axerve

Your Payment Partner to Grow

Tokenization: the strategic tool for PSD2 compliant Ecommerce

Axerve • Whitepaper

axerve

Contents

Ecommerce in Italy in 2020 3

Online purchasing: data security and management 4

Tokenization: what it is and how it impacts on business 5

Greater security for merchants and consumers 5

Token: the key to a personalised customer journey 5

Use cases in a PSD2-compliant context 6

Types of tokens: Service Payments Provider and Circuit 8

Future impacts of tokenization and SCA delegation 10

Sources 11

Ecommerce in Italy in 2020

The number of online **consumers in Italy has grown by 2 million** since the beginning of the year – in the same period of 2019 the increase was 700,000 – reaching a **total of 29 million**[1]; despite this, the 48.5 billion in turnover estimated in Italy in 2019 by the Ecommerce sector is only a part of the potential that could be tapped by Italian companies. In fact, at the end of 2019 Italy saw the number of consumers purchasing online increased to 48%, but it **is still one of the countries with the lowest Ecommerce penetration** compared to countries such as Switzerland or the United Kingdom which vastly exceed 80%[2]. However, the growth rates are promising for the entire sector, which have seen Italy **grow by 17% compared to 2018**, a two-digit increase in line with the data of the last five years[3].

The data analysis of Axerve, which currently manages online payments of about 50% of Italian Ecommerce sites, offers a snapshot of **alternative payment trends** since the beginning of the year. A comparison of the half-yearly 2020 figure with last year shows progressive growth in the use of alternative instruments besides credit and debit cards. In particular, in the last quarter (June still to be verified), the growth was exponential and recorded an average of +500% compared to March (April and May recorded +150% compared to +29% in March, the figure will change with the addition of June). **Consumers** are therefore seeking payment experiences that are increasingly in line with their needs, regardless of the channel chosen and perhaps a bit forced by the historic moment we are all experiencing in 2020, and to do so **they rely on a wider offer of payment instruments, compared to even very recent times**. The goal is to obtain a shopping experience as pleasant as possible.

On this very topic, **Axerve CEO Alessandro Bocca** recently stated the following during the presentation of a digital payment solution for in-store purchases:

"Merchants, especially those from small and medium-sized stores, need to regain competitiveness and regain ground vis-à-vis Ecommerce today, which has inevitably increased exponentially in recent months. Retailers must win back their customers and can only do so by meeting their needs and increasing the number of services or products offered. Payment and its management are no exception and play a key role in the relationship with customers. With this evolution of 'Axerve Pay by Link', we want to give all merchants the opportunity to keep up with the new sales methods in which the digital channel also fits into the physical one, offering the end customer a faster, smoother and safer shopping experience in the store, and at the same time offering the merchant the opportunity to approach the increasingly established purchasing habits deriving from the growth of Ecommerce without having to support the efforts to have a site of their own."

Alessandro Bocca
Axerve CEO

All that remains is to **identify the touchpoints on which to invest** in order to promptly respond to market demands, and tokenization has all the characteristics to be one such touchpoint.

1 - Data presented by Roberto Liscia, President of Netcomm at Netcomm Forum Live 2020
2 - European Commerce Report 2019 | Ecommerce Europe
3 - E-commerce in Italia 2020 | Casaleggio Associati

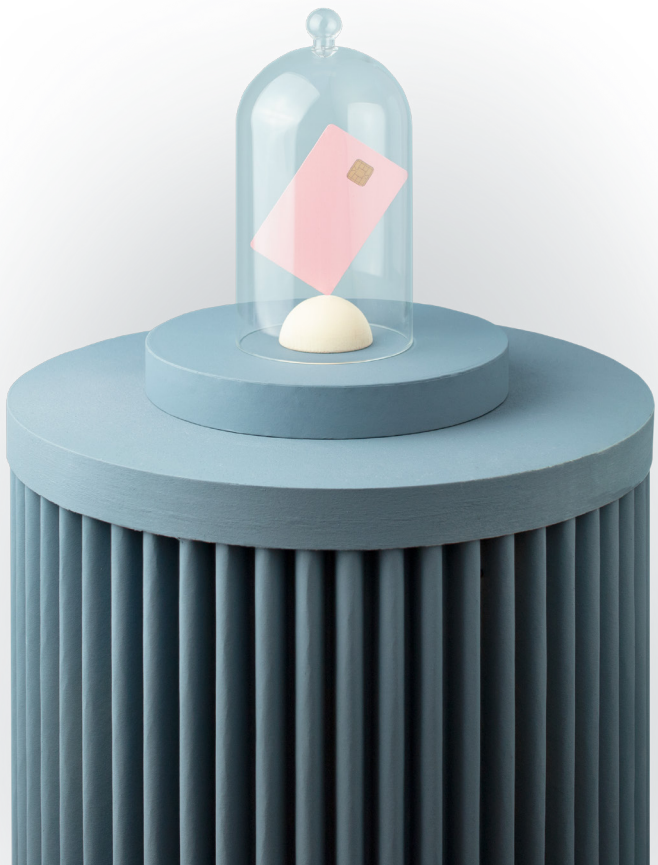
Online purchasing: data security and management

