Entersekt

Open banking **state of play**

Why the work to secure open banking has only just begun

AN EBOOK FROM ENTERSEKT IDEAS LAB

ideas lab

FOREWORD

Onwards **and upwards**

The European conception of open banking – providing third parties with secure access to banks' rich repositories of customer data – is intended to stimulate innovation and the development of new consumer services, but there have been many delays reaching this goal in a highly complex environment.

I speak to financial institutions across Europe every day and a strong message I'm hearing from them is that 2021 will be the year we see true, widespread adoption of PSD2-powered products and services. The number of such services doubled over the last six months – jumping from one to two million. It's time to take this continent-wide project seriously.

Money management services will be a significant driver of open banking – we will see all-encompassing financial dashboards, improving our ability to budget, for example. Challenger banks offered this first, but the tier-one financial institutions are now doing it too, which will spur growth significantly.

Improvements in lending services is also something to look forward to. It will be so much easier and quicker to advance loans than before because of the amount of data available in an open banking ecosystem.

Changes in the payments framework will cause some disruption. The new ability of third parties to initiate payments directly from accounts held at other businesses could put the card networks under some pressure, although these companies are already adapting to the new environment. Their response should, in itself, drive change.

PSD2 is about opportunity, about creating value for businesses and consumers, while offering a secure, low-friction user experience. Entersekt makes it easy to authenticate users, and that's not lost on a growing number of organizations ready to embrace the future of financial services.

FRANS LABUSCHAGNE

Entersekt country manager for the United Kingdom, Ireland, Benelux, and the Nordics

Table of **contents**

INDUSTRY VOICE

Open banking needs more than **a European directive to fulfil its promise**

There could be many reasons for open banking's tepid performance in 2020. One or two of them are as obvious as they were unavoidable, but what else is holding us back in Europe? Consumers' security concerns or ignorance of open banking's benefits? The seeming absence of practical, life-enhancing use cases? The lack of a common technical approach across EU member nations? All of the above?

Rik Coeckelbergs

FOUNDER AND MANAGING DIRECTOR, THE BANKING SCENE

Founder of the The Banking Scene, Rik Coeckelbergs is passionate about building communities and, together with stakeholders of all kinds, develop ideas for sustainable new business models.

In 2009, he created a Linkedin community Innovation In Payments, which now has over 30,000 global members. He is based just north of Brussels, Belgium.

Open banking keeps making headlines in the financial services sector, with local interpretations, cultural perceptions, and market demands making for interesting opinions and discussions. So, when Entersekt asked me to write a piece on why open banking has not (yet) achieved its full potential, I decided to focus on only one continent: Europe, in this case.

Everyone in Europe expected 2020 to be *the* year for open banking. Brexit aside, the United Kingdom is celebrating its third open banking anniversary already and, despite all the negative effects of Covid-19, the pandemic did provide a welcome boost to digital banking services. Yet, there is no real consensus that open banking is delivering on its promises.

In September 2020, Europe counted 410 licensed account information service providers and payments initiation service providers, an increase of 79% year-on-year.[1] The United Kingdom's Open Banking Implementation Entity, which oversees the technology rollout, announced 3.4 million open banking payments in 2020. These numbers clearly show an appetite for open banking, yet adoption is lagging across the Channel.

So, what exactly is stopping open banking in Europe from creating the eagerly anticipated competition and innovation on the massive scale it promised?

I mean, make no mistake, banks are hesitant – and with good reason. Open banking, in full effect, could result in them having to give their data away to their biggest competitors with no reciprocation, a grave prospect for many. They might also lose the ability to promote their brand or upsell to existing customers in the way they did before. But there are other success factors at play as well, including:

- Leadership (within the bank),
- Value (for the customer), and
- Standardization (of the technology framework).

> So, what exactly is stopping open banking in Europe from creating the eagerly anticipated competition and innovation on the massive scale it promised?

Internal alignment of banks' strategies

Tink, an open banking solution provider, teamed up with YouGov recently and asked 290 financial executives from 12 European countries for their views on open banking. On a C-level, the vast majority understood the value of a long-term strategy for their banks. But where 62.5% of channel owners acknowledged open banking as an opportunity, only 45% of product owners agreed.[2] This lack of alignment within the bank is partly responsible for slowing down open banking developments.

Banking is changing. Strategic thinkers understand this and realize that banks will either do business differently in the future or not at all. On the one hand, banks must provide the most convenient and secure way for their customers to share data. They should also take their role as a "data custodians" a lot more seriously instead of claiming the data to be their own. By creating relationships based on reciprocity with third parties, they can make their customers' financial lives a lot easier, as they won't have to do everything themselves.

[1] "Number and type of TPPs per country" (September 2020); Open Banking Europe
[2] *Taking advantage of open banking: Open banking survey 2020* (December 2020); Tink

This convenience will make those customers appreciate their banks much more as it will empower them to be owners of their own financial data. Furthermore, the certainty provided by their customers falling back on third-party services will allow banks to concentrate on their core value propositions in their innovation projects.

On the other hand, banks should also start realizing the enormous value in the additional data they can collect as AISPs and how it could help personalize and streamline the service they provide to their customers.

But success comes with a shared understanding of goals, milestones, and strategies. Only if the entire organization understands open banking and is aligned to the bank's strategy in that respect, can it *really* be successful.

> Every good conversation I have had about digital transformation over the last few years has ended on the same note: that people, communication, and culture are the biggest challenges to overcome, not technology.

Of course, it is very easy to say that "a bank must understand this or that". The reality is that banks are made up of thousands of people, no two of whom will understand the implications of PSD2 in the same way. Therein lies the challenge: while it is absolutely true that the days of siloed thinking are over, groups within these large organization have their sights set on the future while others are still figuring out how to keep them running profitably today.

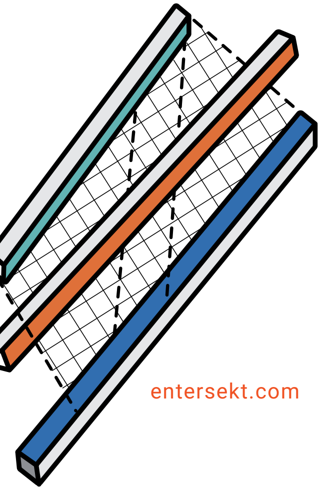
Only with consistent leadership across an entire organization will a bank be capable of fully embracing open banking opportunities. Every good conversation I have had about digital transformation over the last few years has ended on the same note: that people, communication, and culture are the biggest challenges to overcome, not technology.[3]

