



3-D SECURE 2.x

Information for merchants on the new 3-D Secure protocol

What you as a merchant have to consider



Since the announcement of the roll-out of 3-D Secure 2.x, EVO Payments has been dealing in depth with the requirements of the new procedure and would like to answer the essential questions on 3-D Secure 2.x for its customers and all interested merchants on the following pages.

Contents overview

On the following pages you can find out

- > how the new 3DS 2.x procedure works and how it differs from its predecessor,
- > which advantages and challenges are connected with an introduction of the procedure for you as a merchant,
- > whether you have to integrate 3-D Secure 2.x and which deadlines have to be observed.

3-D Secure and 3-D Secure 2.x at a glance



The 3-D Secure procedure

The globally standardized 3-D Secure Protocol (3DS), which was introduced in 2002, offers merchants and consumers additional security for the authentication of credit card transactions made online. With this procedure, online shoppers verify that they are the legal cardholder vis-à-vis their card-issuing bank (issuer). In contrast to a normal credit card payment process on the Internet, for which only the card data is required, 3-D Secure requires the additional entry of a code by the buyer in order to successfully complete the order process. This makes misuse of credit cards much more difficult.

At the same time, the card-issuing banks assume liability for fraudulent transactions that were successfully executed despite the use of the procedure. The prerequisite for the use of the procedure is that 3-D Secure is supported both by the card-issuing bank of the buyer and by the relevant online shop.



How does 3-D Secure 2.x differ from the conventional method?

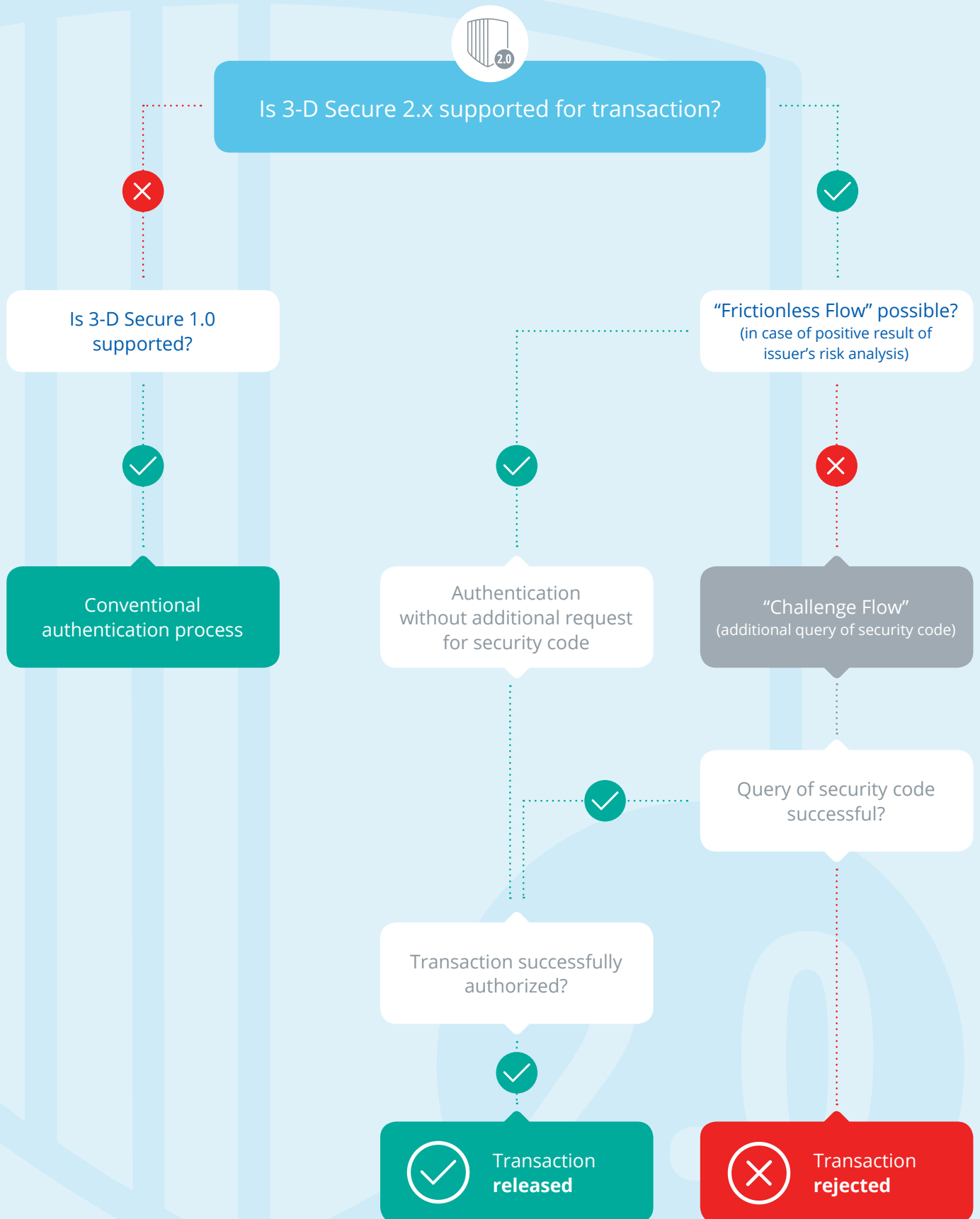
Essentially, 3-D Secure 2.x is a further development of the conventional 3-D Secure protocol. The automated transmission of up to 10 times the volume of transaction- and buyer-related data enables issuers to replace the previously static code query with a real-time risk analysis.