Increasing the security of Ecommerce purchases is one of the elements that could **consolidate the growth of Ecommerce** and even allow reaching those who continue to prefer offline shopping today.

In fact, a great deal can still be done from this point of view. Some data published by Proofpoint[4] show that **85% of the main European Ecommerce sites, and only 70% of Italian ones, did not integrate security systems to combat email scams** and 80% of the cyber attacks against apps involved the use of stolen credentials.

Some data recently published by Riskified, the international leader in the field of fraud prevention, highlight this very issue. It interviewed 4,000 consumers and 425 online merchants[5], revealing that **27% of Ecommerce sites have not implemented solutions to prevent account takeover actions**, and of their customers who are victims of this fraudulent practice, only 7.5% have become aware of it through the online merchant.

The above data offer an idea of how many aspects of fraud prevention can still be improved. The tokenization of payment instruments through certified platforms can greatly contribute to the security of online purchases, customer experience and the reputation of the entire Ecommerce sector.



4 - Proofpoint Q4 2019
5 - Survey Says?! ATOs Are a Major Threat and Many Merchants Are Unprepared | Riskified

Tokenization: what it is and how it impacts on business

The concept of **tokenization**, in the context of payments, identifies a **service for which the buyer's card data is replaced by strings**, made by numeric or alphanumeric codes, **called "token"** which can be used to finalise payments, replacing the data associated with them.

This solution allows the operator to save codes on its servers which have no value individually but which, once forwarded to the payment gateway, are "translated" into the underlying card data. There are many advantages to tokenization, which especially impact the security and shopping experience offered to customers.

Greater security for merchants and consumers

Saving payment card information can help **retain customer loyalty** and make **the shopping experience more frictionless**. The merchant can save the data directly see to saving the data, without the aid of tools such as tokenization. However, this choice entails very high costs because it requires very strict rules to protect consumer data.

In fact, the Payment Card Industry Security Standards Council (PCI SSC), a body formed by the main card circuits in the world - Visa and Mastercard to name two of the best known – has developed a series of rules over time that identifies real standards of a different level – Payment Card Industry Data Security Standard (PCI DSS) – in the context of payments with which all companies that deal with payments, in different ways, must comply. Saving card data on proprietary servers requires a very high degree of security and compliance with the most complex level of PCI compliance. Tokenization services have been created precisely to reduce the impact on merchants while maintaining high security standards, in compliance with the requirements of the PCI standards, **tokenization services have been created that relieve the merchant of the need to have particularly onerous certifications** and, at the same time, offer it greater opportunities for collection. The card data is actually saved on the service provider's servers, typically the payment gateway, which returns the token to the merchant to finalise the payment.

The advantages for the merchant are evident: it is relieved of the burden of data management and can simultaneously enjoy the benefits of delegating specialised subjects, increasing the security of its Ecommerce site. In reality, the opportunities are not limited to the area of security but also benefit the customer's shopping experience and, consequently, sales.

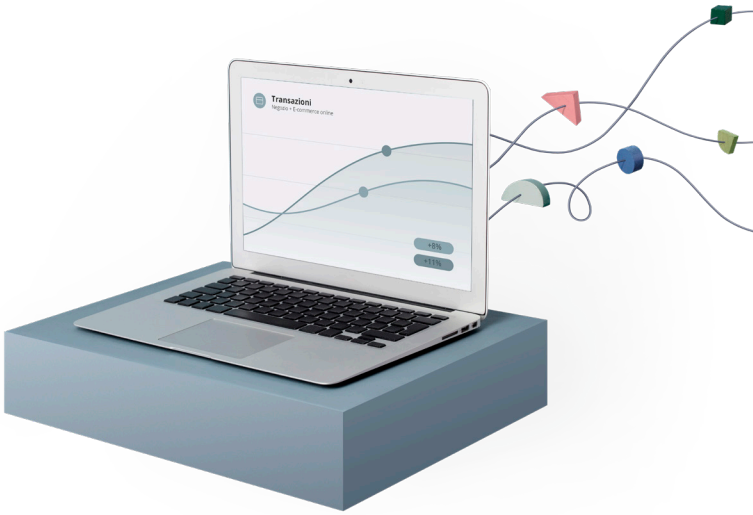
Token: the key to a personalised customer journey

