Do you have any questions about the Computop solutions? Our experts will be pleased to help you.

DE
COMPUTOP GMBH
BAMBERG (HQ)

Schwarzenbergstraße 4
96050 Bamberg
T: +49 (0)951 98009-22
M: sales@computop.com

UK
COMPUTOP LTD.
LONDON

T: +44 1932-895735
M: uk@computop.com

USA
COMPUTOP INC.
NEW YORK

T: +1-800-701-7806
M: usa@computop.com

CHINA
COMPUTOP CHINA
SHANGHAI

T: +86 (0)21 646850530
M: info@computop-china.cn

computop.com

3D Secure 2.0

Computop
the payment people

INFORMATION FOR
MERCHANTS ON THE NEW
3D SECURE PROTOCOL

YOUR GATEWAY
TO EVERYWHERE

Computop 3D Secure 2.0

INFORMATION FOR MERCHANTS ON THE NEW 3D SECURE PROTOCOL

What you need to know about the new 3D Secure process

The announcement of the new 3D Secure 2.0 process (3DS 2.0) has caused significant uncertainty among all stakeholders in e-commerce in recent months.

In particular, on the merchant side, discontent is growing over the information policy of the responsible initiators, especially as many payment processes in online trading have to be examined anyway in the wake of the new European Payment Services Directive (PSD II).

Since the announcement of the 3D Secure 2.0 rollout, Computop has been intensively grappling with the requirements of the new process and would like to answer key questions about 3D Secure 2.0 for its customers and all interested merchants on the following pages.

Overview of 3D Secure and 3D Secure 2.0

THE 3D SECURE PROCESS

The globally standardized 3D Secure Protocol (3DS) established in 2002 provides merchants and consumers with additional security for online credit card transactions. Online shoppers use the process to verify that they are legitimate cardholders to the issuing bank (issuer).

In contrast to a normal online credit card payment, which only requires the card information, 3D Secure requires the purchaser to enter an additional code to complete the ordering process successfully. This makes the misuse of credit cards much more difficult.

At the same time, liability for fraudulent transactions that are executed despite the use of the process is borne by the issuing banks. In order for the process to be used, 3D Secure has to be supported by both the purchaser's issuing bank and the relevant online shop.

HOW DOES 3D SECURE 2.0 DIFFER FROM 3D SECURE?

3D Secure 2.0 is basically an upgraded version of the regular 3D Secure protocol. The automated transmission of up to ten times the volume of transactional and buyer-related data allows issuers to replace the previously static code request with real-time risk analysis.

Each credit card purchase triggers the transmission of up to 100 data points to the issuer. The data is collected and forwarded by both the backend of the merchant's online shop and the Payment Service Provider (PSP) through which 3D Secure 2.0 is connected to the respective shop (see diagram). The data is transferred to the issuer in the secure environment of a 3D Secure server. The subsequent real-time risk assessment of each transaction is the sole responsibility of the issuer. Analytic software calculates a score for each transaction based on data signals that indicate possible fraud attempts.

If a transaction is classified as low-risk, it is approved without asking the purchaser to enter an additional code. On the other hand, if there is an increased likelihood of fraud (applicable to a maximum of 5 percent of all credit card transactions), the purchaser will be requested by text message or e-mail to reconfirm his or her identity.

The purchaser is not aware of the risk assessment process, which runs in the background. So, in the majority of cases a smooth payment process can be ensured without requesting additional security information from the purchaser.

