axerve

Your Payment Partner to Grow

Strong Customer Authentication (SCA) in 2021

Analysis of the first European and Italian data

Axerve • Whitepaper

Contents

3DS2 adoption statistics in Europe

According to **a study by Mastercard on cards by country of issue and covering the period 1 to 24 January 2021, most European countries** are experiencing a growing **transaction authentication rate, often greater than 50%**. The states that registered the lowest rates are: Portugal (53.5%), Italy (51.1%) and Belgium (50.7%).

The **UK**, included in the study despite its withdrawal from the European Union, is the **best performing nation** overall, as shown in Table 1. In fact, 90.4% of the transactions in the reporting period were authenticated, of which 62.2% were frictionless authentication, i.e. without 2-factor authentication by the buyer.

	% Authenticated	% Auth Frictionless by issuer or SCA Delegation
Grand Total	71,3%	25,8%
UNITED KINGDOM	90,4%	62,2%
CZECH REPUBLIC	87,5%	29,9%
IRELAND	86,5%	63,7%
SLOVAKIA	83,3%	4,7%
GREECE	80,1%	37,0%
CROATIA	73,9%	2,0%
SPAIN	73,2%	33,9%
NETHERLANDS	72,2%	26,4%
SWEDEN	71,2%	19,8%
DENMARK	71,7%	0,0%
BULGARIA	70,2%	35,7%
POLAND	67,1%	13,2%
FINLAND	67,1%	3,8%
GERMANY	66,6%	36,3%
AUSTRIA	66,3%	27,4%
ROMANIA	65,0%	4,4%
HUNGARY	64,3%	7,2%
FRANCE	60,8%	6,1%
PORTUGAL	53,5%	21,6%
ITALY	51,1%	7,3%
BELGIUM	50,7%	2,3%

Table 1
Source: Mastercard Analysis

3DS2 in Italy: one of the lowest performance in Europe

As shown in Table 1, **Italy was one of the least effective than the rest of Europe**, which had an average authentication rate of 71.3%. Even the application of frictionless authentication, at 7.3% of the total, was further behind the European average of 25.8%. These figures not only give the picture of the Italian market in terms of application of SCA, but also explain why **Italy currently loses about 43.9% of its 3DS transactions**, as shown in Table 2.

This data, in March, exceeded the European average of 25.3% by far. This means that, for a little less than half of the payments, the request for 2-factor authentication was not completed, **leading to a drop in sales**.

When the **Access Control Server** (ACS), i.e. the entity that verifies whether the card adheres to the protocol and manages the authentication of the card at the payment stage, is **unable to provide an outcome to a payment made with a card with active 3DS2 protocols** due to technical problems, then it is referred to an **Attempt**. In this regard, as shown in Table 2, **Italy is above the European average**, 5% versus 3.4%, making it **one of the least performing countries**. In fact, while it is true that the transaction goes directly to authorization, it is worth considering that the issuer often responds with a "KO" so as not to incur fraud costs if the payment is not genuine.

While this may appear to be a ploy to avoid SCA, in reality, **a high number of *Attempts*** again results in a **drop in conversion of the cart**.

	% Not Authenticated	% Attempt
Grand Total	25,3%	3,4%
UNITED KINGDOM	8,6%	1,0%
IRELAND	10,5%	3,0%
CZECH REPUBLIC	12,0%	0,5%
SLOVAKIA	15,4%	1,3%
GREECE	18,2%	1,7%
HUNGARY	21,9%	13,8%
SPAIN	24,9%	1,9%
GERMANY	25,3%	8,0%
CROATIA	25,6%	0,4%
AUSTRIA	25,8%	7,9%
NETHERLANDS	26,6%	1,2%
BULGARIA	26,9%	2,9%
DENMARK	26,9%	1,4%
POLAND	27,7%	5,2%
SWEDEN	28,1%	0,7%
FINLAND	30,7%	2,2%
ROMANIA	33,8%	1,2%
FRANCE	37,4%	1,8%
PORTUGAL	42,3%	4,2%
ITALY	43,9%	5,0%
BELGIUM	48,3%	1,0%

Table 2
Source: Mastercard Analysis

Overview of authentications in Italy: comparison of January data with Q1 2021

As we have also seen above, the rate of transactions for which authentication failed was around 43.9% in the first days of March, which is still very high, especially when compared to the system average. The graph in Table 3 shows the daily results of the authentications registered in the first 24 days of the year from which some conclusions can be drawn.