The token code is therefore no longer just a technical element but becomes a strategic marketing tool and, in certain contexts, an indispensable one.

Saving a customer's card data plays a key role in the customer's purchase process because it **facilitates the customer's subsequent purchases**. Furthermore, offering customers the opportunity to save multiple payment cards further customises the customer journey, **offering a wider range of**

opportunities during checkout.

Tokenization then **reduces payment time** and helps to make the experience more fluid, especially if the customer is also asked by the company issuing the card to authenticate through Strong Customer Authentication.



Use cases in a PSD2 compliant context

The advent of PSD2 (Payments Service Directive 2) has made online payments even more secure thanks to the introduction of Strong Customer Authentication (SCA) which requires enhanced authentication with two or more factors by the buyer during payment.

In this scenario, the use of tokens becomes **essential for all those business models that involve recurring payments or payments sent by the merchant in place of the customer**. In fact, if the new PSD2 legislation provides for some exceptions and exemptions precisely for the management of these forms of collection, the use of tokens remains fundamental to finalise purchases without requiring the customer's intervention each time.

There are two types of payments affected by tokenization and included in the concepts of **exception and exemption**:

1. Merchant Initiated Transactions (M.I.T.)

These are payments entered by the operator, with the prior authorisation of the buyer, without the customer's payment order being contextual. These payments can only be made for a limited number of cases (e.g. bills and fees, telephone subscriptions, digital services, digital wallet top-ups).

2. Recurring Payments

In the case of recurring subscriptions or transactions with a fixed value, the SCA is only required for the first transaction (and not for subsequent automatic renewals). If at any point the cost of the subscription or recurring transaction changes, 3DS (3D Secure) will be required again. This obviously does not apply to those products with a cost that varies according to period and use (e.g. costs based on consumption), and that fall within those transactions labeled as "merchant

initiated" and, therefore, exempt from SCA.

By saving the card on gateway servers, these transactions can be handled independently by the merchant without the buyer's periodic intervention, who would otherwise have to periodically enter their card data to finalise the individual purchases.

Today **about 15% of Axerve merchants use the tokenization service**, and with the entry into force of PSD2 this figure is growing. The use of tokens to replace card data varies depending on the needs and commodity sector in which the merchant operates. The **most common uses** include:

1. Payment from a reserved area

The most common use is when, during payment, the **customer confirms that they want to use a card previously saved** on the merchant site. This is very common, especially with Ecommerce sites that offer a customer area within which the customer can save data for future purchases: billing address, shipping address and, precisely, card data. Today, most Ecommerce sites evaluate the implementation of tokens, regardless of the commodity sector to which they belong.

2. One-time and/or one-off payments

In this case the **token is used in the case of spot charges**. There is no specific relationship with a specific commodity sector. The transaction is often generated when an unpredictable event occurs, without a specific schedule over time. For example, in the case of tolls, parking or recharging electric vehicles at charging columns or, more generally, in the case of the occasional use of a service.

