Showing 3-D Secure Analysis

3-D Secure 2.x - background

For some time now, Computop merchants have been processing VISA and MasterCard payments using the latest protocols from the holding companies: the protocols have now been introduced and a wide variety of expert groups are discussing a wide variety of analyzes. In order to put you in a position to interpret the development of your card payments, we have put together the most important key figures for you on our dashboard.

Here is a brief background on 3-D Secure:

How does 3-D Secure 2 differ from the previous procedure?

Essentially, 3-D Secure 2 represents a further development of the previous 3-D Secure protocol. From now on, up to 100 data points are transmitted to the issuer with every order made by credit card; Based on these data points, the issuer carries out a real-time risk assessment. If a transaction is classified as low-risk, it can be authorized directly and without further interaction on the part of the buyer. However, if there is suspicion of fraud, the buyer will be asked to confirm his identity again with an additional security query (e.g. using a push TAN). The risk assessment is not perceptible to the buyer in the background. The necessary data is recorded and forwarded both via the retailer's shop backend and via the Payment Service Provider (PSP), via which 3-D Secure 2 is connected to the respective shop.

When and why will 3-D Secure 2 be introduced?

The declared aim of the introduction of 3-D Secure 2 is on the one hand to meet the requirements for Strong Customer Authentication (SCA) and to establish it as the standard for electronic payment methods from December 31, 2020.
On the other hand, the introduction of the abandonment rate is also intended to decrease: thanks to the individual, data-based risk assessment, transactions can be approved in approx. 95 percent of all cases directly and without further buyer interaction - a majority of purchases will therefore take place in the future without entering a 3-D Secure code.

Computop KPI for 3-D Secure

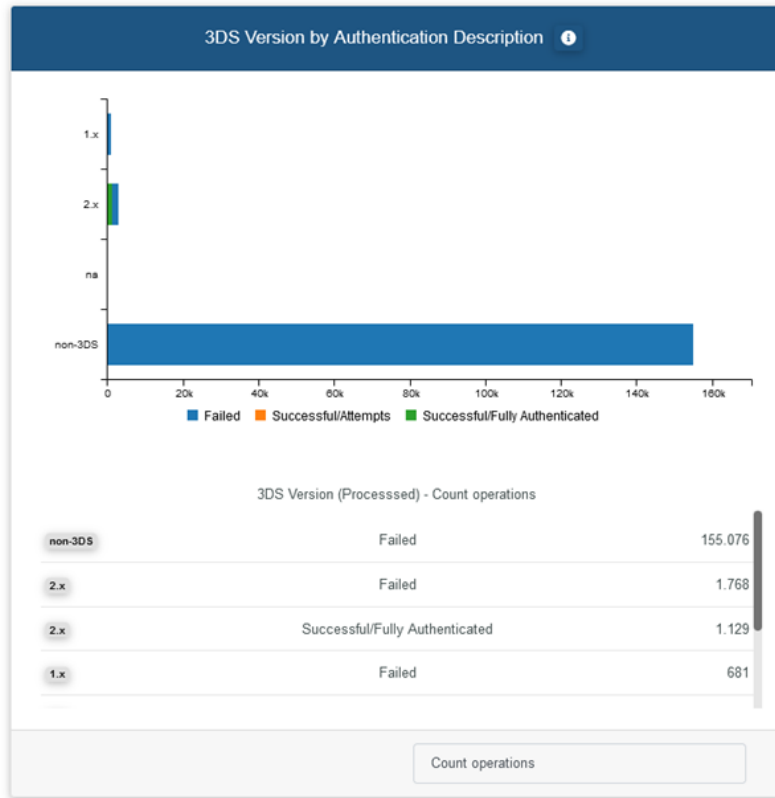We have taken care to make the optimization approaches of the new protocol measurable.

	Value Proposition
For consumers	• Simple authentication
For merchants	• Less false declines • Less abandoned purchases in the checkout
For banks/issuers	• Improved fraud prevention • More transactions • More safety

How are my payments made up?

The first two dashboards provide an overview of the proportions of the various protocols and their performance.