Each credit card order triggers the transmission of up to 100 data points to the issuer. The data is collected and forwarded both via the merchant's shop backend and via the Payment Service Provider (PSP), via which 3-D Secure 2.x is connected to the respective shop (see diagram). The transfer of data to the issuer takes place in the secure environment of a 3-D Secure server.

The subsequent real-time risk assessment of each transaction is the sole responsibility of the issuer. Analysis software calculates a scoring for each transaction based on data signals that indicate possible fraud attempts.

If a transaction is classified as low-risk, it is released without the buyer being asked to enter an additional code. If, on the other hand, there is an increased probability of fraud (applicable to a maximum of 5 percent of all credit card transactions), the buyer is requested to reconfirm his identity by SMS or e-mail. The process of risk assessment runs in the background, not perceptibly for the buyer. This means that in the majority of cases smooth payment process can be guaranteed without additional security information being requested.

Schematic sequence of the 3-D Secure process





Why is 3-D Secure 2.x being introduced?

The declared goal of 3-D Secure 2.x is to remedy the weaknesses of the conventional procedure, which have been criticized by merchants and buyers alike, and to meet the requirements of strong customer authentication (SCA), which will become legally binding for electronic payment procedures from September 14, 2019.

Since buyers will no longer have to enter a 3-D Secure code and the majority of credit card transactions do not require further information to be requested by the buyer, it is assumed that the new procedure will significantly reduce the number of aborted purchases in the checkout process. In addition, the individual, data-based risk assessment of each transaction promises even better protection against fraud.

Merchants who opt for the integration of 3DS 2.x also benefit from significantly improved usability for mobile and in-app purchases. Input windows for 3DS queries can now be displayed in a format adapted to the respective end device (responsive design). At the same time, the new process is no longer exclusively browser-based, but can also be integrated into the merchant's own shopping apps with the aid of ready-made software development kits (SDKs).

However, it should be noted that the relevant forms can only be adapted to the corporate design of the respective online shop to a very limited extent. If an authentication request is made in case of suspicion, the online buyer can still see that the form has been forwarded to the card-issuing institute.





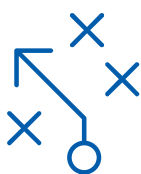
What data is transmitted and who is responsible for collecting it?

Data collected, processed and subsequently transferred to the 3-D Secure server by the merchant's Payment Service Provider (PSP) is:

- 01 **Credit card data** that must be collected and processed in accordance with the PCI DSS requirements
- 02 **Transaction-related data.** This includes the identification numbers required to assign the transaction and the merchant, as well as the purchase amount and currency.
- 03 **Browser information** that provides information about the end device used and the location of the user. This includes IP address, screen height and width as well as the browser language used.

The following data is recorded in the merchant's shop system and transferred to the 3-D Secure server via the PSP's payment interface. This is not mandatory for the 3DS 2.x procedure. However, their transmission is recommended in order to guarantee precise risk scoring:

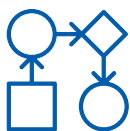
- 04 The complete **billing and delivery address** of the order.
- 05 Data recorded in the context of an existing **customer account**. This includes, but is not limited to, information on the duration of the customer account, the number of transactions carried out within certain time intervals, and the frequency with which passwords and delivery addresses are changed.
- 06 Data about **delivery details**, such as the chosen shipping method, availability of the goods, the delivery time window, the e-mail address in the case of digital goods, or the date of initial availability for unpublished products.



Is the transmission of all possible data points necessary?

No. EMVCo (the credit card industry association), the organisation responsible for defining the 3DS 2.x standard, distinguishes between mandatory and optional data. The latter includes all data collected during the ordering process from the merchant backend.

In order to be able to use the new 3DS 2.x procedure sensibly, however, it is strongly recommended that you enter and transfer all parameters: The more data that flows into the issuer's transaction analysis, the more precise the assessment of the probability of fraud in a transaction will be.



