WHITE PAPER

Ensuring e-commerce security

FIDO authentication comes to payments

netcetera

entersekt
and you're in.

Introduction

The global economy has moved online.

E-commerce currently accounts for around 21% of global retail sales and is **growing at 17% a year worldwide**[1]**.** This means there is an urgent need for reliable authentication technologies that secure e-commerce transactions without generating unnecessary friction.

While successful fraud as a percentage of e-commerce transactions remains stable at between 0.8% to 1.2% of transactions by volume[2], the number of dollars lost to criminal activity is growing fast as e-commerce volumes keep rising. Beyond these losses, fraud attempts – as distinct from successful fraud – are growing six times faster than the number of e-commerce transactions[3]. In particular, fraud methods such as Account Takeover (ATO) and synthetic ID fraud are growing very rapidly. Both rely on faking consumer identities: ATO involves stealing credentials to access accounts, while synthetic ID fraud means creating a fake identity to defraud merchants and financial institutions.

Securing transactions, smoothing the process

EU regulators and payments professionals are alive to this challenge. We expect Europe's third Payment Services Directive (PSD3) to include more stringent requirements to combat fraud beyond PSD2's existing Strong Customer Authentication (SCA) protocols. Meanwhile, the EMV[4] consortium is introducing a third generation of its 3-D Secure (3DS 2.3.1) protocols designed to protect card transactions.

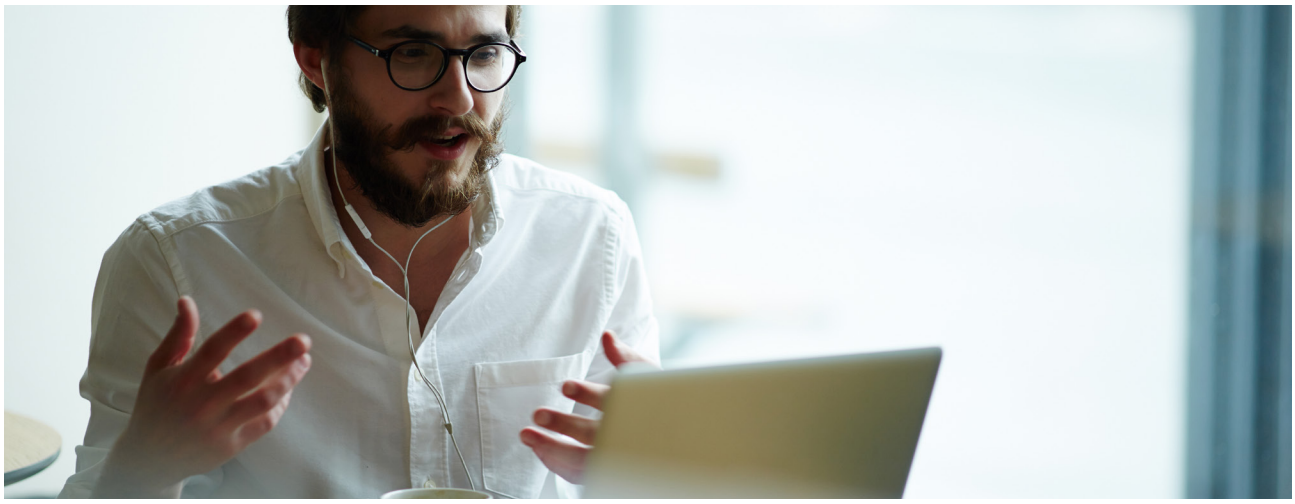
"The central challenge in e-commerce is to achieve the security of face-to-face transactions without unnecessary friction."

[1] See The Digital and Card Payment Yearbooks 2021-2022, PCM, January 2022: www.paymentyearbooks.com

[2] See FICO European Fraud Monitor, 'Total Fraud Levels': https://www.fico.com/europeanfraud/total-fraud-levels

[3] See TransUnion, 'Digital Fraud Attempts Rise 149%': https://newsroom.transunion.co.uk/suspected-financial-services-digital-fraud-attempts-rise-149-globally-as-prevalence-of-digital-transactions-increase/

[4] EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.