Convincing customers about open banking

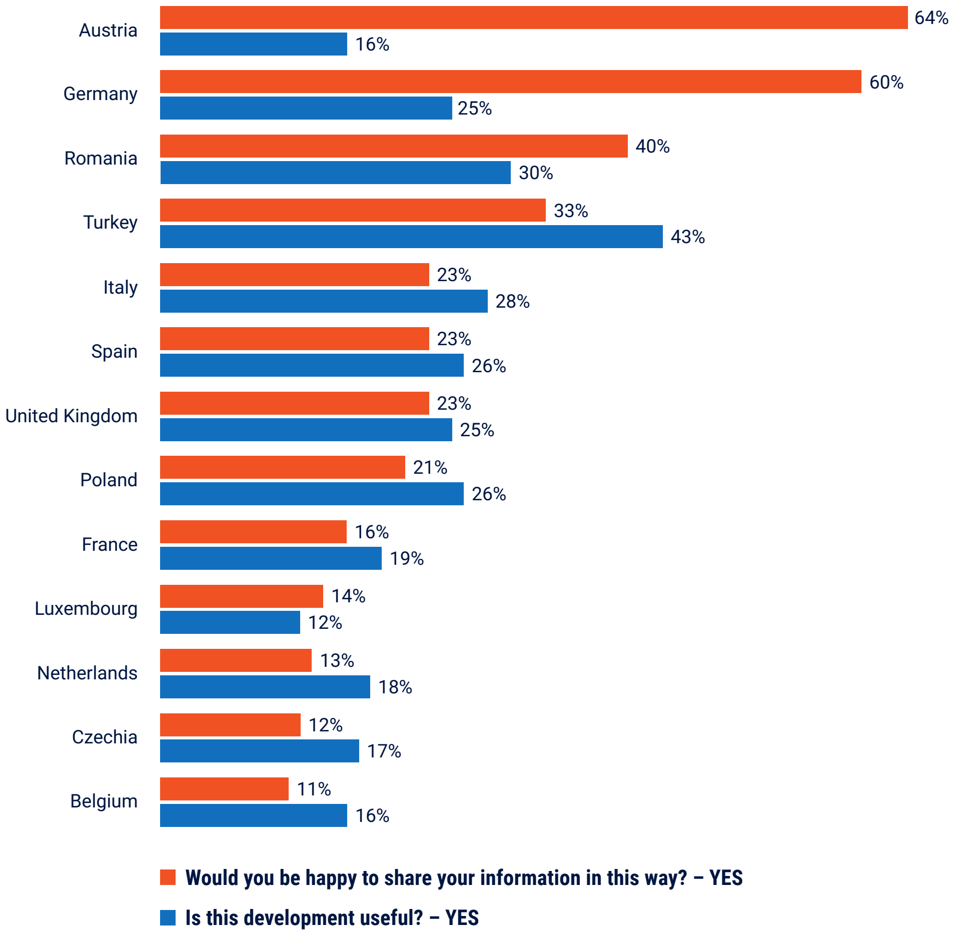
Open banking principles are much more appreciated in a business environment than in a retail environment. With more tangible advantages in the finance department and communication in a multi-bank environment, this does not come as a surprise. Embracing open banking has an immediate effect on a business's profit and loss.

According to a recent study, 50% of SME businesses in the United Kingdom are using services offered by open banking providers. The same research shows that almost 60% of them started using those services during the Covid-19 crisis, with 90% citing the pandemic as the main reason for using open banking enabled services.[4]

[3] "Banks Doing Digital Right: My Learnings of The Banking Scene Summer Event" (6 July 2020); Rik Coeckelbergs; *The Banking Scene*
[4] "Half of UK's small businesses now use open banking, says OBIE" (7 December 2020); Ruby Hinchliffe; *Fintech Futures*



In some parts of the world, new regulation makes it possible for financial providers to access your financial information held by other companies, if you give them permission.



Source: ING

Consumers seem harder to convince, though. ING surveyed consumers in 13 European countries and revealed an attitude–behavior gap when it came to open banking. It found that many people would use the new tools made available to them under PSD2 if doing so offered them greater convenience, but people were also nervous about sharing their personal data and engaging with technology in unfamiliar ways. And that included people who actually knew something about open banking.[5]

Mass adoption of open banking will require a clearer understanding of the advantages it has for consumers and the security underpinning it. It doesn't all come down to education, however. The authors of the ING survey report believe that "trust in providers, rewards, short-term needs, familiarity and even what we see our friends doing, may all conquer suspicions."

The latest *Global Open Banking Report 2020* from *The Paypers* also quite correctly states that success "will require a relentless focus on removing friction from the experience of all stakeholders – not just [end users] but also the developers and [third-party providers] that will play an integral role in shaping the future customer experience".[6]

[5] "ING survey: We're still suspicious about Open Banking" (6 October 2020); ING
[6] *The Global Open Banking Report 2020: Beyond Open Banking, Into the Open Finance and Open Data Economy* (October 2020); *The Paypers*

Lack of technological standardization

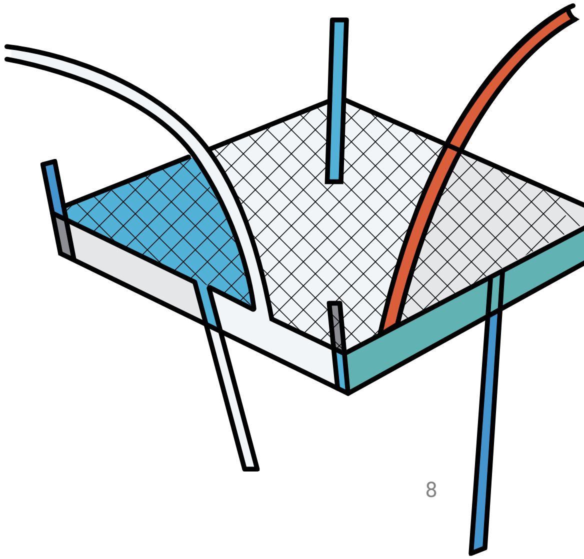
With PSD2, Europe has a continental set of regulations that is mostly implemented at the national level. The directive is technology agnostic, leaving lots of room for interpretation. However, on a second level there are regulatory technical standards set by the European Banking Authority.[7] These mandated the building of open banking on API technology to guarantee the right levels of consumer protection, privacy, and security.

But, with so many questions on the APIs unanswered and different standards across Europe, the so-called Old Continent ended up being a highly fragmented market that hindered standardization. Also, the quality of implementations on the account servicing payment service providers' side was often below expectations, causing frustrations for TPPs and compliance supervisors.

> Ever more voices in the industry are asking for an open banking scheme with a standardized set of rules for data sharing in place of the principle-based approach of PSD2.

This bad quality of implementation will, no doubt, be resolved as fintechs continue to bemoan banks' market power and supervisors become less tolerant. But the fragmentation of the market will remain. One way to overcome this is to let the market do its job and hope that, over time, most banks connect with market integrators, who also talk to each other about ensuring continental readiness.

However, ever more voices in the industry are asking for an open banking scheme with a standardized set of rules for data sharing in place of the principle-based approach of PSD2. This will certainly help grow open banking use cases to a continent-wide scale, since TPPs will no longer have to adapt to every single national interpretation.

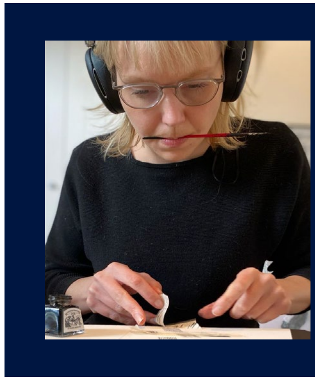


[7] Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (23 February 2017); European Banking Authority