Proportion of payments according to the protocol

3DS Version by Authentication Description ⓘ

3DS Version (Processsed) - Count operations

non-3DS		155.076
2.x		2.897
1.x		939
na		14

3DS Version (Processed) - Count operations

non-3DS	Failed	155.076
2.x	Failed	1.768
2.x	Successful/Fully Authenticated	1.129
1.x	Failed	681

Count operations

Version	Description
non-3DS	Payments without 3DS
1.x	Payments using the "old" 3DS protocoll
2.x	Payments using the new 3DS protocoll

ⓘ You can hide different versions in the diagram by clicking on the icons in the table area, so that you can only see the comparison between 3DS 1.x and 3DS 2.x, for example:

Performance der Versionen
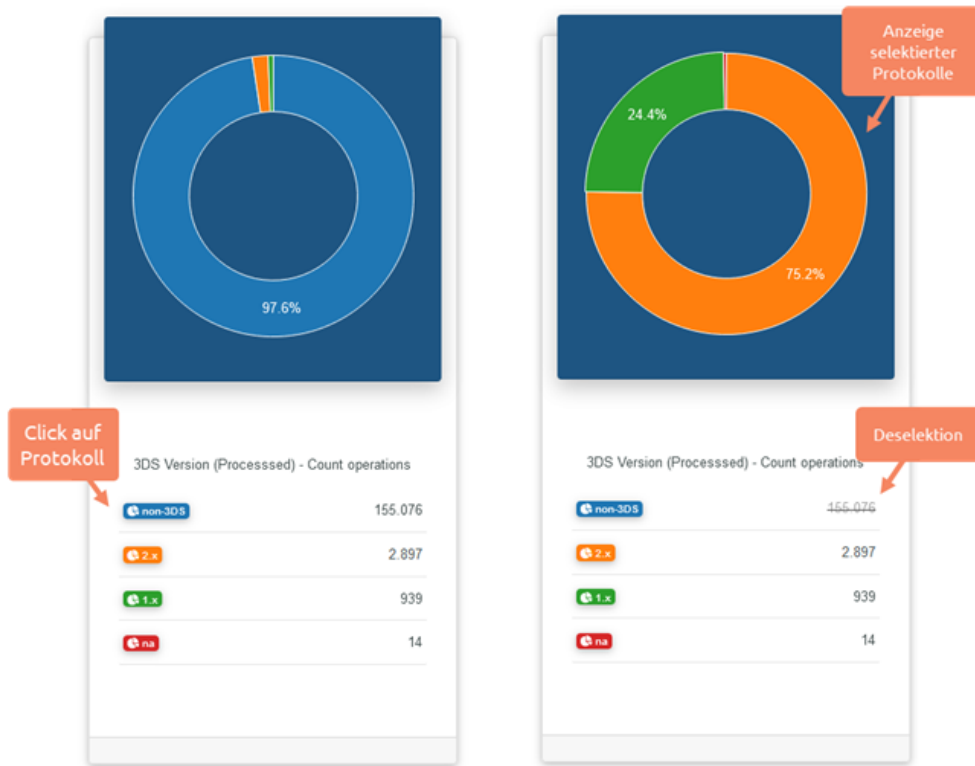
The diagram shows the volume of transactions by protocol and lists the results of the authentication as a bar chart. With a mouseover you can see a small table view of the breakdown.
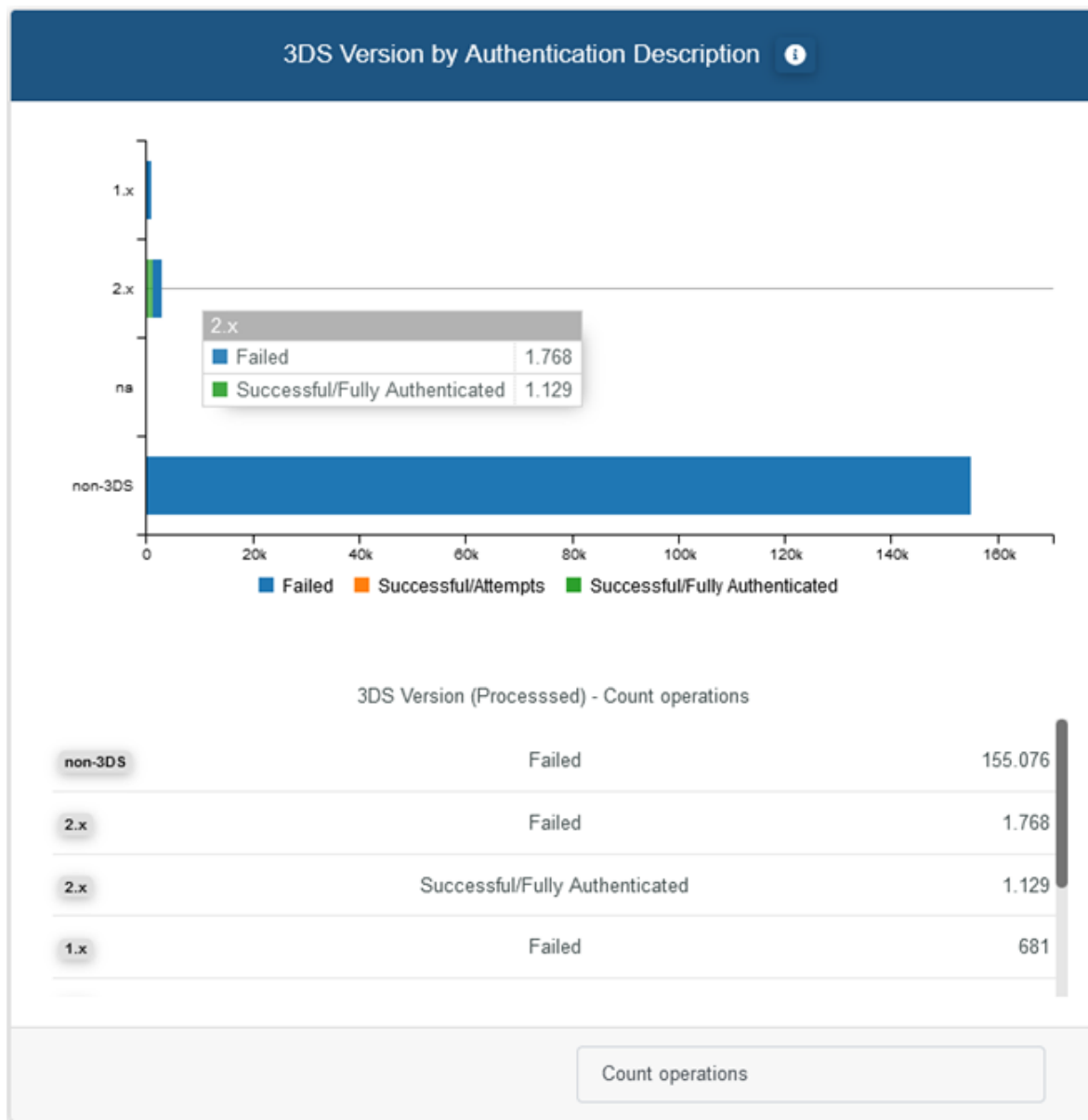
The lower area shows you in a table according to the protocol version:

