product Provider (3DS Server) Pre-Implementation Guide and Checklist* and/or *Visa 3-D Secure (3DS) 2.0 Product Provider (ACS) Pre-Implementation Guide and Checklist.*

[10] Details of qualification requirements and enrolment process can be found in *Visa Trusted Listing Program Implementation Guide* and *Visa Delegated Authentication Program Implementation Guide.*

References

Document/Resource	Version/Date	Description
EMVCo 3-D Secure Specification	**V2.2.0**	**Specification for the core 3DS technology that includes message flows, field values etc. 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 2.2.0.**
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 2.2.0.**
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.
Implementing Strong Customer Authentication for Travel and Hospitality	Version 1.1 11th March 2019	Provides merchants and Acquirers with examples of performing SCA across common payment use cases common in the travel and hospitality sectors.
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
Visa Secure Cardholder Authentication Verification Value (CAVV) Guide	Version 3.0 April 2019	Provides detailed information on CAVV creation and verification and use in authorization for both 3DS 1.0 and EMV 3DS.
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.

Document/Resource	Version/Date	Description
Visa Delegated Authentication Program Implementation Guide	Version 1.0 5th April 2019	Describes the Visa Delegated Authentication Program and provides practical guidance to Issuers, Acquirers, technology providers, Delegates, and potential Delegates who participate in the Program on implementation and usage of the solution.
Visa Trusted Listing Program Implementation Guide	Version 1.0 9th April 2019	Describes the Visa Trusted Listing Program and provides practical guidance to Issuers, Acquirers, technology providers, and Merchants who participate in the Visa Trusted Listing Program on implementation and usage of the solution.
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 3DS 2.0 Performance Program Rules	VBN 25th October 2018	Summary of Visa requirements and rules on Issuers, Acquirers and merchants for implementation of EMV 3DS
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.