let's make payment happen

CCV

Strong Customer Authentication

January 2020

Table of Contents

Preamble

What is Strong Customer Authentication (SCA)?

A new set of rules that will change how consumers confirm their identity when making purchases online.

When does it apply?

The rules apply in full for card payments, starting 31 December 2020 in the EU. This deadline will not change. Card issuers will start enforcing these new rules as of September 2020.

Why does it matter to you?

If you do not take action, e-commerce card-based payment transactions that are non-compliant will eventually be declined. Implementation of these new rules may require testing and implementing specific changes to your payment process.
We therefore encourage you to take immediate action to ensure you are not at risk of declined transactions which may impact your business.

What should you do?

Urgent action should be taken by businesses with an online presence. You should work together with CCV to make sure that your implementation will comply with the new rules in time.

Time for action

This whitepaper provides important information for businesses of all sizes looking to avoid customers experiencing declined e-commerce transactions after the Strong Customer Authentication enforcement deadline of 31 December 2020.

After this point, card issuers will start declining non-compliant transactions. As of September, Dutch issuers will start declining transactions that are not compliant to these rules. If you have an online presence, we actively encourage you to read this whitepaper and to get in touch with CCV. This should be done with urgency due to the implementation lead times and the testing period required.

What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a new set of rules that will change how consumers and business customers confirm their identity when making purchases online to help further protect them from fraud.

Following its implementation, consumers shopping or banking online will often need to undertake an extra step to confirm their identity. For example, the card issuer or provider (this could be a bank) may use one of a number of ways to verify a purchase or login, such as a passcode via text message, a phone call to the consumer's landline, the use of a card reader or the use of a smartphone app. Under the new rules, all parties are required to make the necessary changes to enable consumers to authenticate their actions in a manner compliant with the underlying regulation.

Background

Starting 14 September 2019, changes were introduced to online payments in order to provide further protection to customers. Under the Payment Service Directive 2 (PSD2), Strong Customer Authentication (SCA) is required where a payment service user (customer) initiates an electronic payment transaction.

The European Banking Authority (EBA) allowed for regulatory flexibility on enforcement[1] until 31 December 2020. The aim was to ensure all parties move towards full compliance in an orderly manner, thus avoiding negative impact for both consumers and merchants.

The new enforcement date takes effect on 31 December 2020 across the EU. **All merchants, acquirers, gateways, and issuing banks or payment service providers must be ready to support SCA** from this date, to avoid consumers experiencing declined e-commerce transactions and a loss of business for webshop owners. CCV encourages all parties to take action. This whitepaper sets out what is required and by when, so that you can be ready for this change.

[1] EBA opinion issued in October 2019 provided for enforcement of the new rules to start after 31 December 2020. Most member states have aligned to this deadline.

What does SCA require?

SCA will be required for all online (website or app) card-based payments, unless one of the limited exceptions or exemptions[2] is applicable. For card payments this means **e-commerce transactions that are unable to be authenticated or those without exemptions will be declined after 31 December 2020.**

For merchants, this means you will need to work with CCV to ensure you upgrade your payment process to support a technology called EMV 3DSecure, in order to be able to cater for the new requirements. This often requires testing, so you should engage as soon as possible to avoid any delay.

What is EMV3DSecure?

EMV 3DSecure (EMV 3DS) is a technology created by the major card schemes that can be used to facilitate Strong Customer Authentication for online card payments. This new version of 3DS makes it possible for your customers to perform a payment without an extra authentication

For further details, please refer to Appendix Table 1 – SCA E-commerce Compliance for the definition of SCA-compliant versus non-compliant transactions.

[2] Please refer to the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication for more information about SCA exceptions and exemptions.

What should I do as a business with an online presence?

Are you a customer of CCV? Get in touch with us via onlinepayments@ccv.eu or for any technical questions about our API via psp-support@ccvlab.eu.

If you are a new CCV customer, you can get in touch with one of our local offices.