- Authentication failures
- Successful authentications
- Successful Attempts: 3DS was started, but the cardholder is not registered for 3DS

In addition to the total number, you can also see the number of transactions and the response codes depending on the protocol version.

Easy authentication: Frictionless

The greatest added value for customers and dealers, namely simple processing, comes from the introduction of so-called "frictionless" payments. The card issuer saves the end customer from having to authenticate. The "Authentication Type" diagram shows you how this feature performs.

On the right side you can see the results of the cardholder authentication at a glance.

Authentication Type

50.9%	
42.0%	
7.1%	

🔵 Not Mapped	1.475
🟠 Dynamic	1.217
🟢 Frictionless	205

Authenticaton Results

63.7%	
16.3%	
9.9%	

🔵 Authentication completed	1.135
🟢 Connection timed out	291
🟠 Authentication failed	176
🟣 Unknown error	58
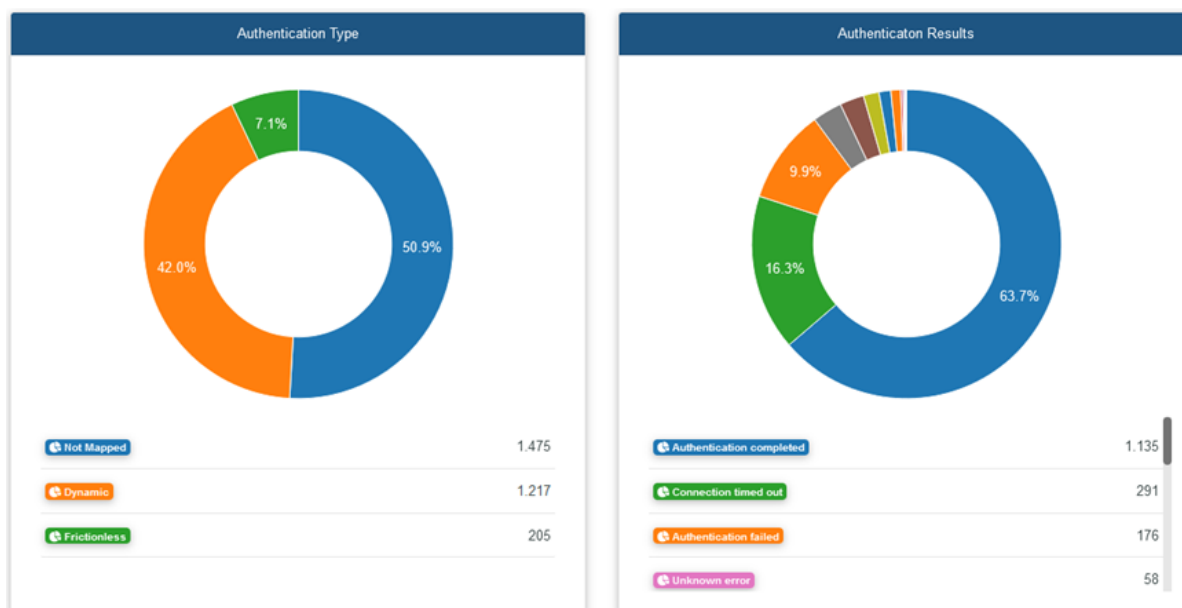
Please note that the messages "Frictionless" and "Dynamic" are new components of 3DS 2: If you would like to shed light on this aspect, please select the protocol version 3D 2.x in the filters.

Description of the values:

Authentication Type Code	Authentication Type	Description
00	Frictionless	Issuer has not prompted card holder to go through authentication process
01	Static	Issuer challenges authentication with static password
02	Dynamic	Issuer challenges authentication with a dynamic password, usually SMS or TAN or OTP
03	Out of Band	Authentication is performed in another device, e.g. the user is shopping in desktop/laptop and the authentication is performed via the banking app on the mobile phone
04	Decoupled	Usually for MOTO transactions: the authentication is performed separately from the request
	Not mapped	Authentication Type could not be retrieved.

Fallback

Year	Merchant	Brand	3DS Version (Started)	3DS Version (Processed)	Authentication Result	Fallback reason	Currency	Count operations	Amount authorized	Amour captur
2020	felixtest	DINERS	2.x	2.x	Successful/Fully Authenticated	-	EUR	2	0,22	
2020	felixtest	DISCOVER	2.x	2.x	Successful/Fully Authenticated	-	EUR	1	0,11	
2020	felixtest	Maestro	2.x	1.x	Failed	PERMANENT_SYSTEM_FAILURE	EUR	1	0	
2020	felixtest	Maestro	2.x	2.x	Failed	-	EUR	3	0	
2020	felixtest	Maestro	2.x	2.x	Successful/Fully Authenticated	-	EUR	4	0,44	
2020	felixtest	MasterCard	2.x	1.x	Failed	INVALID_CHARACTERS	EUR	1	0	
2020	felixtest	MasterCard	2.x	1.x	Failed	REQUIRED_ELEMENT_MISSING	EUR	2	0	
2020	felixtest	MasterCard	2.x	1.x	Successful/Attempts	INVALID_CHARACTERS	EUR	8	80	
2020	felixtest	MasterCard	2.x	1.x	Successful/Attempts	ISSUER_NOT_READY	EUR	1	0	
2020	felixtest	MasterCard	2.x	1.x	Successful/Attempts	REQUIRED_ELEMENT_MISSING	EUR	11	110	

Showing 1 to 10 of 84 entries

Previous 1 2 3 4 5 ... 9 Next

Year

Fallback means that 3-D Secure authentication via the new EMV 3-D Secure 2.x was not possible (e.g. issuer is not ready, cardholder has not yet registered). To save your checkout, our platform will switch to the older 3-D Secure 1.x. The table shows the sums of the payments that were processed with the incoming 3-D Secure version ("Started") and the 3-D Secure version used for authentication ("Processed").