First of all, it is clear that the number of **authentications not completed due to ACS technical problems has been gradually decreasing** to approximately 7%, at the end of the period considered in the graph. It should be remembered, however, that although these transactions are sent directly to authorization and therefore pass the 'barrier' of 2-factor authentication, a **large proportion of these transactions are rejected by the issuer**, and in fact the data in March has fallen up to 5%.

What should also be taken into account is that the **growth trend in Authenticated**, after initially weak growth **around 46%** towards the end of the analysis period (42.3%, monthly average), has progressively improved settling down at 51.1%. **Not authenticated transactions followed the same trend**, sharing the space freed up by Attempts with authenticated transactions, reaching values of around 46% at the end of January (46.2%, monthly average) arriving at almost 44%.

Although they occur infrequently, ***Challenged, Unavailable*** and ***Undefined*** transactions **point to technical errors and system anomalies** that fortunately account for only one or two percent

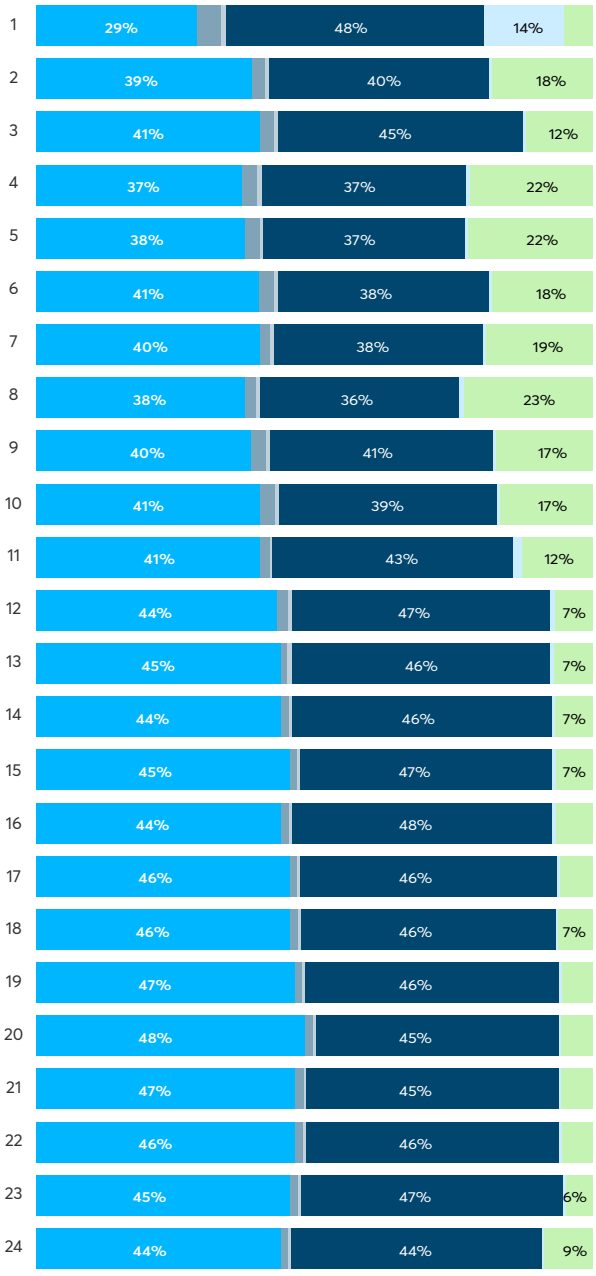


Table 3
Source: Mastercard Analysis

of the total and, as with Challenged transactions, the whole ecosystem is working to eliminate them completely.

Another particularly interesting finding relates to the substantial difference in the outcomes of 2-factor authentication between in-app and browser-based transactions, where Mastercard's data shows an authentication **success rate of 63.1% for browser-based payments** and only **9.6% for app-based payments**.