Get in contact with one of our colleagues to make sure your payment solution is configured correctly to comply with this regulation. We will inform and help you with the actions you need to take in order to prepare and meet the agreed timeline.

We will guide you through the steps:

1. Which version of 3DSecure to use (the technology which enables SCA) and what the new version of 3DS means to your business;

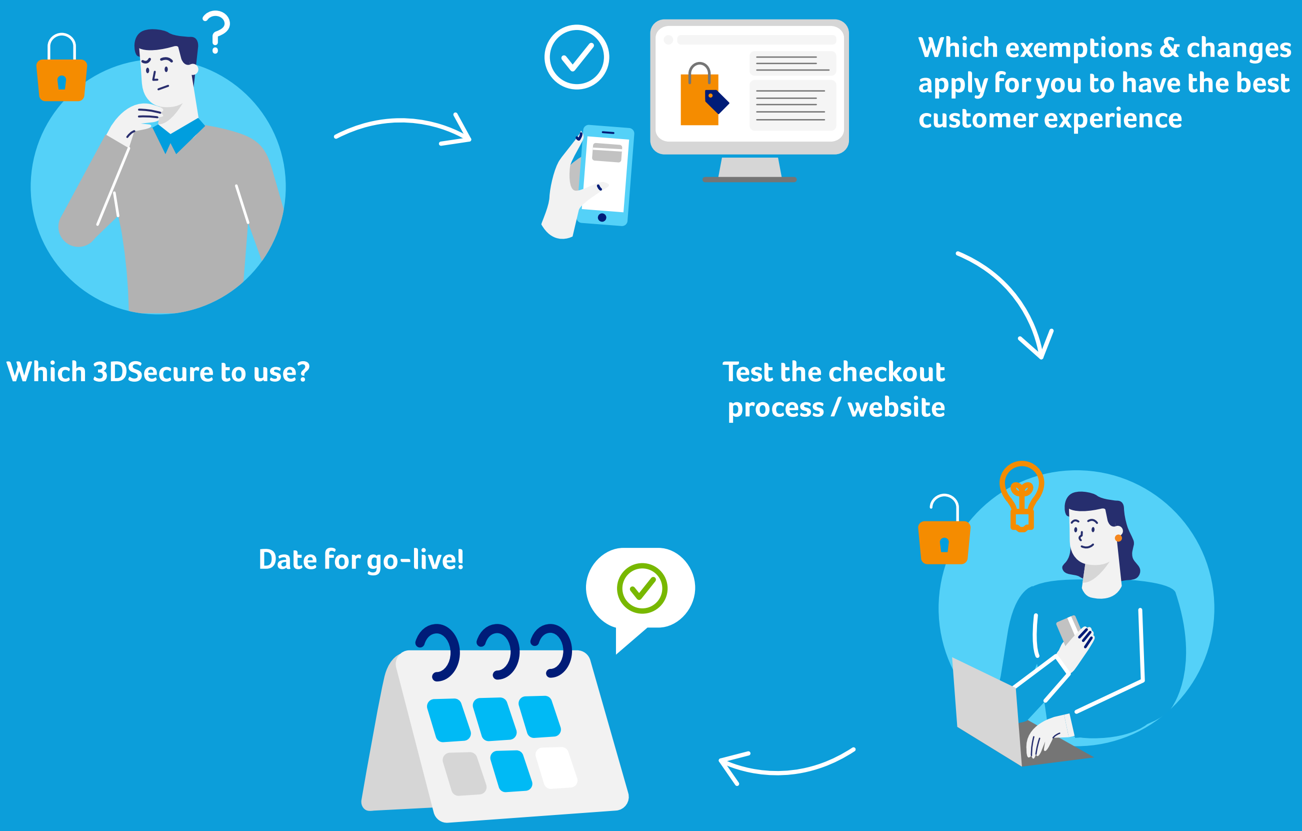
2. Which exemptions you might be able to use to encourage a better customer experience, and how to use these;

3. Which changes will apply for you for the interface to start the payment process. Please note that this interface will need more parameters than in your current interface;

4. Dates and windows for testing your checkout process/website;

5. Date for go-live.

We encourage you as a merchant to make plans as soon as possible, due to the amount of change that may be required.