CHARTS & GRAPHS

Not your average **open banking glossary**

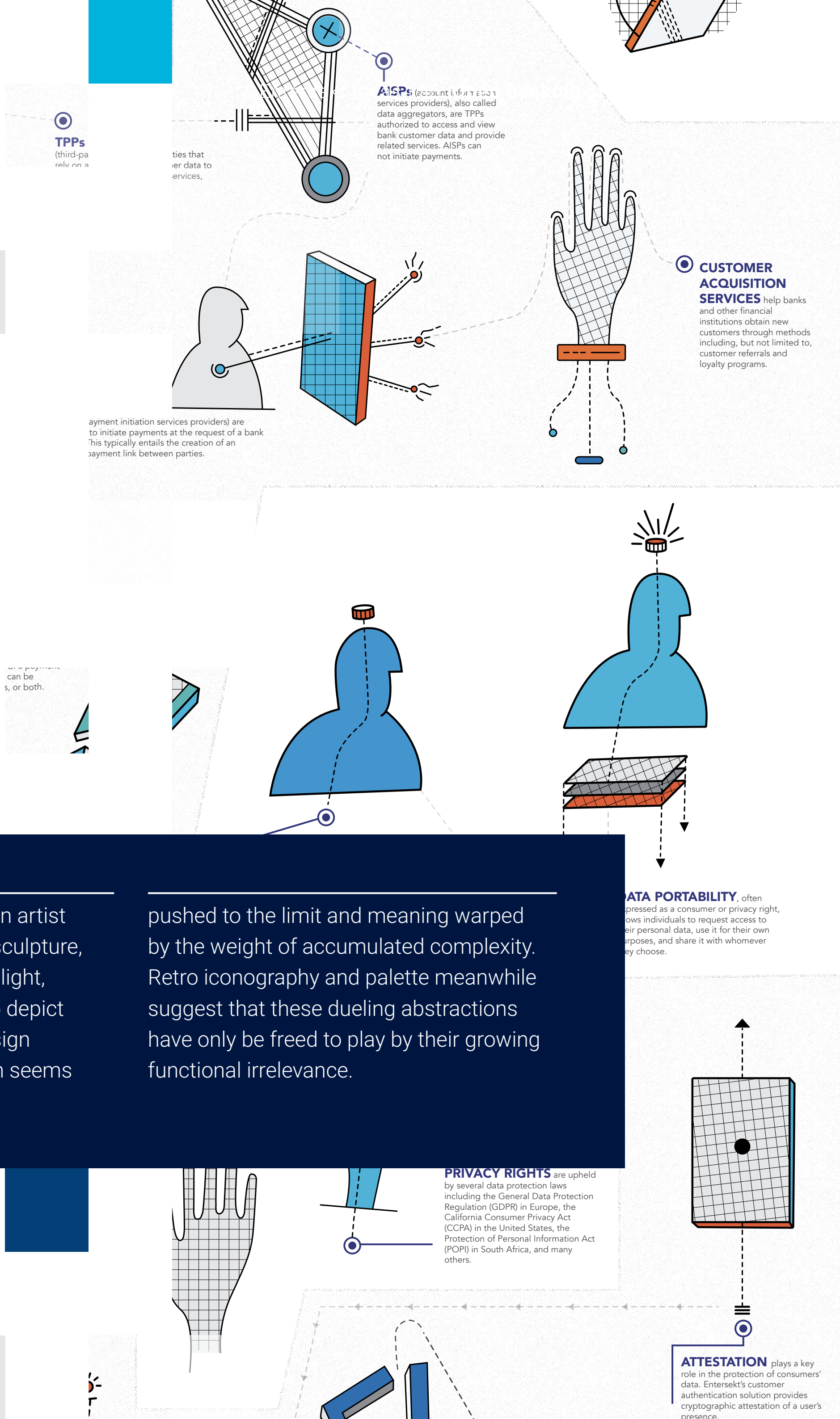
There have been scores of nearly identical PSD2 glossaries online for years, so Entersekt wanted to approach our one a bit differently. Thankfully, Maaike Bakker was at hand to help. She's an artist who frequently subjects visual metaphors from business, engineering, and science to the kind of disruptive energy open banking is set to release.



Maaike Bakker

ARTIST

Maaike Bakker is a South African artist whose work includes drawing, sculpture, and installation. She employs a light, line-driven style of illustration to depict clashing visual languages and sign systems, where communication seems pushed to the limit and meaning warped by the weight of accumulated complexity. Retro iconography and palette meanwhile suggest that these dueling abstractions have only be freed to play by their growing functional irrelevance.


TPPs (third-pa
rely on a
ties that
er data to
ervices,
AISPs (account information services providers), also called data aggregators, are TPPs authorized to access and view bank customer data and provide related services. AISPs can not initiate payments.
CUSTOMER ACQUISITION SERVICES help banks and other financial institutions obtain new customers through methods including, but not limited to, customer referrals and loyalty programs.
ayment initiation services providers) are to initiate payments at the request of a bank his typically entails the creation of an payment link between parties.
or a payment
can be
s, or both.
ATA PORTABILITY, often pressed as a consumer or privacy right, ows individuals to request access to eir personal data, use it for their own rposes, and share it with whomever ey choose.
PRIVACY RIGHTS are upheld by several data protection laws including the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, the Protection of Personal Information Act (POPI) in South Africa, and many others.
ATTESTATION plays a key role in the protection of consumers' data. Entersekt's customer authentication solution provides cryptographic attestation of a user's presence.

OPEN BANKING involves the sharing of customer data with other financial institutions and third-party providers (TPPs), essentially removing barriers between competitors and enabling access to functionalities previously reserved only for banks.

PSD2, the second Payment Services Directive effective in Europe, for example, already requires banks to cooperate with TPPs and provide the necessary security.

RECIPROCITY between banks and TPPs, or a lack thereof, has been of great concern to banks, especially under PSD2. They argue they've been placed at a competitive and liability disadvantage.

APIs (application programming interfaces) enable different pieces of software to communicate with one another, acting as a conduit of sorts for data transmission. APIs are preferred among banks and TPPs for accessing customer data.

PLATFORM BANKING takes the form of a digital marketplace that offers both banking and non-banking financial services.

SCREEN SCRAPING also enables access to customer data but involves the copying of data from a website using a program. Though technically allowed under PSD2, screen scraping conflicts with certain privacy laws and is not as secure as APIs.

AISPs (account information services providers), also called data aggregators, are TPPs authorized to access and view bank customer data and provide related services. AISPs can not initiate payments.

TPPs
(third-party providers) are entities that rely on access to bank customer data to provide account information services, initiate payments, or both.

CUSTOMER ACQUISITION SERVICES help banks and other financial institutions obtain new customers through methods including, but not limited to, customer referrals and loyalty programs.

PISPs (payment initiation services providers) are authorized to initiate payments at the request of a bank customer. This typically entails the creation of an electronic payment link between parties.

PSUs (payment service user) are users of a payment service. These can be payers, payees, or both.

CUSTOMER DATA
comprises more than personal or financial details, but all identifiable information that can be used for account-related purposes or even to perform know-your-customer (KYC) and due diligence checks.

DATA PORTABILITY, often expressed as a consumer or privacy right, allows individuals to request access to their personal data, use it for their own purposes, and share it with whomever they choose.

DIGITAL IDENTITY is all personal data stored in electronic form that, once validated, can serve as the digital equivalent of a unique identity in the physical world.

PRIVACY RIGHTS are upheld by several data protection laws including the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, the Protection of Personal Information Act (POPI) in South Africa, and many others.

CONSENT by every PSU is required before any TPP can access their bank account or data. The process of obtaining consent is normally handled by the TPP.

ATTESTATION plays a key role in the protection of consumers' data. Entersekt's customer authentication solution provides cryptographic attestation of a user's presence.

SCA (strong customer authentication), as defined in the European Banking Association's regulatory technical standards, is Authority's comprising two or more of the following factors: knowledge, possession, and inherence. Under PSD2, banks must provide SCA to achieve compliance.

AUTHENTICATION is the process by which a pre-established identity is verified, typically in a digital context.

3-D SECURE is a security protocol protecting card-not-present payments. It not only meets SCA requirements under PSD2, but ensures a desirable mix of passive and step-up authentication, depending on risk.

SOLUTION SPOTLIGHT

It’s 2021. **Compliance is no longer enough**

PSD2 has two central goals: to protect the consumer by increasing payments security and promote competition in the pan-European payments market. Unfortunately, SMS OTP technology fails to support either of these.

Pieter de Wet

SALES DIRECTOR GLOBAL ACCOUNTS, ENTERSEKT

A recognized authority on banking and payments technology, Pieter was fundamental in establishing the Emerging Payments Exchange Southern Africa.

With ten years’ experience in senior management, his expertise spans the entire payments industry, with a special focus on mobile and payments business models that promise to grow Entersekt’s presence across the world.

With multiple deadlines for implementation behind us, almost every European bank should be operating within the compliance limits of the second Payment Services Directive (PSD2). Only those in the United Kingdom have been granted a further extension on the directive's strong customer authentication (SCA) requirement.

While banks were focused on compliance in 2020, a lot changed around them. And no more so than for consumers owing to the pandemic. Much more happens online these days; in fact, consumers in some countries barely leave home as lockdowns continue to be enforced. There has also been a sharp increase in first-time online shoppers. According to a Lumina Intelligence report, for example, 18% of UK consumers have changed their primary method of grocery shopping to online in the last year.[8]

Which begs the question… with the uptick in online activity, and SCA posing an abandonment risk at checkout, shouldn't banks be focusing on more than mere compliance? Where one unsuccessful transaction is one too many, surely it is worth pursuing an approach that makes SCA as frictionless as possible for most users, most of the time?

Entersekt

New directions in **authentication**

How advanced new technologies, deployed in tandem, point to a passwordless future

AN EBOOK FROM ENTERSEKT IDEAS LAB

ideas lab

New directions in authentication

Download this ebook, which throws the spotlight on passwordless authentication.