Since this function is only available in the new protocol, please select "3DS Verion Started 2.x" as the filter

Country level analysis

We have prepared the following evaluation so that you can see details including the affected countries and payments. In addition to the map countries, you can see the development of the protocol usage in a timeline.

Trend of 3DS Version by credit cards country of origin ⓘ

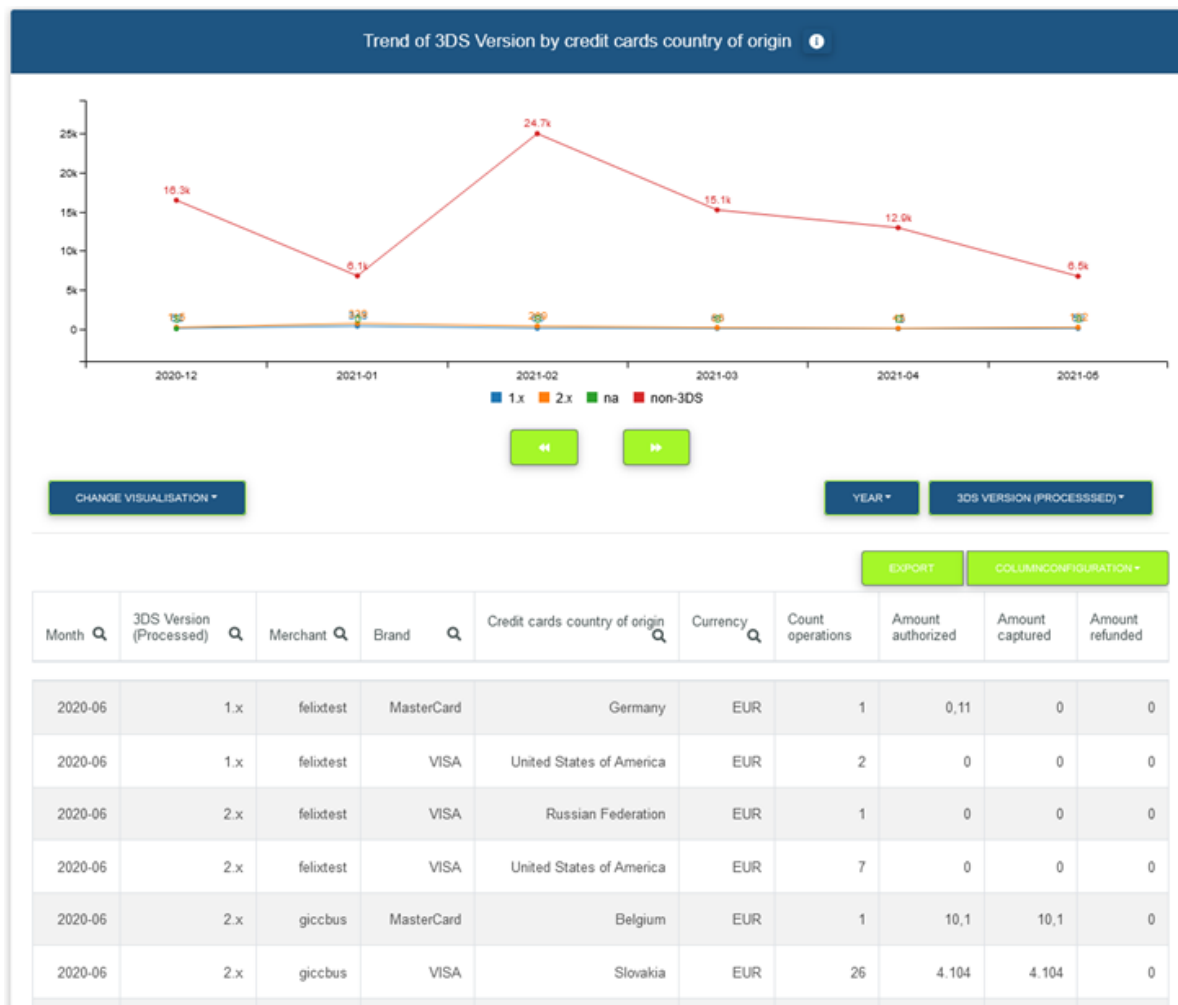| Month Q	3DS Version (Processed) Q	Merchant Q	Brand Q	Credit cards country of origin Q	Currency Q	Count operations	Amount authorized	Amount captured	Amount refunded
2020-06	1.x	felixtest	MasterCard	Germany	EUR	1	0,11	0	0
2020-06	1.x	felixtest	VISA	United States of America	EUR	2	0	0	0
2020-06	2.x	felixtest	VISA	Russian Federation	EUR	1	0	0	0
2020-06	2.x	felixtest	VISA	United States of America	EUR	7	0	0	0
2020-06	2.x	giccbus	MasterCard	Belgium	EUR	1	10,1	10,1	0
2020-06	2.x	giccbus	VISA	Slovakia	EUR	26	4.104	4.104	0