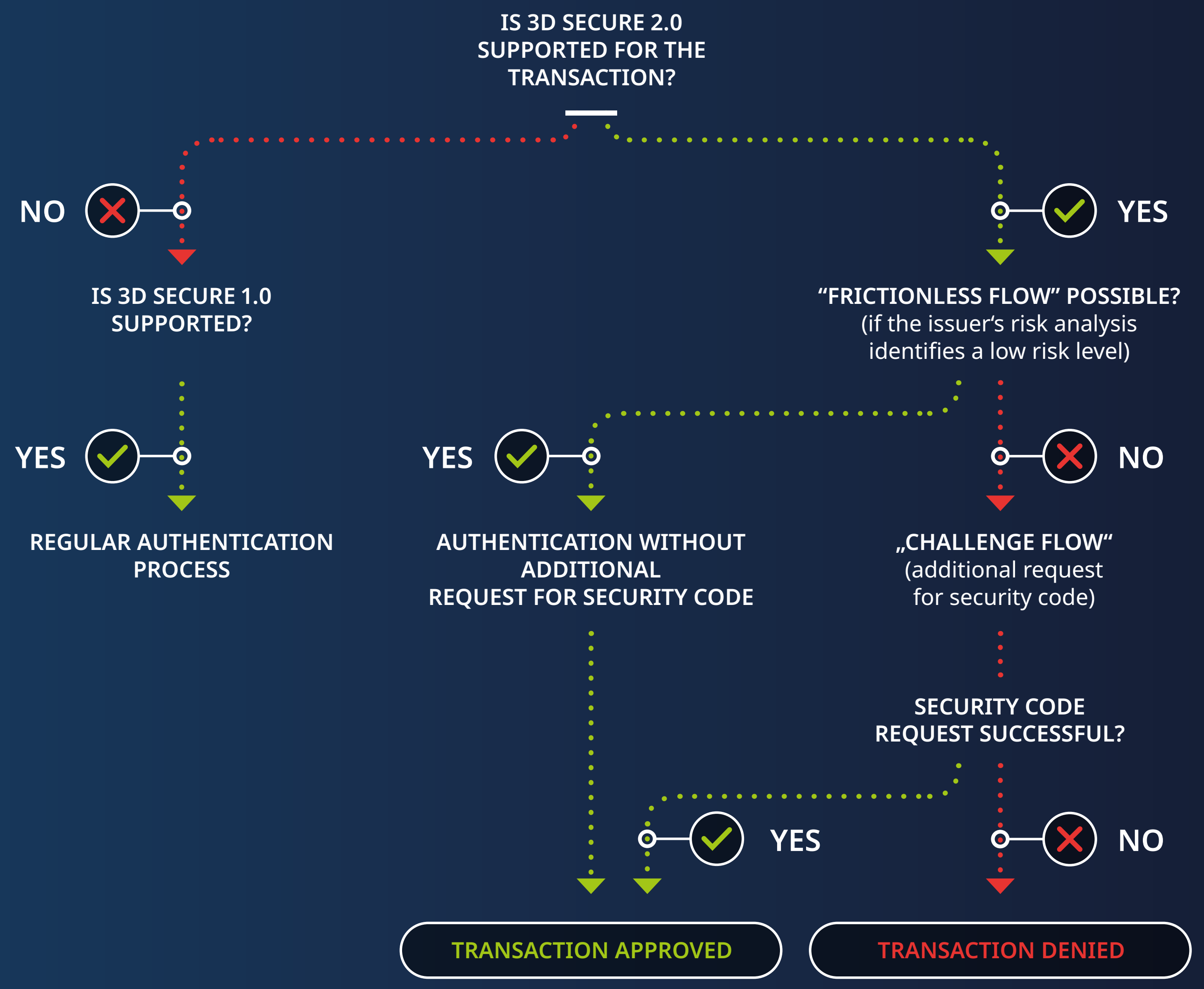
WHY IS 3D SECURE 2.0 BEING INTRODUCED?

The declared goal of 3D Secure 2.0 is to resolve the vulnerabilities of the former process that have been widely criticized by merchants and purchasers, and to meet the requirements of strong customer authentication (SCA), which will become legally binding for electronic payment processes as of September 14, 2019.

Since online shoppers will no longer be required to enter a 3D Secure code and the majority of credit card transactions will not require additional information from the online shopper, it is presumed that the new process will have a positive impact on conversion rates in the checkout process.
In addition, the individual, data-based risk assessment of each transaction promises even better protection against fraud.