How strong is strong?

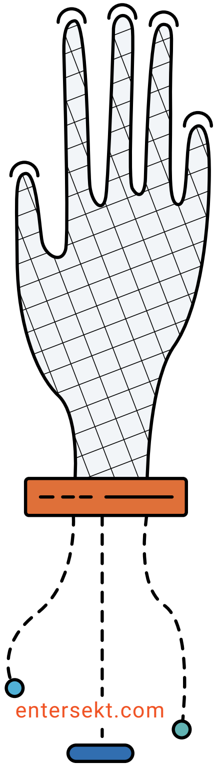
A few years ago, KuppingerCole found SMS one-time passwords to be the most popular form of authentication among European banks in the lead-up to the PSD2 deadline.[9] Unfortunately, their continued widespread use has done nothing but prove how short they fall on both security and user experience.

> Since 2015, SIM-swap fraud has increased by 400% in the UK, resulting in a staggering loss of 10 million British pounds between then and mid-2020.

Not only can an SMS be intercepted through malware, but it's susceptible to SIM-swap fraud as well. Since 2015, SIM-swap fraud has increased by 400% in the UK, resulting in a staggering loss of 10 million British pounds between then and mid-2020.[10]

A high-profile example that jumps to mind is the hacking of Twitter CEO Jack Dorsey's own Twitter account via a SIM swap in September 2019. Dorsey's account posted rogue messaging for a full 15 minutes before his team could regain control. Although his bank account was untouched, the incident severely impacted the credibility of the platform and proved how easy it is for fraudsters to engineer an attack – and how brazen they are.

Realizing its flaws, and to protect consumers, the EU Banking Association mandated the use of a PIN or a password along with an OTP. While the combination satisfies the SCA regulatory requirement, it still adds another step to the payment process – with no guarantees. There is often a second or two's delay before the SMS arrives, then the user must switch screens to retrieve the OTP and switch back again to continue with the transaction. On occasion, the SMS may be delayed or not arrive at all, in which case the user needs to request another OTP via SMS.

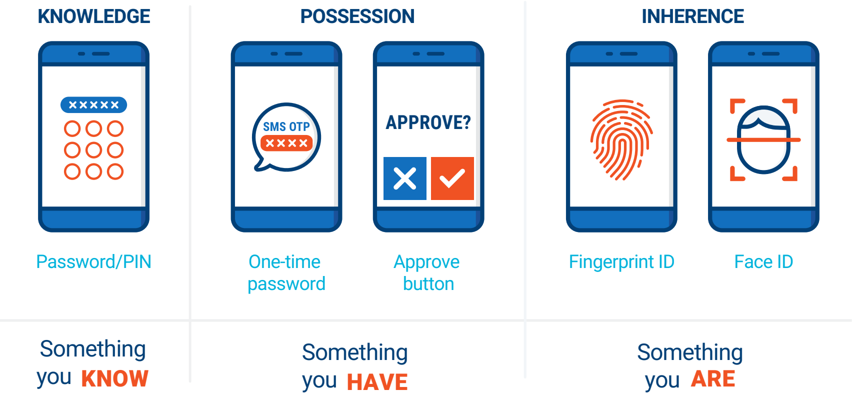


[8] "Local shopping trend set to continue, says Lumina Intelligence" (11 February 2021); Findlay Stein; *Scottish Local Retailer*
[9] "The future of banking: Innovation and disruption in light of PSD2" (March 2017); KuppingerCole
[10] "On the perils of SIM swap fraud (and how to stop it)" (3 December 2020); Chris Curd; Mi-Pay

In pursuit of safe, sophisticated payment experiences

Under PSD2, multifactor authentication comprising at least two of three types of customer information must be presented:

- Something they own, such as a mobile phone
- Something they know, like a PIN code or password
- Something they are, as determined by, say, a fingerprint scan or behavioral analysis



Under PSD2 SCA, multifactor authentication comprising two of three types of customer information must be presented: possession, knowledge and/or inherence.

There are several alternatives to SMS one-time passwords and indeed other SIM-based authentication methods that can fulfil these requirements. Only a few of them strike that all-important balance between robust security and a smooth experience.

Fintech champion MEDICI recommends a combination of 3-D Secure and "mobile intelligence-based identity technology" – which could include biometrics, behavioral biometrics, or location-based services – to not only meet PSD2 SCA compliance but tick several other boxes as well.[11] Indeed, this is the method Entersekt recommends to its own customers, as it allows for implementation of:

- A frictionless flow *without* step-up, minimizing the need for SCA.
- A challenge flow *with* step-up, ensuring a seamless in-app authentication experience when invoked.

The latest version of 3-D Secure from EMVCo, a global industry consortium, uses risk-based authentication – a method that draws on several enhanced data sources to verify identity – to passively authenticate users through their devices. This combination eliminates active step-up events for all but the most risky or suspicious transactions, greatly helping to smooth online payments for consumers.

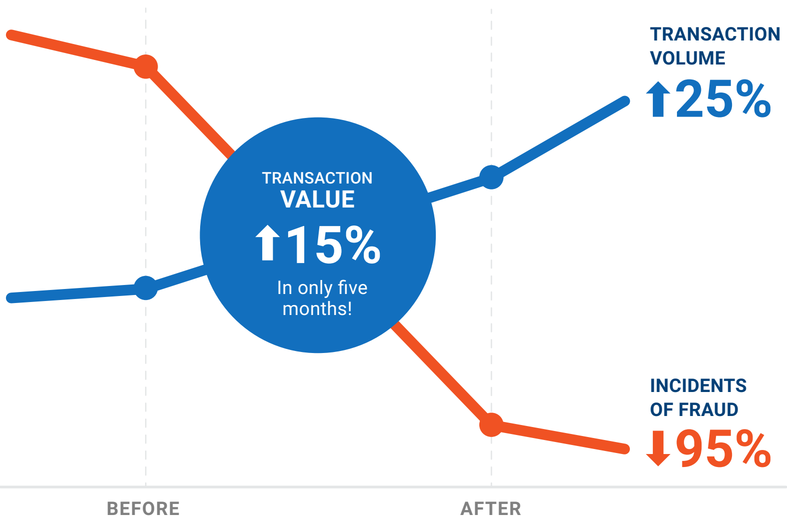
Entersekt has improved the user experience of 3-D Secure with features like automatic cardholder enrolment, interactive screens to guide the user through the process, and certificate-based push authentication and transaction signing. Only the first 3-D Secure transaction involves a step-up authentication in order to identify the consumer's device and tie it to their profile at the bank. All subsequent transactions are a one-click-only procedure, thus far superior to one-time passwords in ease of use.

[11] "PSD2 SCA: The Strategic Value of 3DS2 and Phone-Centric Identity" (13 January 2021); MEDICI

For the consumer, this method guarantees a frictionless, smooth, and secure process, much more in keeping with the spirit of PSD2. When implemented for one customer in Europe, our method substantially reduced cart abandonment, cut fraud by 95%, and increased transaction volume by 25% over a period of five months. Not only did the number of transactions increase, but their value did too by 15%, signaling greater consumer confidence in the payment process.

> For the consumer, this method guarantees a frictionless, smooth, and secure process, much more in keeping with the spirit of PSD2.

Customer success: Improved usability driving channel growth



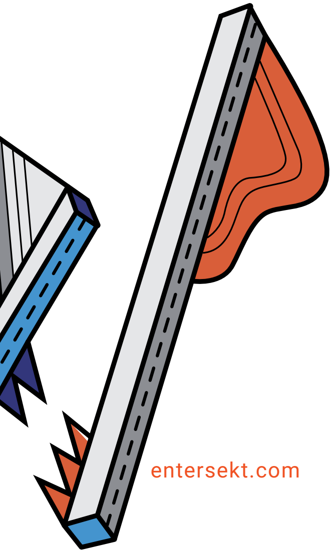
The road ahead for PSD2 compliance?