While new standards are welcome, they mean that action must be taken by banks and merchants to meet these new regulatory requirements in user authentication. The central challenge in today's online environment is to achieve the security of face-to-face transactions without creating unnecessary customer friction and cart abandonment. One recent study suggests almost nine in ten consumers would abandon transactions that cause too much friction[5], meaning the time is ripe for a low-friction, secure authentication technology.

Digitalizing a superior real-world solution

In what follows, we review the current authentication landscape and examine the growing challenge posed by online fraud. We look at work being done by the FIDO alliance to secure everything from investment accounts to tax returns, and consider how this level of authentication can be applied to e-commerce. Finally, we outline a world-first deployment of FIDO's industry-leading authentication standard in digital commerce and show how this solution reduces risk while delivering low friction and a smooth customer journey.

We welcome any questions about the application of FIDO's methodologies to e-commerce, and in particular how FIDO can reduce fraud risk and improve the transaction process for your customers.

Kurt Schmid

Marketing & Innovation Director Secure Digital Payments

Netcetera

Uwe Härtel

Country Manager Central Europe

Entersekt

Mathew Love

Senior Product Marketing Manager

Entersekt

[5] See this study by Tink a Visa company, in May 2022: https://ffnews.com/newsarticle/new-research-from-tink-finds-88-of-consumers-abandon-payments-with-friction/

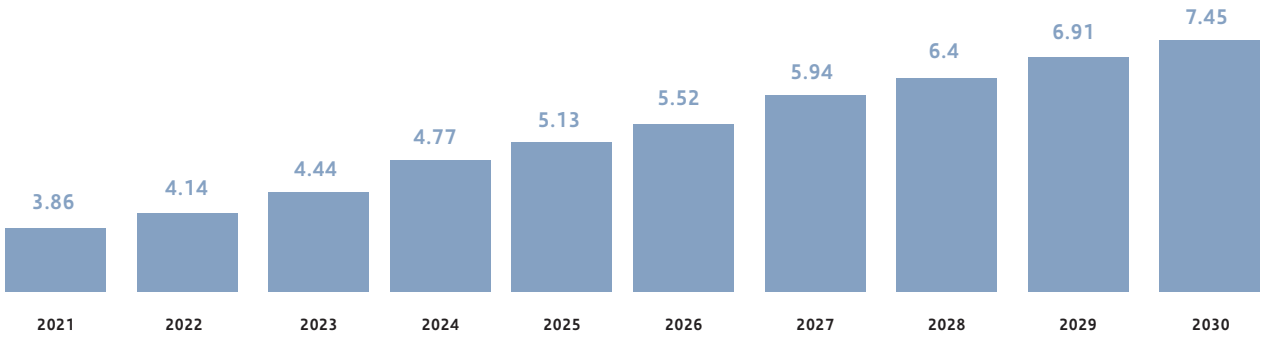
Authentication: Challenges and Opportunities

The growth of online shopping continues to be a cornerstone of the global digital revolution.

While adoption rates vary from region to region and market to market, the broad picture is that e-commerce is set to grow at between 15 and 20 percent per year over the next decade, according to Shopify[6]. Since the turn of the millennium, e-commerce has created economic opportunity and lowered costs for producers and consumers around the world.