3. Bill and fee payment

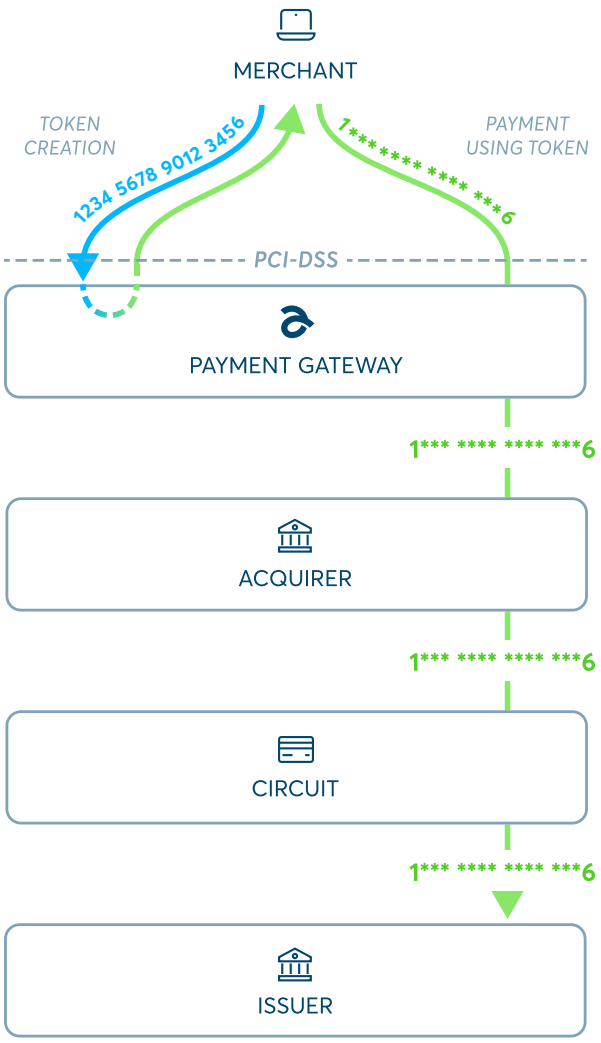
This is a typical requirement of Telco and service companies in general. Tokenization **allows the recurring charge of bills or fees** attributable to the services provided. Consider, for example, fees for ADSL and mobile telephony, or audio and video streaming services.

In all cases, the benefits of this feature are manifold, both for the merchant who, depending on the business model, wouldn't perhaps be able to collect – unless, of course, it has decided to save the card data on its servers but, as we have seen, considering a cost benefit ratio in favour of the former – and for the customer, who can count on a customer journey within which a possible obstacle is eliminated, because they may not have the card data at the moment of purchase.

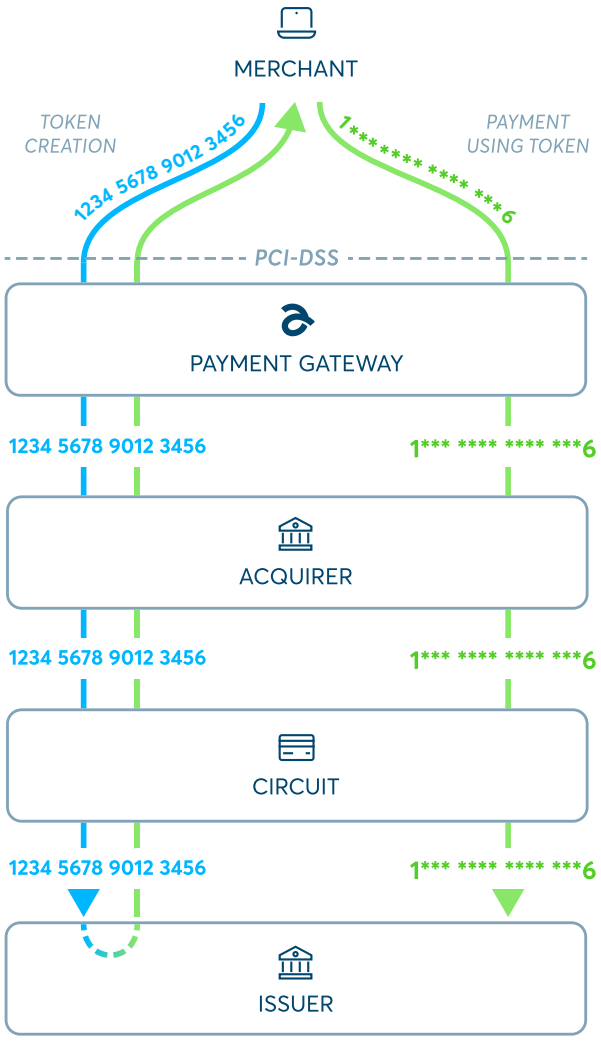
Types of tokens: Payments Service Provider and Circuit

Once the essential utility of using the tool has been ascertained, **two types of tokens can be distinguished**. In fact, if **"proprietary" tokenization** services have long existed, offered by Service Providers or payment gateways, the advent of the new European legislation regulating payments has prompted the **Circuits to develop dedicated solutions**, for example MDES for Merchants by Mastercard, with the aim of internationally standardising management processes.