There is no doubt that SMS one-time passwords tick the necessary compliance boxes, but their deployment now could signal a lack of attention to the aims of PSD2 and a lack of awareness of the increasingly vigorous competition in the online payments industry.

Does that sound too harsh? I understand, of course, that many businesses needed a stopgap and went with the devil they and their customers knew. But it will be user experience that determines market share, and it's possible that only a small percentage of businesses have, as a whole, grasped this. Banks have, after all, traditionally focused on providing financial products, rather than experiences. Tech companies are much more inclined to concentrate on identifying and solving user problems.

Over the next few years, we expect to see increasing collaboration between banks and tech firms as competition surges, and it will be interesting to see how a new dynamic develops. New players will enter the market, while some will disappear. We are at the beginning of a new era, and regulations like PSD2 will have a substantial impact on the market.

Compliance is, of course, a critical issue. It's how you approach it that could make the difference between success and failure. To stay competitive, current industry participants should pay closer attention to the *subtext* of the regulation. Their customers' fast-emerging new lookout and modus operandi will flow from it.



IN THE LAB

Security and compliance – **on paper and in reality**

SCA compliance can be assessed conceptually, but it is essential that the security provided by any new application be evaluated by an experienced auditor, who must take into account the method of implementation and its intended environment. Take, for instance, app-based authentication, which must address vulnerabilities of the mobile device itself.

Dr Detlef Hillen

MANAGING CONSULTANT, SRC SECURITY & CONSULTING

Detlef Hillen is a security consultant at SRC Security Research & Consulting, an independent German digital security consultancy that designs, develops, evaluates, and certifies security applications for electronic payment transactions, smart card applications, e- and m-commerce, digital signatures, and computer network security. He joined SRC in 2001 following time at debis IT Security Systems, the Technical University of Munich, the University of Münster, and the University of Bonn.

Part of PSD2's regulations state that access to account data and payments must be secured using strong customer authentication (SCA).[12] While similar requirements already existed for payments on the Internet, PSD2 extended their scope to all types of electronic payments (payments at the POS terminal, payments on the internet, credit transfers via online banking) and the online access to account data.[13] [14] These requirements are specified in more detail in the associated regulatory technical standards and other opinion documents of the European Banking Authority.[15] [16]

The directive and regulatory technical standards define SCA and specify what elements must to be implemented, but they do not say *how* to do it. This means that SCA compliance on paper may not necessarily meet the level of security intended by national and international regulators, nor by banks' own security policies and risk management systems.

REPORT

Transakt: **PSD2 strong authentication compliance report.**

SRC compliance report

SRC described Entersekt's SCA solution "state of the art" in 2018. Download a summary of its compliance report.

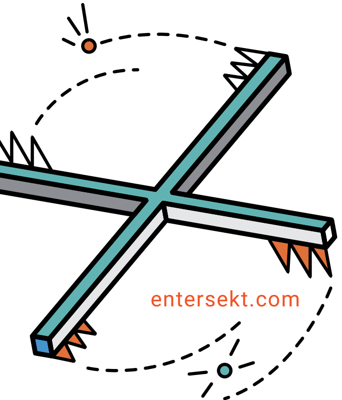
The true measure of security

Complying with PSD2 requires that SCA applications meet certain regulatory technical standards; for example, that the possession factor cannot be replicated (Article 7) and that authentication factors must be independent of each other (Article 9). Implementing these requirements improves security, but by how much – and does it even indicate PSD2 compliance?

To determine a solution's security level, it is necessary to know the attack potential needed by an attacker, which also indicates the probability of a successful attack on an application or its associated authentication process. Attack potential is based on human or other entities':

- General and application-specific knowledge,
- Experience, and
- Possible efforts (in terms of money, time, equipment).

The common criteria and the framework for implementing the eIDAS regulation define attack potential and the related security levels, as well as formal procedures for assessing it.



[12] Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market (25 November 2015); The European Parliament and the Council of the European Union
[13] Recommendations for the security of internet payments (April 2012); European Central Bank
[14] Final guidelines on the security of internet payments (19 December 2014); European Banking Authority
[15] Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (23 February 2017); European Banking Authority
[16] "Opinion of the European Banking on the elements of strong customer authentication under PSD2" (21 June 2019)

PSD2 and regulatory technical standards provide few concrete requirements to ensure SCA is implemented correctly providing a sufficient security level. PSD2 also does not include information regarding resistance to attacks, so there are no related requirements in the technical standards. Therefore, an application's PSD2 compliance does not mean that it ensures an appropriate level of security.

PSD2 compliance can be evaluated *conceptually*, but such an evaluation only determines the level of security achievable when everything has been implemented correctly and integrated into a system environment that supports it adequately. On the other hand, the security level can only be assessed by a full security evaluation of a given implementation, taking into account the system environment of that implementation.

Security of app-based authentication methods using mobile devices

If, for example, an SCA solution is implemented on a mobile device, its security can only be assessed by taking into account the security of the device itself.

For app-based authentication, the possession factor is implemented through an app with personalized keys bound to the customer's mobile device. The second authentication factor is the device's app password or PIN (a knowledge factor) or its biometric login method (an inherence factor). Both factors of authentication are implemented on the same mobile device.

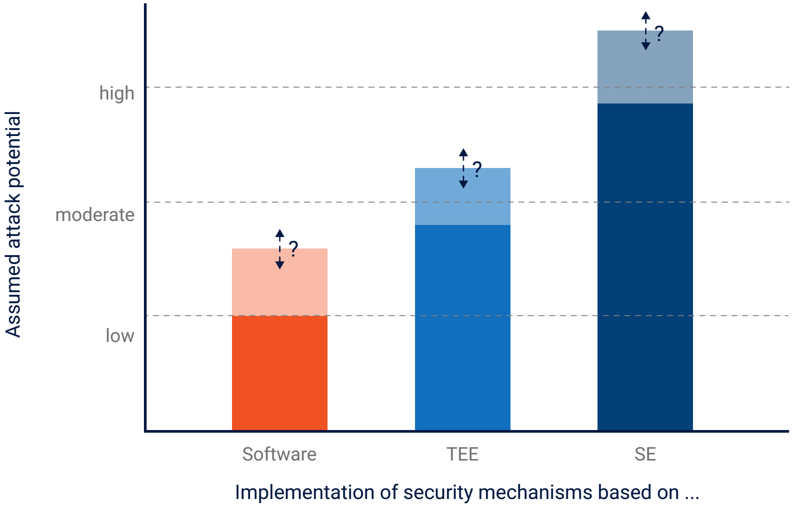
> If an SCA solution is implemented on a mobile device, its security can only be assessed by taking into account the security of the device itself.

App-based authentication is becoming increasingly popular, both for online banking and for card payments (at the POS terminal or as part of e-commerce). The European Banking Authority has confirmed that such single-device solutions can be PSD2 compliant under certain conditions, and as long they also satisfy all requirements of the regulatory technical standards, such as the independence of the two factors of authentication.

> **Erhard Brand, research and development leader at Entersekt, comments:**
> "While mobile device and application security is a very important topic to consider, the server also has a role to play. The mechanism of generating a cryptographic signature on the mobile device and using it to verify message origin and integrity on the server can strengthen the security of the entire solution.
>
> "To protect the keys used to create the digital signatures on the mobile device, hardware-backed key generation using the mobile devices' trusted execution environment or secure element should always be used when available. The use of digital signatures is a widely implemented security pattern, which is followed by Entersekt as well."

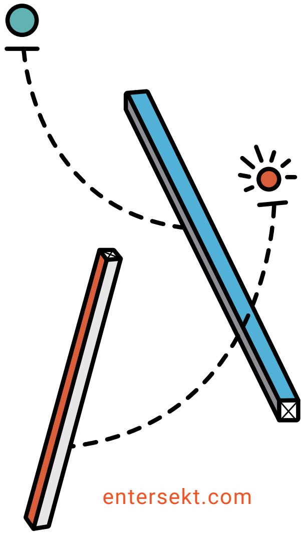
Many of the security measures of app-based authentication solutions are implemented as part of the app's software – often based on a software development kit (SDK). This software exists in a potentially unsafe environment (the operating system and other apps on the mobile device). So, even if the app can theoretically deliver SCA, it could still be vulnerable to attacks. That depends on whether the app's security is supported by the operating system or hardware of the mobile device. Here, it is important to distinguish between a pure implementation in software, the use of a trusted execution environment (TEE), or the use of a hardware-based secure element (SE).