B2C E-commerce Growth, 2021-2030

USD Trillions



CREDIT = Precedence Research

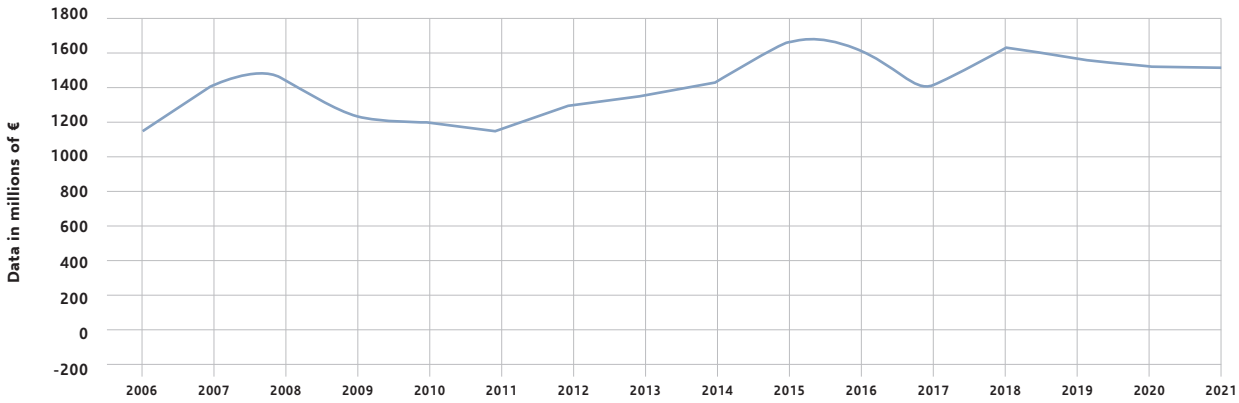
[6] See Shopify, 16 February 2022: 'Stats and Trends to Watch in 2022': https://www.shopify.ca/enterprise/global-ecommerce-statistics

Fraud – the spectre at the feast

While banks, merchants and intermediaries have done a good job to date of controlling e-commerce fraud, their efforts have demanded constant vigilance to keep up with and defend against criminal ingenuity. If the latest fraud reports from European fraud specialists FICO seem to paint a reassuring picture – that successful fraud remains low at around 1% of transaction value across Europe – then such statistics mask a deeper and more alarming truth.

"Successful attempts to keep fraud low mask rising dollar volumes as e-commerce becomes a bigger part of our lives."

Europe's fraud rate is low – but false positives are hitting revenue and trust



CREDIT = FICO

Although overall fraud rates may appear to be under control, a number of factors relating to current fraud prevention methods are affecting merchant revenue and eroding consumer trust. For instance, false positives – when a legitimate transaction is flagged as suspicious, shutting down the payment or locking an account down completely – are costing money and eroding trust. Kount, a digital fraud prevention company, reported a cost of $2 billion for e-commerce merchants in the USA alone due to false positives[7]. Similarly, Lloyd's reports that fraud costs e-commerce merchants 7.6% of their annual revenue - but false positives cost them a further 2.8% of revenue[8]. This statistic displays the extent to which false positives damage the burgeoning e-commerce industry. Worse, they also erode consumer trust and adversely impact reputational image when a legitimate sale is lost. An article by Forbes[9] affirms that 40% of consumers in Europe say they won't do business again with a merchant which declines legitimate purchases.

"40% of consumers in Europe say they won't do business again with a merchant which declines legitimate purchases."

[7] See Kount, The Silent Sales Killer: False Positives': https://www.paymenteye.com/wp-content/uploads/sites/19/2018/01/Kount_eBook_Silent_Sales_Killer_False_Positives.pdf

[8] See Lloyds Bank (UK), 'Fighting Fraud in the age if AI': https://www.lloydsbankinggroup.com/media/press-releases/2019/lloyds-bank/smelling-a-rat-lloyds-banks-fraud-team-uses-artificial-intelligence-to-help-sniff-out-scams-before-they-happen.html

[9] See Forbes Magazine, 'Three Digital Commerce Growth Opportunities': https://www.forbes.com/sites/jordanmckee/2018/11/19/three-digital-commerce-growth-opportunities/#5f0202b83822

Regulators and industry strike back

Responding to these alarming trends, the European Commission has announced the launch of consultation process designed to deliver a third payment services directive (PSD3) that will build on the security provisions set down by PSD2. In particular, the Commission has highlighted the emergence of new forms of payment fraud in the digital environment as a key driver of new legislation, and said that it has not ruled out further strengthening customer authentication requirements in PSD3 to reinforce online fraud defences.