If you are interested in the key figures for a country, simply click on it in the list and you will see all the key figures for that country.

Month Q	3DS Version (Processed) Q	Merchant Q	Brand Q	Credit cards country of origin Q	Currency Q	Count operations	Amount authorized	Amount captured	Amount refunded
2020-07	non-3DS	hakan_test	AMEX	Australia / Brazil / Austria / Belgium / Benin / Brazil / Bulgaria / Cambodia	EUR	2	0	0	0
2020-07	non-3DS	marcotest	MasterCard		EUR	4	0,22	0	0
2020-07	non-3DS	nilstest101	MasterCard		EUR	10	0	0	0
2020-08	1.x	marcotest	MasterCard		EUR	1	0,11	0	0
2020-08	non-3DS	marcotest	MasterCard		EUR	11	1,21	0	0

SCA Excemptions

We will show you the development of this feature in the processing of so called "Soft Declines". These are credit card payments that have been automatically repeated after they have been rejected by the issuer with "Soft Decline". This means: the issuer rejects an authorization without customer authentication and insists on a 3-D Secure transaction. In addition to the number, you can also see successful authorizations via the different views.

Details on handling for a payment transaction that has been rejected with "Soft Decline" can be found on this page in the section: Soft decline handling.

Soft Decline Trend ⓘ
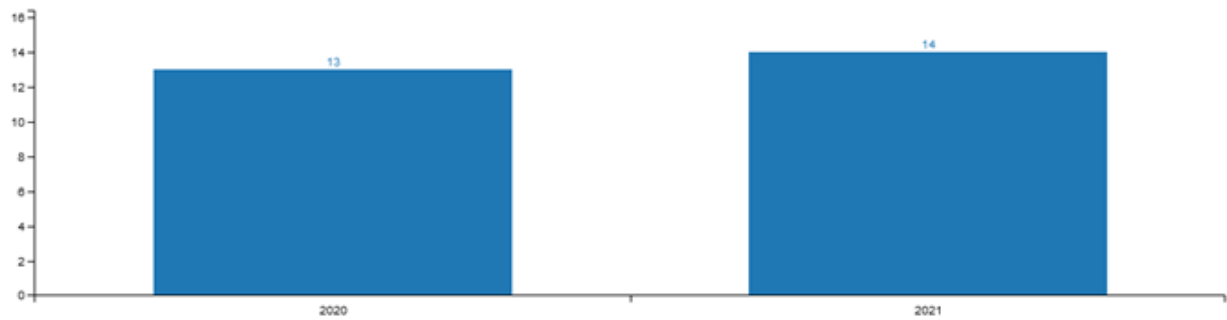
CHANGE VISUALISATION ▾

SUCCESSFULL AUTHORISED ▾   YEAR ▾

successfull authorised
authentication successfull, but authorisation faile
authentication failed

Year 🔍	Soft Decline 🔍	Merchant 🔍	Brand 🔍	successfull authorised	authentication successfull, but authorisation failed	authentication failed
2020	True	felixtest	VISA	13	0	1
2021	True	felixtest	MasterCard	2	0	0
2021	True	felixtest	VISA	12	3	6

Showing 1 to 3 of 3 entries

Previous   1   Next

Year