Merchants who decide to install 3DS 2.0 will also benefit from significantly improved usability with mobile and in-app purchases. Input windows for 3DS queries can now be displayed in a format adapted to the respective device (responsive design). At the same time, the new process is no longer browser-based, but can now be integrated into merchant shopping apps using preconfigured software development kits (SDKs).

Schematic of the 3D Secure 2.0 process


IS 3D SECURE 2.0 SUPPORTED FOR THE TRANSACTION?
NO
YES
IS 3D SECURE 1.0 SUPPORTED?
"FRICTIONLESS FLOW" POSSIBLE? (if the issuer's risk analysis identifies a low risk level)
YES
YES
NO
REGULAR AUTHENTICATION PROCESS
AUTHENTICATION WITHOUT ADDITIONAL REQUEST FOR SECURITY CODE
„CHALLENGE FLOW" (additional request for security code)
SECURITY CODE REQUEST SUCCESSFUL?
YES
NO
TRANSACTION APPROVED
TRANSACTION DENIED

Data transmission in the 3D Secure 2.0 process

DO ALL POSSIBLE DATA POINTS HAVE TO BE TRANSMITTED?

No. EMVCo (credit card industry association), the organization responsible for the definition of the 3DS 2.0 standard, distinguishes between mandatory and optional data points and data. The latter includes all data collected from the merchant backend during the ordering process.

However, to make the best use of the new 3DS 2.0 process, the collection and transfer of all parameters is strongly recommended. The more data that is included in the issuer's transaction analysis, the more accurate the assessment of the fraud probability of a transaction will be.

WHICH DATA IS TRANSMITTED AND WHO IS RESPONSIBLE FOR COLLECTING IT?

The following data is collected by the merchant's Payment Service Provider (PSP), processed, and then transferred to the 3D Secure server:

1. CREDIT CARD DATA

that must be collected and processed in accordance with PCI DSS requirements.

2. TRANSACTION-RELATED DATA

This includes the identification numbers required to match the transaction and the merchant, as well as the amount and currency of the purchase.

3. BROWSER INFORMATION

that provides information about the device used and the location of the user. This includes the IP address, screen height and width, as well as the browser language used.

The following data is collected in the merchant's shop system and transferred to the 3D Secure server via the payment interface of the PSP. This information is not mandatory for the 3DS 2.0 process, but it is recommended to ensure accurate risk scoring:

4. BILLING AND SHIPPING ADDRESS

The complete billing and shipping address for the order.

5. CUSTOMER ACCOUNT

Data that was collected in association with an existing customer account. This includes information on the length of time that a customer's account has been open, the number of transactions carried out within certain time intervals, and the frequency of changes of passwords and shipping addresses.

6. DELIVERY DETAILS

Delivery details, such as the shipping method selected, availability of the goods, the delivery window, the e-mail address for the delivery of digital goods, or the date of first availability for products not yet released.

Facts about the implementation of 3D Secure 2.0

WHAT ARE THE CHALLENGES FOR MERCHANTS WITH IMPLEMENTING 3DS 2.0?

Moving to the new 3DS 2.0 process presents merchants with two main challenges to consider:

Although most of the technical adjustments have to be made by the issuers and payment service providers, merchants cannot avoid revising their order and checkout processes. Existing forms for creating customer accounts and guest checkouts must be expanded to include the required data fields and configured in coordination with the PSP to ensure smooth transfer of the data over the interface.

It is hard to predict how customers will react to the new process. On the one hand, they must be informed of the type and extent of the additional data transmitted in the terms and conditions and privacy policy. On the other hand, with the growing number of mandatory details in the ordering process, the customer's effort to place an order in the shop increases.

IS A CHANGEOVER TO 3DS 2.0 MANDATORY? WHICH DEADLINES SHOULD BE CONSIDERED?