"The European Commission has highlighted the emergence of new forms of payment fraud as a key driver of PSD3."

To date, the introduction of Strong Customer Authentication (SCA) under the provisions of PSD2 has been a success according to checkout.com[10], with 88% of European merchants reporting a positive effect on cart abandonment as a result of using SCA, and up to 92% of online transactions employing security methodologies that involve SCA in leading markets such as the UK, Germany and France. Adopting a smart exemptions strategy – for instance, by trusted buyers who repeat purchases and are identified through multiple factors – can help to further enhance the positive impact of SCA and reduce friction.

Meanwhile, the payments industry – in the form of industry consortium EMV – is introducing an improvement to its 3D secure standard called 3DS 2.3.1. The new iteration is designed to be easier to implement across multiple channels and devices, and features more rapid and accurate fraud identification, alongside richer data exchanges between merchants and issuing banks.

"Faster, easier and higher quality authentication is the core challenge facing today's payment industry."

Whether change comes through PSD3 or new industry standards, it's clear that faster, easier and higher quality authentication is the core challenge facing today's payment industry, especially as new payment forms such as authorized push payments, crypto and instant payments become increasingly popular. Put simply, there is an urgent need to reduce cart abandonment, reduce consumer friction and eliminate 'false positive' transactions that are eroding consumer trust and costing merchants and intermediaries revenue.

[10] See, checkout.com, 'Are mindsets changing on SCA?' https://www.checkout.com/blog/post/are-mindsets-changing-on-strong-customer-authentication

Introducing FIDO

Founded just under a decade ago, the FIDO ('Fast IDentity Online') Alliance is an open industry association that develops and promotes authentication standards to help reduce the world's over-reliance on passwords. Specifically, FIDO addresses the lack of interoperability among devices that use strong authentication and reduces the problems users face creating and remembering multiple usernames and passwords.

FIDO and its partners aim to achieve this through a range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB security tokens, embedded Secure Elements (eSE), smart cards, and near field communication (NFC).

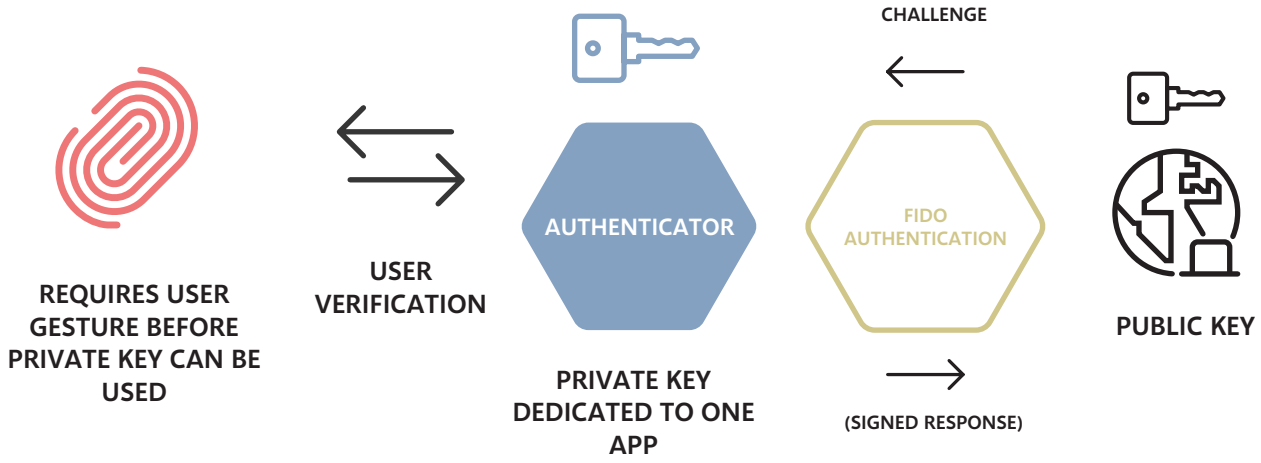
As we'll see in the next section, FIDO has been instrumental in improving user authentication and reducing fraudulent activity across many fields of activity. From a payments point of view, translating this level of authentication into an environment that demands very low levels of friction and maximum convenience is key to success.