In the figure on the right, the level of security that can be achieved based on the various system requirements has not yet been clarified, hence the question marks. Only a full evaluation by an experienced security auditor – taking into account all the particular characteristics of that implementation – can establish its true effectiveness.



An app's security level depends on how the security measures are supported by the hardware and operating system of the device.

Losing PSD2 compliance because of a weak security level



As I have explained, just because an app is PSD2 compliant, it does not necessarily mean it is sufficiently secure. Conversely, if the implementation has a low security level, the authentication process may not be PSD2 compliant.

For example, imagine an app's software (SDK) can be compromised by an attack with a low attack potential in such a way that the second authentication factor can be bypassed. Article 9 of the regulatory technical standards, however, requires that the two authentication elements be independent so that the breach of the first element does not compromise the reliability of the second element. So, if the two factors are not independent (as it is for this example), the authentication application is no longer PSD2 compliant.

Another example involves a device's biometric functionality being used as the second factor of authentication. In this case, the implementation of the biometric method must comply with Article 8, which requires that there be a very low probability that an unauthorized party will be authenticated as the authorized party.[17] If a device's biometric implementation has a low security level, this application may not meet PSD2's SCA requirements.

[17] In Germany, very low probability is defined by the Federal Office for Information Security as lower than 1/33,000 (taken from the probability of guessing a 5-digit PIN in three attempts or less).

Implications for the introduction and use of app-based authentication methods

Authentication solutions have to be usable on a wide range of mobile devices, and not only on the latest models. This adds complexity because the security of a new application depends, in part, on the technical conditions of the mobile device, which vary from model to model. Another factor affecting security is the rapid technical developments in app-based authentication solutions themselves. While this can boost security, it can also increase the sophistication of attacks.

Therefore, according to Article 2, deployers of new app-based authentication methods – providers of online banking systems, schemes responsible of card-based payments – must implement additional security measures, such as ongoing transaction monitoring to detect unauthorized or fraudulent transactions, comprehensive risk management, and well-defined processes for approving new authentication applications.

CHECKLIST

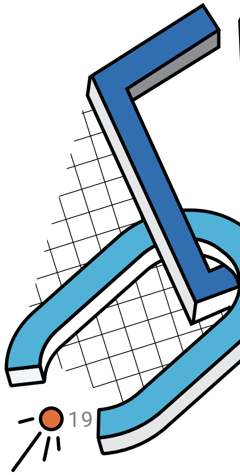
PSD2 strong customer authentication checklist.

Entersekt's RTS scorecard

Download Entersekt's quick reference guide to the European Banking Authority's regulatory technical standards on strong customer authentication.

At least for money transfers in online banking and for card payments in e-commerce, they must also continuously document and evaluate fraud rates in accordance with Article 19. When combined with recorded security-relevant data about the implementation of the authentication app on a particular mobile device, providers can determine on which devices a new authentication method can be safely deployed. This is an ongoing process and is not finished with the authentication solution's rollout.

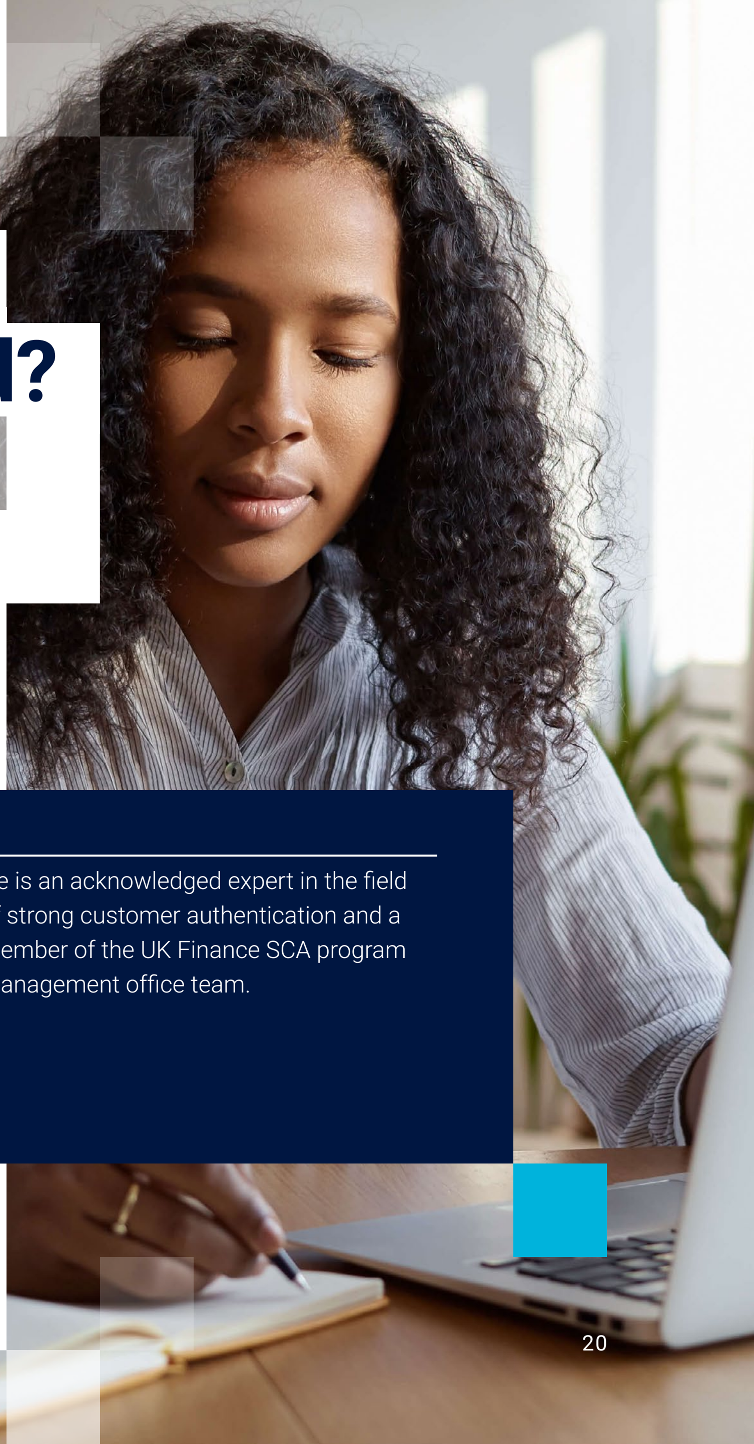
According to Article 3, the provider must have the security measures evaluated and audited by IT security and payments auditors. However, the regulatory technical standards do not specify requirements for this evaluation and auditing. The evaluation of each implementation should look at the specific characteristics of the mobile device to which the solution will be deployed to determine the attack potential it could (probably) resist. The evaluated implementation should only be permitted for use on the given type of mobile devices if the attack potential is acceptable according to the provider's risk management regulations.



FUTURE FOCUS

Where is strong customer **authentication for payments headed?**

The financial services industry's SCA journey is still at a very early stage. Solid progress was made in Europe in 2020, but there is much work to be done by all stakeholders to deliver a great e-commerce customer experience. And SCA is not just a European requirement; it has far wider geographic applicability.



Mark McMurtrie

DIRECTOR, PAYMENTS CONSULTANCY

Mark McMurtrie is the founder of Payments Consultancy, an award-winning independent consultancy working with issuers, acquirers, payments service providers, merchants, and technology providers.

He is an acknowledged expert in the field of strong customer authentication and a member of the UK Finance SCA program management office team.