Therefore, there is a clear need to identify solutions that will improve redemption rates, not least because, given the steady increase of in-app and mobile payments, these numbers are bound to rise. The reasons for this are mainly found in the development of non-optimised provider SDKs and issuer apps that do not always perform perfectly, so these are where efforts should be concentrated.

The reasons for failed authentications in Italy

Why do authentications fail? According to Mastercard's analysis of Transaction Reason Codes, there are three macro-categories:

ACS timeout

In January, more than 60% of failed authentications could be traced back to the communication process with the ACS, data fallen down to 53,9% at the beginning of March. Possible difficulties in handling response messages from or to the ACS may be causing timeouts.

Card without 3DS2 protocols or Transaction not allowed

At the beginning of the year, 25.6% of authentications failed **because the card might not have active 3DS2 protocols** or because the **authentication request has not been allowed** due to the cardholder not providing all the data required for the issuer to complete the authentication (e.g. no phone number to send the OTP to in order to finalise the transaction), while at the beginning of March this data has grown to 28.4%.

Abandonment of authentication

In this case, **the buyer has not completed authentication because they have abandoned** the transaction. This reason, that concerned 10.5% of the total in January and 14.3% in March, is mainly due to the user experience offered by everyone involved in authentication and especially by the issuer that manages the process, including in terms of front-end.

SCA adoption plans in Europe

Although PSD2 is an EU-wide regulation, the European Central Bank has allowed national banks in individual countries to intervene in their plans to adopt Strong Customer Authentication.

As shown in Table 4, **each country has adopted a different schedule for applying SCA** to transactions. What all countries have in common, however, is the criterion based on amounts. In this paper, we focus on Italy which, today, has a plan to adopt the SCA for transactions:

- greater than € 1,000 starting 1 January 2021
- greater than € 500 starting 1 February 2021
- over € 100 starting 1 March 2021
- any amount starting 1 April 2021

At the moment, the time frame described above is still being defined and could change in Italy and abroad depending on how the entire online payment ecosystem performs, in the interest of all stakeholders involved.