As a merchant you will not be able to avoid an implementation of 3D Secure 2.0 in the near future. Although 3DS 2.0 is not a legal standard, it has been declared a new technical standard by the credit card industry: Online credit card payments within the European Economic Area are to be processed using the new protocol from September 14th, 2019 according to the guidelines of the EMVCo industry association. As a result, the predecessor protocol 3D Secure 1.0 will be decomissioned.

However, 3D Secure 1.0 will still be supported by the credit card companies for an indefinite period as a fallback solution. It can also be assumed that most issuer banks will also accept credit card payments that run via the 3D Secure 1.0 protocol on a transitional basis after September 14, 2019. Nevertheless, the update from version 1.0 to 2.0 should be based on the motto: The sooner the better.

From a legal point of view, online merchants are obliged to provide a procedure for processing credit card transactions in their own online shop by September 14, 2019 that meets the requirements for strong customer authentication (SCA). Both 3DS 2.0 and 3DS 1.0 (in its basic mode of operation) meet this requirement.

In this context, however, there is an urgent need for action for those merchants who have not yet integrated 3D Secure 1.0 into their shop. It is recommended that the current 3D Secure 2.0 procedure be integrated as quickly as possible in its minimum scope (only the mandatory data points are transmitted, see p. 6).

HOW IS THE CHANGEOVER DONE WITH COMPUTOP?

The good news for our customers: We can handle most of the required work for you. As with all our products, the appeal of our 3DS 2.0 solution is that we keep implementation as simple as possible for our customers.

But already with the first release, it is equally important for us to provide a fully functional solution that will not require any further modifications by the customer after it has been installed. That is why we have been working intensively on a fast and practicable implementation since the announcement of the new 3DS standard.

If you decide to install the process promptly, we will gladly explain all the necessary steps to you in a consultation with your personal contact and our technical advisors and will work with you to estimate the costs incurred by you as a merchant.

We will also promptly provide you with technical documentation on the installation of 3DS 2.0 in Computop Paygate. If you would like to stay up to date with the latest PSD II and 3DS 2.0 developments, we cordially invite you to visit our website www.computop.com.

What tasks do merchants have to deal with?

MERCHANTS WHO WANT TO IMPLEMENT THE 3DS 2.0 PROCESS IN THEIR ONLINE SHOP MUST:

1. Check with their payment service provider to determine whether they support the 3DS 2.0 protocol
2. Modify the forms involved in the order and checkout process in coordination with the payment service provider to provide the required customer data for transmission
3. Integrate the 3DS 2.0 protocol in their mobile shopping apps (if available) in addition to the online shop
4. Update their general terms and conditions and privacy policy and inform their customers accordingly
5. Register the supported 3D Secure 2.0 process with their acquirer

Find out more about PSD II and 3DS 2.0.

MEASURES RECOMMENDED BY COMPUTOP

The most important rule for handling 3D Secure 2.0: Don’t let it upset you!

We want to encourage all our customers (and merchants who are not yet customers) not to rush into any development projects as a result of the general uncertainty surrounding 3D Secure 2.0.

Although the media, industry associations, and card companies are putting a lot of pressure on merchants, within the next few months it will be up to issuers and card companies to provide the technical prerequisites for the new procedure.

What you need to consider:

1

If you have integrated 3DS 1.0 in your shop, you have a good starting position: In this case, incoming credit card payments in your online shop are automatically processed using the new 3D Secure 2.0 protocol. However, in order for your buyers to benefit from the new process (no additional authentication), additional data from your shop system must be transferred to our Paygate.

2

Together with your development department, you should first estimate the personnel and financial costs that would be involved in carrying out the relevant measures (collecting the data in the shop backend and transferring the data to our payment interface) within the next few months.

3

If you would like to fully integrate 3DS 2.0 by autumn 2019, Computop will be able to easily support the implementation via the Paygate interface.

4

If you are connected to our Paygate in any other way (e.g. via direct post or server-to-server), please contact us immediately. To ensure that all credit card payments in your shop can be processed without exception, your integration must be adjusted by September 14, 2019. Of course, our technical support will help you with the timely implementation.