What are the challenges merchants are faced with in a changeover?

A changeover to the new 3DS 2.x procedure presents merchants with two key challenges that should be taken into account when assessing the timing of an integration:

- > Even though most of the technical adjustments have to be made by the issuers and payment service providers, merchants cannot avoid revising their ordering and checkout processes: Existing forms for creating customer accounts and guest check-outs must be extended by the required data fields and configured in coordination with the PSP to ensure smooth transfer of data via the interface.
- > The reaction of customers to the new process is difficult to assess. On the one hand, they must be informed about the type and scope of the additional data transmitted in the general terms and conditions and data protection provisions. On the other hand, with the growing number of mandatory data in the ordering process, the customer's expenditure for an order in the shop increases – and with it also the probability of a cancellation of the purchase.



Is a changeover to 3DS 2.x mandatory? What deadlines must be observed?

The decisive question for merchants, on the other hand, is whether a procedure for processing credit card transactions that meet the requirements for strong customer authentication (SCA) can be provided in their own online shop by September 14, 2019.

As a merchant, you should take the following steps in order to comply with the SCA legal requirement:

Activation of 3DS 1.0, if this standard is not used by you yet:

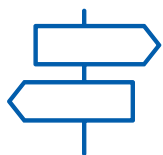
Please inform us by e-mail to support.emea@evopayments.com about the desired activation of 3DS 1.0 and indicate the EVO contractor ID of your agreement as well as the client number. The activation will then be performed at short notice and free of charge for you. All other conditions remain unchanged.

Investigate the possibility of activation of 3DS 2.x: We will be approaching you shortly with the option to upgrade to this version of 3DS.

Implementing 3DS 2.x requires a number of activities, including:

- 01 the update of your shop plugin, if one is in use
- 02 if you do not use a shop plug-in, the update of your interface to capture additional data elements that need to be transferred to the card issuer for risk analysis.

Merchants who have integrated the previous 3DS version 1.0 are still not faced with an acute need for action. Even after September 2019, 3DS 1.0 will continue to be used as the default fallback option for an indefinite period of time (see chart on page 3) if the new 3DS 2.x procedure is not yet supported by the trader or issuer.



How does a conversion with EVO Payments work?

The good news for our customers:

We can relieve you of a large part of the pending work. As with all our products, our 3DS 2.x solution is designed to keep integration costs as low as possible for our customers. However, it is just as important for us to provide a fully functional solution with the first release, which does not require any further adjustments on the part of the customer once the integration has been completed.

This is why we have been working intensively on a fast and practicable implementation since the announcement of the new 3DS standard.

In order to test our product successfully, we are dependent on the card-issuing banks, which must guarantee the proper receipt and processing of the transmitted data, but are currently still working on the technical implementation.

For this reason we ask for your understanding that the final test phase of our product is still ongoing. We will contact you as soon as it is completed. Should you decide to integrate the process in a timely manner, we will be happy to explain all the necessary steps to you in conversation with your individual contact person and our technical advisors and, together with you, make an estimate of the work involved for you as a merchant.





What are the tasks for merchants in the event of a changeover?

Merchants who wish to integrate the 3DS 2.x procedure into their shop have to

- 01 check with their Payment Service Provider whether it supports the 3DS 2.x protocol.
- 02 in coordination with their payment service provider, adjust the forms involved in the ordering and checkout process in order to provide the necessary customer data for transmission.
- 03 integrate the 3DS 2.x protocol into their mobile shopping apps (if available) in addition to the online shop.
- 04 make an adjustment to the general terms and conditions and data protection provisions and inform their customers of this.
- 05 register the supported 3-D Secure 2.x procedure with their acquirer.



What you need to consider now:

- > If you have integrated the 3DS 1.0 procedure into your shop, there is no acute need for action for you. The use of 3DS 1.0 as a fallback option is still possible after September 2019.
- > Together with your development team, first estimate the effort and consequences that a 3DS 2.x integration would entail within the next few months.
- > The connection to 3DS 2.x is smoothly supported by us via our Multi Pay interface.
- > If you have not yet integrated 3DS 1.0, please contact us. We will be happy to help you implement the integration of 3DS 2.x by September 2019.

Our recommendation



The most important rule when working with 3-D Secure 2.x: Don't let yourself be disturbed!

We would like to encourage all our customers (and merchants who are not yet) not to get carried away with rushing development projects due to the general uncertainty about 3-D Secure 2.x.

Even though media, industry associations and card companies are exerting considerable pressure on merchants, it will initially be up to issuers and card companies to provide the technical prerequisites for the new procedure in the near future.

It is good to know at this point that most card-issuing banks are not yet in a position to process all data points required by EMVCo in transaction analysis. This means that the 3-D Secure 2.x process is not yet fully operational.