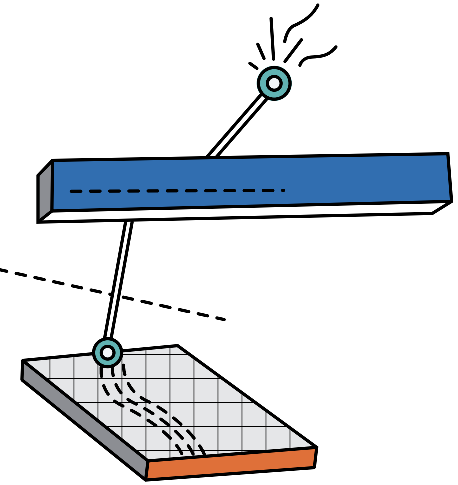
Europe's PSD2 regulations require a form of multi-factor authentication referred to as "strong customer authentication" (SCA) to protect remote electronic transactions and to enable secure access to accounts. Active enforcement by the national competent authorities for e-commerce transactions commenced on 30 December 2020, with the exception of the United Kingdom where the FCA has agreed to a delayed deadline of 14 September 2021.[18] Many countries have also agreed to soft decline ramp-up plans to avoid a "cliff edge" deadline, from August 2020 in Belgium, between January 15 and March 15 in Germany, and from 31 May in the United Kingdom.

Non-compliance comes with significant fines and the risk of losing financial services licenses. Most of the attention has thus been on ensuring legal compliance, with many regulated entities declaring they would be compliant by the deadline even when they didn't have a project plan to back it up.

3-D Secure technology steps into the gap

The underlying technology that most impacted organizations are using to achieve SCA compliance is 3-D Secure, a protocol now managed by EMVCo, a consortium consisting of the larger card networks. The European Banking Authority's regulatory technical standards for SCA do not force use of any particular version of 3-D Secure, so we can expect a variety of versions to be implemented, including the original 3-D Secure 1, which today accounts for 43% of transactions processed in the United Kingdom.

EMV 3-D Secure (also referred to as 3-D Secure 2) will, in future, be the most widely deployed version – as a mixture of EMV 3-D Secure 2.1, 2.1 with Mastercard extensions, and 2.2. There has been strong adoption recently on the issuer side, but the acceptance side is lagging behind and today only accounts for 9% of transactions processed. Latest reports show that 23 of the SCA-implementing countries have lower than 25% merchant readiness for EMV 3-D Secure. Germany, however, saw a rapid increase in adoption during December 2020.



Optimizing the user experience

The priority for 2021 should be to move beyond mere compliance to optimizing the user experiences, ensuring that the right transactions are sent for authentication and that an appropriate level of friction is applied in each case.

The primary reason for the introduction of SCA was to tackle financial fraud and the threat it represented to an effective, widely adopted open banking regime. In the same way that "chip and PIN" improved the security of face-to-face card payments, SCA protects remote electronic payments.

[18] In this context, a national competent authority (NCA) is the organization in each EU member state that holds responsibility for monitoring compliance and enforcement of PSD2. NCAs are frequently national central banks. In the United Kingdom, the NCA is the Financial Conduct Authority.

There has been great concern in the retail, payments, and financial services industries over SCA's impact on the digital user experience, which many fear will drive up abandonment and slow consumer adoption of new services.

> The higher the version of 3-D Secure in use, the greater its support of PSD2 exemptions. All stakeholders should be preparing to add support for EMV 3-D Secure 2.2 during 2021 to take maximum advantage of SCA exemptions.

Fighting fraud with minimal user friction requires a risk-based approach. PSD2 allows certain card transactions to be sent "direct to authorization" with an exemption or out of scope indicator included. The higher the version of 3-D Secure in use, the greater its support of PSD2 exemptions. All stakeholders should be preparing to add support for EMV 3-D Secure 2.2 during 2021 to take maximum advantage of SCA exemptions.

These include:

- **Transaction risk analysis exemption**, which frees payment service providers from applying SCA to transactions with a low risk of fraud.
- **Whitelisting** of merchants by cardholders, who can then enjoy a simpler checkout experience.
- **Delegated authentication**, where the merchant sends data to the issuer proving it has already authenticated the customer. This enables a PSD2 compliant one-click payment.
- **Requestor-initiated payments**, which allows merchants to initiate transactions themselves, drastically simplifying SCA of recurring payments, including those with varying amounts, like utility bills.
- **Decoupled authentication**, where SCA, separated from the transaction event, can take place days after payment has gone through, with the use cases being mail and telephone-based orders.

Using the exceptions optimally should bring down abandonment rates and help reduce transaction costs.

Tackling fraud intelligently

SCA is not a silver bullet for tackling fraud and theft of data. It is a single albeit powerful tool. To cover all bases, issuers should expand their investment in digital security to include a wide range of a fraud prevention and authentication tools. Multiple authentication layers, when weaved together, deliver defense in depth.

SMS one-time passwords have been widely implemented ahead of the SCA deadline, despite industry concerns about their vulnerability to attack, including SIM-swap fraud. In the United Kingdom, one-time passwords are being combined with a behavioral biometric in order to achieve legal compliance. There are, of course, other technologies on the market that offer both improved fraud protection and payments experience.

Mobile banking apps offer a great SCA experience. The channel is expected to become the most significant for authenticating users, but it will take time to reach mass adoption. There is a significant percentage of banking users who are yet to go mobile. In any case, delivering a consistent user experience across multiple known end points is increasingly important.

PSD2 allows issuers to delegate authority for authentication to a third party, a concept called “delegated authentication”. With the right tools – EMV 3-D Secure and FIDO being two – merchants can thus take back control of their customers’ SCA experiences, bringing authentication into their apps and under their own brand.

Entersekt

New directions in **authentication**

How advanced new technologies, deployed in tandem, point to a passwordless future

AN EBOOK FROM ENTERSEKT IDEAS LAB

ideas lab

New directions in authentication

Download this ebook, in which Entersekt CTO Gerhard Oosthuizen explains how delegated authentication works.

Snag list

No system this complex goes live without a hitch. There are tasks outstanding, improvements that must be made, and some unanswered questions.

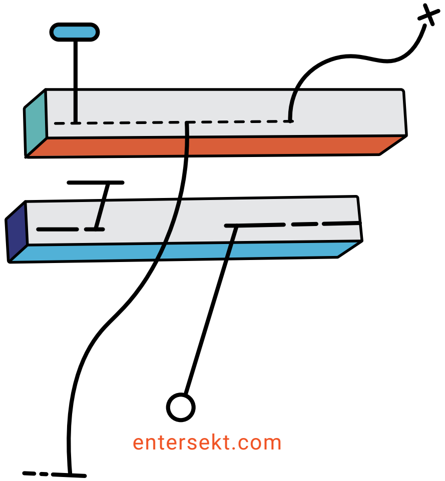
To meet the SCA deadline, several key initiatives have been delayed. These include wide support for the trusted beneficiary and secure corporate payments exemptions. The travel and entertainment sectors continue to face significant challenges stemming from the involvement of various intermediaries and indirect agents. The card networks have proposed short-term fixes but long-term solutions must still be developed. There remain several edge use cases, such as online gaming purchases, where enhancements to the EMV 3-D Secure specification are required.

EMV 3-D Secure allows 10 times as many data elements to be included with each payment to allow the issuer to make improved risk-based decisions. However, only the bare minimum is currently being sent, which hampers banks’ efforts to square security with usability.

Dynamic linking is a further challenge. PSD2 requires a unique authentication code per transaction with both the amount to be paid and the recipient made clear to the payer at authentication. The current low levels of merchant name matching and the European Banking Authority’s ruling that tolerances will not be permitted between authorized and authenticated amounts are causing a lot of headaches.[19]

> An estimated 12% of EMV 3-D Secure transactions fail to go through due to a combination of declines, abandonments, and technical errors.

At the time of writing, the authentication challenge results for 3-D Secure 2.1 are, quite worryingly, below those of 3-D Secure 1. An estimated 12% of EMV 3-D Secure transactions fail to go through due to a combination of declines, abandonments, and technical errors.



[19] All merchants must be identified at authentication with a unique name that is registered with the relevant payments networks.

The main problems we are seeing are:

- The wrong directory server transaction IDs sent by acquirers,
- The inclusion of special characters in the cardholder name field,
- Low authentication rates via mobile app channels, and
- Incorrect merchant registrations.