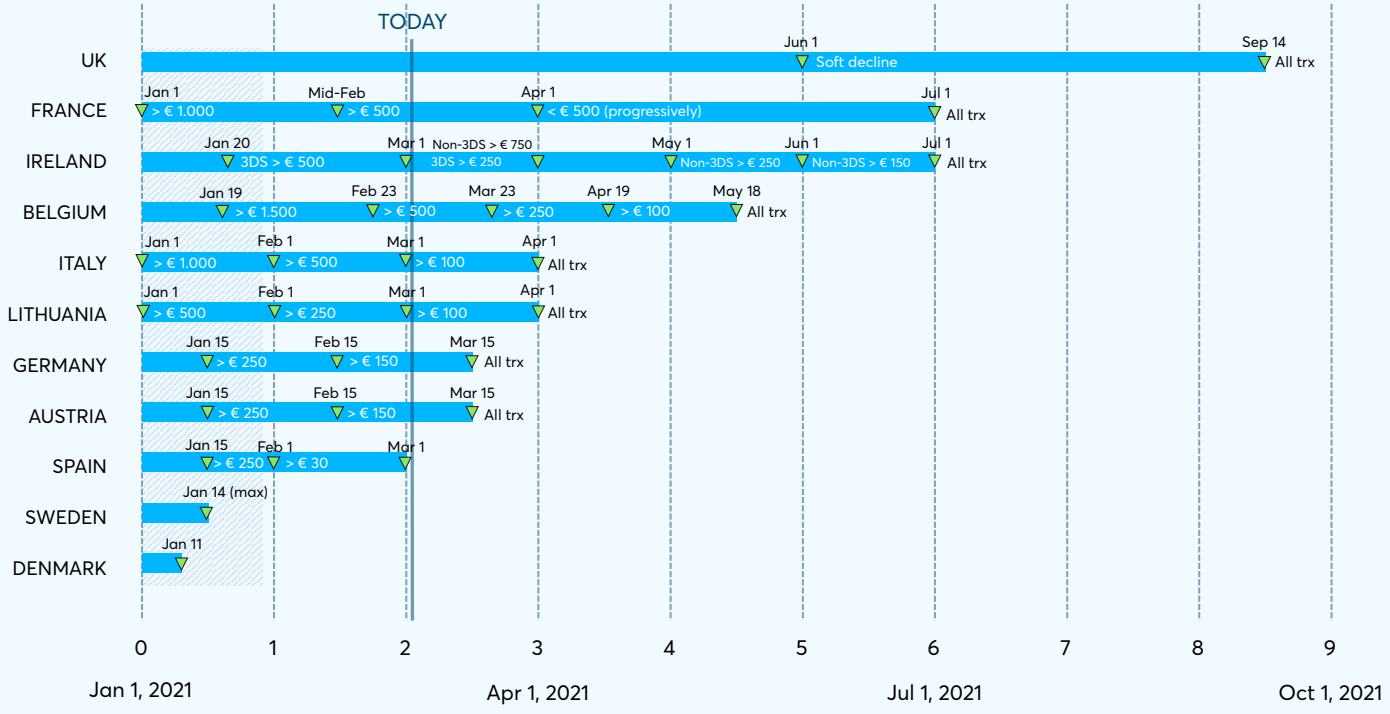


Table 4
Source: Mastercard Analysis

EEA-UK transactions and Brexit

The implementation of Brexit, which was ratified last 24 December with the signing by the European Union and the United Kingdom of a trade and cooperation agreement that entered into force provisionally on 1 January 2021, at the end of the transition period, has also created a new scenario in the area of payments. As of **this year, Great Britain and Northern Ireland are no longer subject to ECB directives** but to those of the FCA (Financial Conduct Authority), which also regulates payment services and electronic money in the UK.

As can be seen in Table 5, the UK has decided to adopt Strong Customer Authentication starting 14 September 2021, but with the possibility of applying soft declines, i.e. refusals on authorization due to lack of authentication, starting 1 June 2021.
So, before and after 14 September 2021, what actually changes for the UK and Italy? Before 14 September, Italian issuers can apply SCA to transactions from UK acquirers depending on the latter's authentication features (with or without 3DS2), while UK issuers can authorize transactions of Italian acquirers, according to the adoption schedule shown in the chart.

From the kick-off date of 14 September, Italian issuers will have to apply SCA to payments from UK acquirers, net of possible exemptions and exceptions. It is worth remembering that PSD2 requires 2-factor authentication for one-leg transactions, i.e. payments where only the issuer or acquirer is in the European Union.

UK payment card companies, in turn, will also have to apply SCA to transactions from acquirers in the European Economic Area (EEA), again taking into account possible exemptions and exceptions.

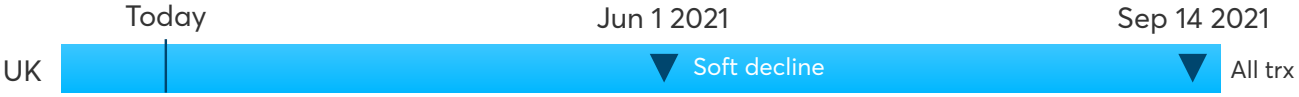


Table 5
Source: Mastercard Analysis

Strong Customer Authentication: Axerve observation data in January 2021

Axerve's calculations on a total of 180 BINs with at least 100 transactions in the month allow a comparison of pre- and post-PSD2 conversion trends.

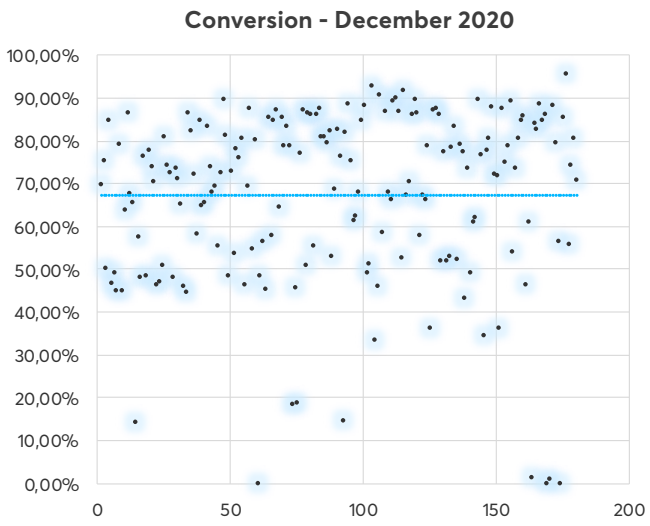
As can be seen from the graphs in Table 6, **the average conversion decreased slightly** from 67.53% to 67.15%, but what is more evident is the deviation from the reference value. As can be seen from a comparison of the two graphs, the **standard** deviation in **December**, i.e. the deviation from the reference average, was **lower** (20.34%) **than in January**, at around 23.38%.