FIDO in action

FIDO authentication standards are now used on more than four billion devices around the world, and supported by 95% of active web browsers.

More than 150 million people benefit from FIDO's password-free authentication each month. Below, we explain how FIDO works together with some live examples of FIDO in action.

How FIDO works



CREDIT = FIDO

When a user creates an account or registers on an online service that employs the FIDO standard, the device generates a set of cryptographic keys. The system registers the public key with the online service (with a FIDO server in the background) and stores the private key on the device. During authentication, the system challenges the user to prove the possession of the private key. This can be done through different FIDO-enabled authentication methods such as biometric authentication, facial recognition or multi-factor authentication, among others. Private keys are entered to the user's device after it is securely unlocked by PIN, biometric factors or other methods.

Once authentication is complete, access to online services in the cases below is very rapid and almost friction free. Another advantage of FIDO's cryptographic keys is that third-party organisations do not receive user information and therefore cannot track the user's activity across services with that information.

"For Yahoo! Japan, FIDO reduced the time taken to log in by 37%."

From virtual to digital

Having proven its worth as an authentication method for leading organisations world-wide, the challenge is to establish FIDO as an effective means of authentication in e-commerce transactions. Doing so will help stem the rising tide of fraud attempts while delivering a smoother, faster and more secure checkout process for customers, reducing cart abandonment and consumer friction while growing revenue. In the next section, we provide a case study of FIDO being implemented effectively to authenticate e-commerce transactions – and an overview of a new product that's enabling e-commerce payments with FIDO.

Key benefits of FIDO authentication

- ✓ Reduce reliance on complex passwords
- ✓ Single gesture to log on
- ✓ Works with commonly used devices
- ✓ Same authentication on multiple devices
- ✓ Fast and convenient

Yahoo Japan is an internet company offering more than 100 services, including search engine, auction, news, weather, sport, email and shopping to more than 51 million active users on its platform. For Yahoo! Japan, the act of signing in is the entry point to all of its services. This makes it critical that the experience at that entry point is a positive one for all users. At the same time, it's equally critical that every user's personal information is well protected. To find the right balance between convenience and security, Yahoo! Japan turned to FIDO. Implementing a biometric factor powered by FIDO reducing the time taken to log in by 37% and resulted in increased usage and dramatic improvements in user satisfaction.

The world's leading provider of online tax, accounting and banking services, Intuit sells these services through its three brands: Turbotax, Quickbooks and online money management service Mint. With customers in nine countries worldwide, the company wanted to reduce its reliance on passwords and cut the cost of support for login-related issues while improving security controls and standardizing its approach to security across all three brands. To achieve this, they adopted a mobile-first approach, migrating from TouchID to FIDO on their mobile apps before adding FIDO to their internet site access. Having embedded FIDO, Intuit then decreased their reliance on passwords. Through using FIDO, Intuit cut authentication times by 20% and achieved 99.9% authentication success – a 15% uplift when compared with One-Time Passcodes (OTP) delivered by text message.

A global e-commerce leader connecting millions of buyers and sellers around the world, eBay Inc. enables economic opportunity for individuals, entrepreneurs, businesses and organizations of all sizes. eBay emphasizes providing a positive and secure experience for both buyers and sellers. To add an extra layer of security to the login process, eBay implemented SMS one-time passcodes (OTPs). While this helped provide a more secure option, the method added costs and friction while remaining vulnerable to certain security issues. eBay rolled out FIDO for strong authentication across its mobile app and browser-based mobile and web sites, building its own open source FIDO server to provide maximum control of the user experience and the end-to-end login flow. Less than one year into implementation, opt-in rates are higher than for SMS OTPs and login success and completion rates have significantly improved, especially on mobile devices.