Many hands, light work

Financial services organizations and technology providers must collaborate more in order to enable seamless systems integration, overcome teething pains, and deliver a great user experience.

The UK Finance SCA PMO team, to which I belong, has done a great job coordinating the adoption of SCA, with all stakeholders working together to resolve issues and ensure compliance by the enforcement date.[20] The Netherlands offers another excellent example of a centrally managed SCA program in the form of the Dutch Payments Association.

It goes without saying that an actively engaged national competent authority is also vital to success.

Answering the identity question

Implementing SCA has made clear the shortcomings of not having effective national and regional ID schemes, whether public, private, or a combination of both. Countries like the Nordics, with well-established eID programs were far better prepared to avoid confusion or friction with the expansion of SCA.

As it stands, the mishmash of different approaches to eID has limited cross-border interoperability, which the European Commission fears could retard innovation in payments. It has committed to revising the eIDAS program and extending is application beyond trusted access to public services:

> “With a view to facilitating cross-border and domestic interoperability, the Commission will explore, in close cooperation with the EBA, ways to promote the use of electronic identity and solutions based on trust services, building on the further enhancement of eIDAS, to support the fulfilment of Strong Customer Authentication requirements under PSD2 for account login and initiation of payment transactions.”[21]

Brexit has added further complexity, as the United Kingdom is no longer part of the eIDAS program.

[20] UK Finance is the voice of the UK banking industry. Its SCA program helps plan the rollout and communicate necessary information to all parties, including consumers.

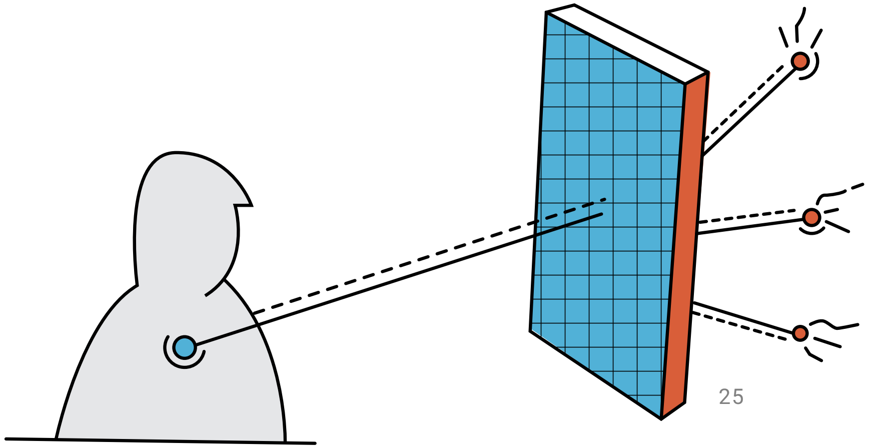
[21] “A Retail Payments Strategy for the EU” (24 September 2020); European Commission

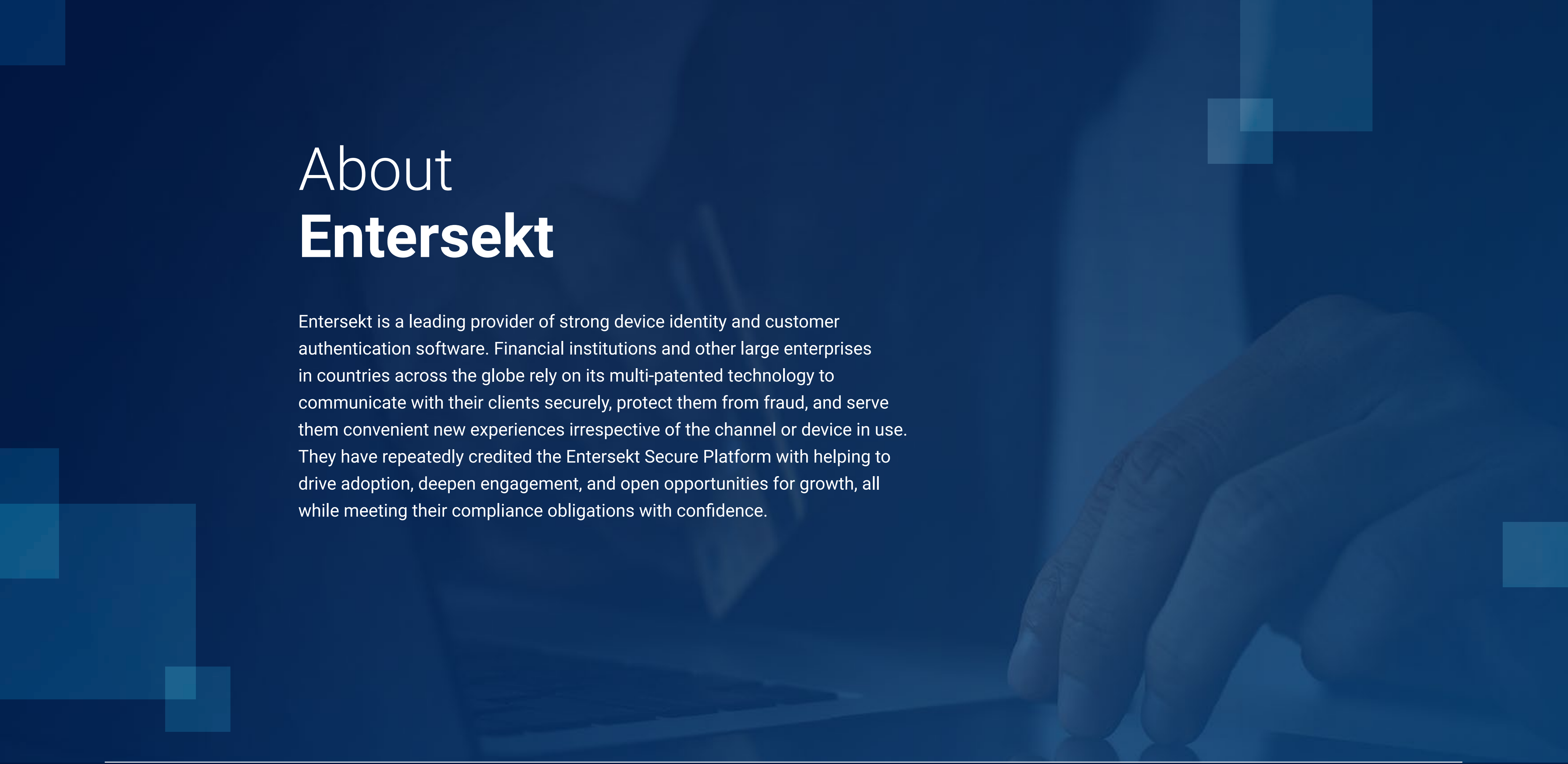
Further afield and further down the line

As the worldwide growth in popularity of the term itself indicates, SCA is attracting interest outside of Europe and its adoption in other jurisdictions can be expected soon. The EMV 3-D Secure technology also has global applicability and the card networks have already set mandates for issuers and acquirers in parts of the world where 3-D Secure was not previously used.

A lot was achieved in Europe last year, but there is much else to do. Further layers of fraud prevention and authentication will need to be added in the years ahead to help European businesses stay competitive, protect users, and win the war on fraud.

Discussions are starting in preparation for PSD3, in recognition of the ever-changing technological and commercial reality of the European banking and payments industries. And if some other regions' variations on the theme of open banking are a clue to what comes next, many more industries may find themselves looking at SCA with great interest in future.





About Entersekt

Entersekt is a leading provider of strong device identity and customer authentication software. Financial institutions and other large enterprises in countries across the globe rely on its multi-patented technology to communicate with their clients securely, protect them from fraud, and serve them convenient new experiences irrespective of the channel or device in use. They have repeatedly credited the Entersekt Secure Platform with helping to drive adoption, deepen engagement, and open opportunities for growth, all while meeting their compliance obligations with confidence.

Entersekt

For more information about Entersekt please visit our website or email us on info@entersekt.com

/Entersekt @Entersekt /Entersekt