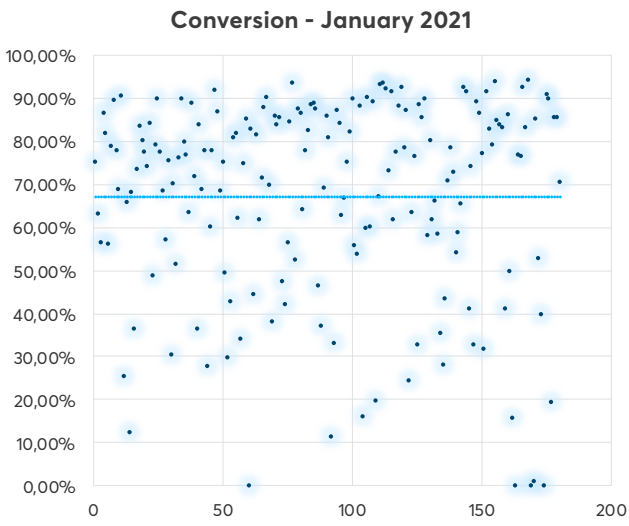
In practice, **a greater dispersion of the conversion rate** can be seen, an indication that we are still in a very heterogeneous phase, in which the scenario shows a high dispersion presumably due to an initial period of adjustment in many respects, which can range from the user experience of authentication processes to the physical increase in buyer abandonment.

Let's **focus on handling Attempted transactions**, i.e. transactions for which authentication could not be performed due to impossibility on the part of the ACS but for which a proof of attempted authentication was nevertheless returned.

For these transactions, the specifications require that they be handled as if they had been authenticated and then generally authorized. It was noted that, on this front, **issuer behaviour is irregular**, with a consequent drop in conversion, unpredictable for the merchant and due to the functional logic of the individual issuer.

Table 6
Source: Axerve Analysis





How to improve conversion rates on authentications with Axerve

We have seen how, in the face of the difficulties relating to the conversion of carts described in this document, which were mainly due to the activities of all the participants involved in PSD2, **many of the national banking authorities**, in agreement with the ECB, **granted a "ramp-up" period**. **Axerve** has seized the opportunities of this transitional period **by developing a solution that aims to improve conversion rates** while remaining within the perimeters identified by European regulations.

Axerve's technical solution

During this 'transition' phase, it is possible for merchants to process certain transactions even without 3DS2 authentication, usually on the basis of amount.
The 3DS2 waiver function developed by Axerve offers merchants **the possibility to process waiver transactions directly in authorization**, maintaining the merchant's liability in case of fraud.

How the waiver solution works

Once enabled at the individual shop login level, **processed transactions are checked** and, if passed, **sent directly to the authorizer**, avoiding 2-factor authentication.

Each transaction gets verified. The function is associated with a table containing the ranges of waived BINs and the respective threshold amount. When the criteria are verified, the transaction is processed directly in authorization, thus avoiding 2-factor authentication.

The function is also able to **repeat the authorization request for a soft decline**, effectively automating a part of the process that would otherwise require manual intervention.

Activation of the solution does not require any changes to the Axerve Ecommerce Solutions integration, and you can contact your sales representative for detailed specifications and activation.

axerve

Your Payment Partner to Grow

www.axerve.com

Axerve S.p.A. - gruppo Sella – P.zza Gaudenzio Sella, 1, 13900 Biella (BI) – segreteria@pec.axerve.com – www.axerve.com – Capitale sociale:
€ 1.500.000,00 i.v. – P. IVA 02675650028 / CF 02686620028 – REA BI-205559 – Società appartenente al Gruppo IVA Maurizio Sella S.a.a. e soggetta all'attività di direzione e coordinamento di Banca Sella Holding S.p.A. – Iscrizione Tribunale di Biella n. 71524