Securing e-commerce with FIDO

A world-first deployment: PLUSCARD's alternative to app-based authentication

PLUSCARD is a full-service processor for financial institutions across Germany. The company has teamed up with Entersekt, a specialist in strong customer authentication and market-leading digital solutions partner Netcetera to launch the first FIDO Certified alternative to app-based authentication in Europe.

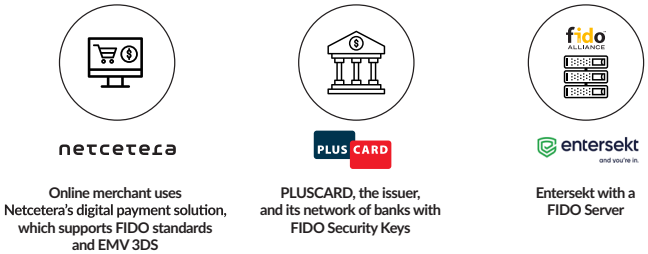
"For the first time, users are able to use FIDO security keys to authenticate and pay without leaving the merchant's website – making for a consistent, smooth and fast shopping experience."

The solution developed by PLUSCARD, Netcetera and Entersekt gives its customers the option to use FIDO2 Security Keys to authenticate themselves for payments with online merchants leveraging the latest EMV 3DS protocol. FIDO2 is a set of strong authentication standards that enables users to leverage common devices like on-device biometrics and FIDO security keys to authenticate to online services with phishing-resistant cryptographic security. The FIDO2 specifications are the World Wide Web Consortium's (W3C) Web Authentication (WebAuthn) specification and FIDO Alliance's corresponding Client-to-Authenticator Protocol (CTAP).

"Together with Netcetera and Entersekt, we have implemented a future-proof solution with the FIDO standard. To date, this is a unique alternative to app-based authentication on the German market."

- Thomas Niederauer, Product Manager at PLUSCARD

'Customers without a mobile device now have the possibility to approve their online payments conveniently and securely with the FIDO token' says Thomas Niederauer, Product Manager at PLUSCARD. 'Together with Netcetera and Entersekt, we have implemented a future-proof solution with the FIDO standard. To date, this is a unique alternative to app-based authentication on the German market.'



Every online payment that must be authenticated by PLUSCARD requires a verification of whether the account or card data were entered by the legitimate cardholder. Various methods exist that prove the identity of shoppers online, however most require the use of a mobile app. For customers that do not have a mobile device or prefer to make payments via a laptop or computer, there are very few secure alternatives available.

How it works

Entersekt provides a FIDO-certified server to the solution. PLUSCARD's cardholders then register their FIDO Security Key with their bank. The security key is linked to the customer's credit card and can then be used to easily authenticate their online transactions at merchants that have implemented the latest version of EMV 3DS.

> **"We are proud to open this new chapter of payment authentication together with PLUSCARD and Netcetera."**
>
> **—Uwe Härtel, Country Manager Central Europe, Entersekt**

As more merchants implement the latest version of EMV 3DS, which supports FIDO authentication, they will be able to work FIDO into their checkout authentication process. For the first time, users are now able to use their FIDO security keys to log into their accounts and pay without leaving the merchant's website – making for a consistent, smooth and fast shopping experience.

Secure Payment Confirmation: next-level authentication

Developed by standards consortium The World Wide Web Consortium, or W3C, Secure Payment Confirmation (SPC) allows issuing banks or their payment service providers to directly authenticate consumers using FIDO standards. SPC works as a web-based Application Programming Interface (API) that enables streamlined authentication during a payment transaction. It is designed to scale authentication across merchants using FIDO authentication protocols, and to produce cryptographic evidence that the user has confirmed transaction details.

In practice, this means taking advantage of FIDO-based authentication methods built into (for example) the operating system of a laptop, such as Windows Hello. The user simply extends the use of a fingerprint sensor normally used for Windows login to permit secure and easy payment authentications.

SPC adds payment-specific capabilities atop WebAuthn and is designed with stronger privacy protections than risk analysis approaches that rely on data collection. SPC is easy to adopt and exceeds the standards set by Strong Customer Authentication under the EU's PSD2 regulations while also preserving privacy thanks to not sharing user information with third parties.