Which 3DSecure to use?

Which exemptions & changes apply for you to have the best customer experience

Test the checkout process / website

Date for go-live!

To whom does this apply?

The key aim is to minimize any costumer impact by avoiding a cliff-edge implementation around the enforcement deadline. This means all parties in the ecosystem need to ensure all necessary preparations are carried out during Q2 2020 if not before.

For merchants already supporting 3DS, the changes will be adding new information fields to the transaction initiation. These fields will be specified in the CCV supplied interface documentation. Adding these fields will also increase the possibility that the customer check-out will be frictionless, meaning that no authentication by the cardholder may be required.

For merchants not supporting 3DS today, this will impact their business as these transactions will be declined if no action is taken. CCV will take action to ensure they are working towards operational readiness ahead of the deadline.

3DS2.x is required in order to achieve operational readiness

For card payments, the common industry practice to facilitate Strong Customer Authentication is something called 3DSecure (3DS[3]). This technology is also required in order to facilitate the use of SCA exemptions and enable SCA when needed. There are currently three main versions of 3DSecure on the market. Versions 2.1 and 2.2 are summarised below.

» 3DSecure version 1.0

» EMV 3DSecure version 2.1[4]

» EMV 3DSecure version 2.2[4]

[3] EMV Three-Domain Secure (3DS) is a messaging protocol developed by EMVCo to enable consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorised CNP transactions and protects the merchant from CNP exposure to fraud. The three domains consist of the merchant / acquirer domain, issuer domain, and the interoperability domain
(e.g. Payment Systems).

[4] Mastercard has developed 3DS message extensions which are applicable to 3DS2.1 (3DS2.1. with merchant extensions) and 3DS2.2 (3DS2.2 with merchant extensions). This message extensions will facilitate the usage of SCA exemptions via 3DS2.1. Please refer to the Appendix – Table 3 for more information

Table 1: SCA Ecommerce Compliance

Applicable as of December 31, 2021

- Includes in-scope e-commerce card-based payment transactions only and excludes mail and telephone order, one-leg-out and merchant-initiated transactions (MIT)
- Although MIT is out of scope, the first transaction (recurring payment set up) requires step up to Strong Customer Authentication. Therefore, references to MIT are made within the table below

	Via 3D Secure	Directly to Authorisation
Compliant Transactions	» Transactions with an acquirer exemption flag (Acquirer TRA) » Transactions sent for issuers to step up (SCA) or use an issuer exemption (TRA, low value or trusted beneficiary flag) » Recurring payments set up (1st transaction) request for an issuer step up (SCA to be applied)	» Transactions flagged with an acquirer exemption flag (Acquirer TRA, low value) » MIT transactions with the relevant Auth Code or Transaction ID generated during recurring payments set up (1st transaction) ***This process will allow MIT transactions to be recognised as out-of-scope**
Non-Compliant Transactions	**Note:** All in-scope transactions need to be sent via 3DS unless they are sent directly to authorisation with an acquirer exemption flag	» Transactions sent directly to authorisation with no acquirer exemption flag » MIT transactions with no Auth Code or Transaction ID

Table 2: VISA and Mastercard 3DS Scheme Mandates

	Issuer mandate			Acquirer mandate		
	VISA	mastercard	[illegible]	VISA	mastercard	[illegible]
3DS2.1	March 2020	April 2019	October 2019	Optional	April 2019	October 2019
3DS2.1 with message extensions	TBC	July 2020	N/A Not supported	TBC	July 2020	N/A Not supported
3DS2.2	September 2020	No mandate in place	October 2020	October 2020	No mandate in place	October 2020
3DS2.2 with message extensions	September 2020	July 2020	N/A Not supported	October 2020	July 2020	N/A Not supported

Let’s make payment happen

Want to know more?

Get in touch with us
+31 (0) 88 228 9911
onlinepayments@ccv.eu
www.ccv.eu