PSP's Token



Circuit's Token

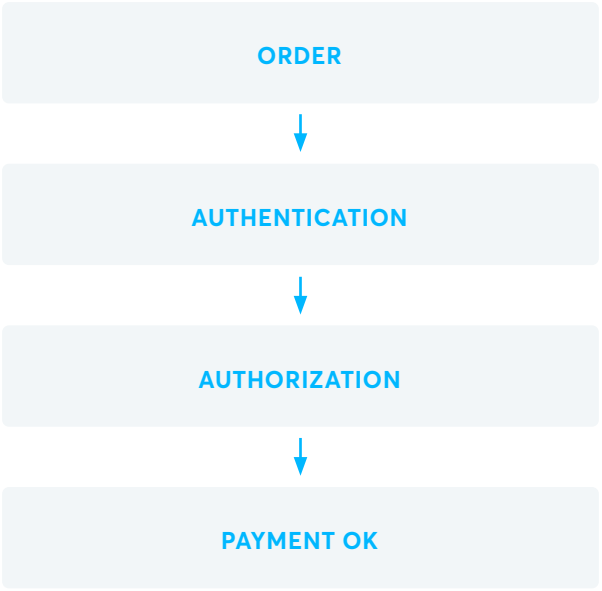


The introduction of these new forms of tokenization has brought a number of advantages to the entire system:

1. Increased authentication and authorization rate

Circuit tokens are tools developed directly by circuits that therefore fully understand their characteristics and underlying processes. The most obvious advantage is the **potential increase in authorization rates**, i.e. the possibility of having a greater number of authorized transactions and fewer SCAs required from buyers.

The payment follows this streamlined flow:



2. Simplification and cross-cutting use

The possibility of using Circuit tokens **can simplify the integrations** between Ecommerce sites and payment platforms, and the possibility of using the same tokens across multiple gateways is being studied. Before their advent, switching payment management partners also involved switching between proprietary tokenization systems, with the consequent need to use a new encryption system for the underlying card data.

3. Automatic token updating

The card data underlying the tokens may change, for example in the case of expired, stolen or lost cards. In this case, the **information** kept by the Circuits on which the payment instruments are issued **is automatically updated**, effectively eliminating the risk of non-authorisation of payments due to the failure to update card data ("Preventable" card's lifecycle declines).

4. Greater security for the consumer

Saving cards on Circuit servers also **increases the security perceived by the consumer** who, presumably, may distrust the merchant and/or payment gateway handling the payment simply because he has never relied on them for a purchase before, but it is plausible to imagine that he is amenable to entrusting his data to the circuit, even banally because the logo of the same is also printed on the card he is using. In addition, the buyer will be able to eliminate any card tokenizations from the internet banking of the card's issuing bank, further reducing the risk of fraudulent purchases.

The adoption of Circuit tokens does not in fact presuppose the abandonment of those of PSPs, but can instead be used in "combination", both to avoid radical changes in the integrations between site and gateway for merchants and to avoid complicating already-established business processes. In addition, until all issuers have joined, Payment Service Provider tokens will still be the primary tool.

Future impacts of tokenization and SCA delegation

By the end of 2020, the implementation of the provisions of PSD2 will reveal the impact on the payment system, certainly opening up new opportunities for all the actors involved. An already very topical issue that concerns the next possible developments related to tokenization is that related to the concept of SCA Delegation and Liability Shift, which in practice is the possibility for the merchant to assume the burden of Strong Customer Authentication, thus shifting the responsibility for any fraud from the Issuer to the operator.

This possibility is being studied and will be created thanks to the continuous comparison between Circuits, Acquirer, Issuer and Merchant. The role of Service Providers in this process will be fundamental, because they will be able to offer the tools and platforms to enable operators to proceed in this direction, thanks to the know-how and certifications required by the ecosystem.

Within this articulated scenario, **Axerve** has a prominent role and together with all the actors involved **is already ready to offer PSD2 compliant tokenization services**. In collaboration with the entire supply chain, it is investing in research to propose a flexible offer that can adapt to the upcoming changes in a timely manner.

Sources

1. Data presented by Roberto Liscia, President of Netcomm at Netcomm Forum Live 2020
2. European Commerce Report 2019 | Ecommerce Europe
3. E-commerce in Italia 2020 | Casaleggio Associati
4. Proofpoint Q4 2019
5. Survey Says?! ATOs Are a Major Threat and Many Merchants Are Unprepared | Riskified

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