SPC: A single user credential for all merchants

CREDIT = W3.org

How SPC works in practice

As a first step, users register a payment credential to their device consisting of a FIDO public key credential authenticated by their issuing bank or the bank's PSP.

SPC then initiates an application programming interface (API) call to the user's bank via the web browser, omitting the need to navigate away from the merchant's checkout page.

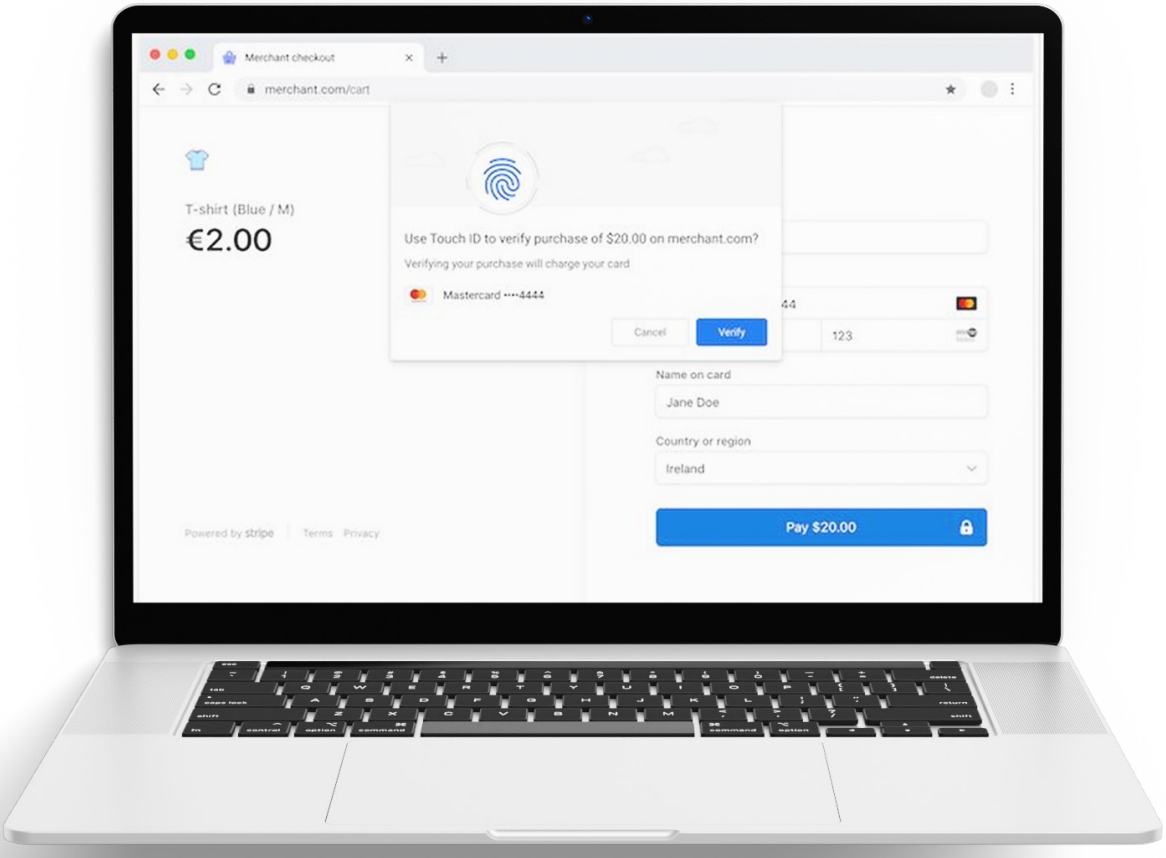
The bank or PSP confirms the user's ID via this API call, employing a secondary authentication factor (such as biometric fingerprint) for additional security and the transaction is approved.

The SPC advantage

- ✓ Rapid and secure authentication in-browser
- ✓ No navigation away from merchant site
- ✓ No requirement for external hardware
- ✓ Privacy inherent in system'

There is no requirement for dongles, external hardware or other additional software – and no navigation away from the merchant's site. Just fast, safe and secure transactions with strong authentication.

SPC is also natively supported by EMV 3DS 2.3.1, the enhancement of EMV's 3D secure (3DS) security standard for e-commerce that significantly improves the user experience by increasing the number and quality of transaction data shared between merchants and issuing banks.



Conclusion: A friction-free, secure future for e-commerce

As the world recovers from the COVID-19 pandemic, e-commerce finds itself at an inflection point. As we explain in the introduction to this paper, growth to date has been impressive, but is increasingly hampered by the very anti-fraud measures that seek to protect users from crime.

As fraud attempts grow and innovative new fraud methodologies emerge, banks and merchants need to find ways of authenticating their customers which are effective – but which are also easy to use, reducing cart abandonment, consumer friction and the false positives which can cause merchants to lose valuable revenue while eroding customer trust.

In the next few years, establishing and building customer trust is going to be vital if e-commerce is to expand from its current focus in which it is used for streaming services, gaming and the purchase of physical goods into sectors such as personal services, consulting and others. A mid-2022 study from Nexi[11] – to cite one example – claims that growth in European consumer's spending on travel over the internet has slowed dramatically as users revert to physical shopping to navigate the complexity of travel post-COVID.

"Securing payments through FIDO authentication responds to many of the concerns held by industry and end users."

In such situations, the last thing consumers are looking for is more friction at checkout and transactions unfairly blocked through 'false positive' flags. Meanwhile, consumer concerns about misuse of their personal data continue to rise, with 86% of consumers surveyed by KPMG last year[12] saying they feared what happens to their data after it's collected by companies.

Securing payments through FIDO authentication responds to many of these concerns. By using existing browsers and extending the use of authentication technologies such as biometrics which are already in place on the user's device, payments authentications are easy for the consumer to adopt. Employing an API call on the user's bank means rapid authentication and introduces the additional security of secondary confirmatory factors such as the consumer's bank details.

Coupled with the fact that FIDO authentications using Secure Payment Confirmation (SPC) exceed the existing security stipulations of PSD2 and are natively compliant with the EMV 3DS2.3 standards, FIDO-based authentications are a compelling solution to the authentication challenges faced by the payments industry. Finally, the fact that consumer data is not retained, stored or manipulated in any fashion speaks to growing consumer anxiety over privacy and data manipulation.

With more than four billion devices already using FIDO to secure access to services, we expect the introduction of FIDO via web browsers, as represented by Secure Payment Confirmation, to further enhance the consumer shopping experience and deliver faster, more accurate and easier authentications. This, in turn, should help merchants, banks and intermediaries to grow revenue, and see more sectors benefit from the digitalization of the shopping experience.

[11] See Nexi, '2021 European e-Commerce Report', 6 June 2022: https://www.nexigroup.com/en/media-relations/news/2022/06/european-e-commerce-report-2021/

[12] See Techrepublic, 'Data Privacy is a Growing Concern for Consumers' 17 August 2021: https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/

Entersekt ensures that digital financial transactions are frictionless and secure. The company provides a single cross-channel platform for financial services institutions to meet authentication requirements and optimize user experiences. With a range of options available for deployment and configuration, Entersekt's solutions are fully customizable across all channels and devices. A strong track record of over ten years' working with leading financial services institutions across the US, Europe and Africa, combined with multiple patented security innovations, has established Entersekt as global industry leader in authentication. Backed by companies like Silicon Valley-based Accel-KKR, one of the world's top private equity firms, Entersekt continues to expand its footprint across key regions. For more information, visit **entersekt.com**.

Netcetera is a global software company with cutting-edge IT products and individual digital solutions. More than 2,500 banks and issuers, and 160,000 merchants rely on their digital payment solutions and globally certified 3-D Secure products. Founded in 1996, Netcetera has 800 employees across Europe, Asia, and the Middle East.

Further information: **netcetera.com**