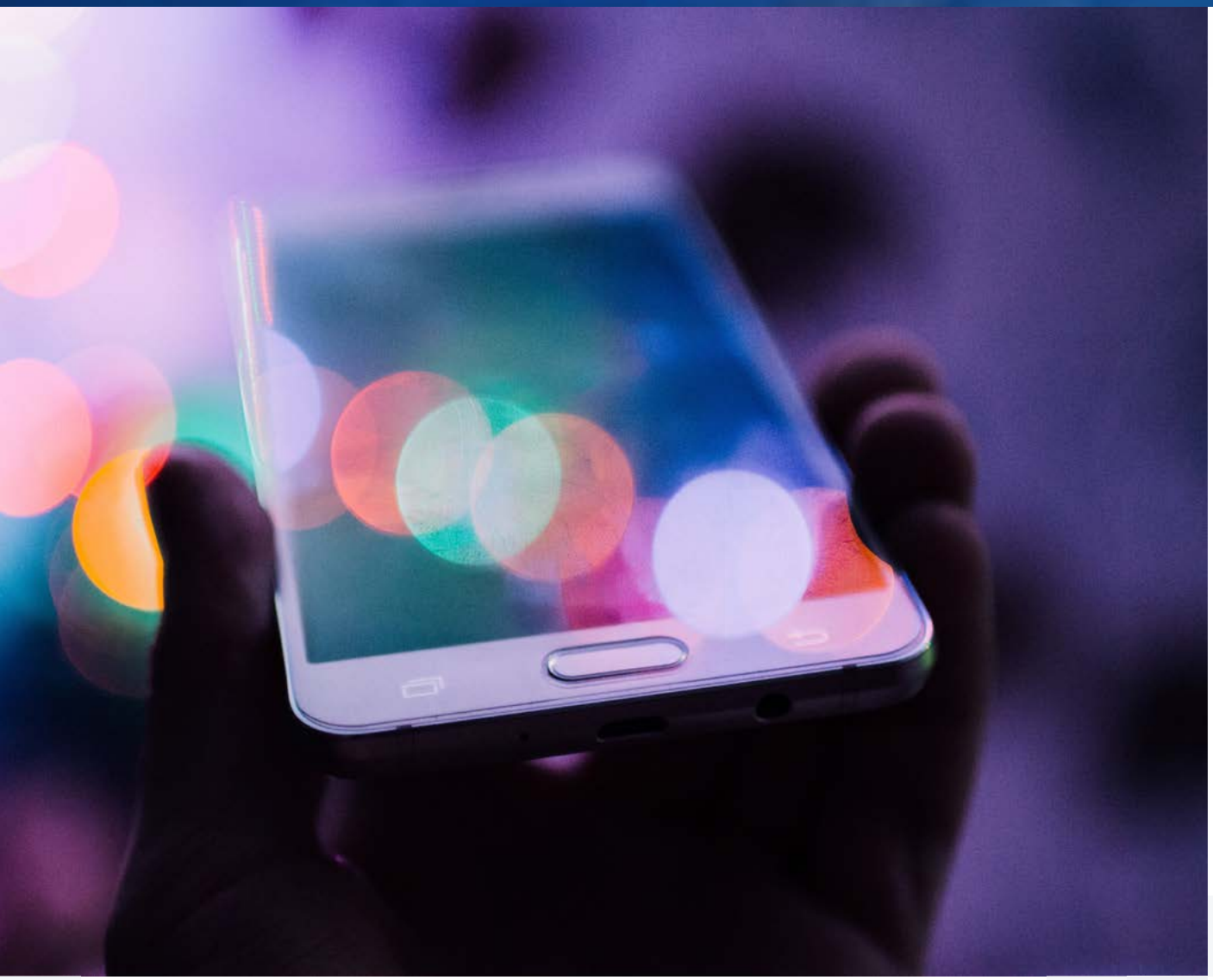
Entersekt

WHITE PAPER

PSD2: Turning a compliance challenge into business success

Can you transform a set of mandatory security standards into a competitive advantage? With the right partners, you can.



Approaching PSD2 **compliancy with vision.**

The European Union's revised Directive on Payment Services (PSD2) is more than a complex compliance project; it will usher in years of dynamic market change. Entersekt's patented security product Transakt provides a clear path to PSD2-compliant strong customer authentication, but it delivers a lot else too.

In packaging our PSD2 offering, Entersekt has aimed at more than mere compliance. Our customers face a dual challenge, to be met in record time. Firstly, they must address the new requirements comprehensively and manage additional security risks and liabilities imposed by them. Secondly, they have to prepare for an entirely new business dynamic in a way that secures their business against disruption.

In packaging our PSD2 offering, Entersekt has aimed at more than mere compliance. Our customers face a dual challenge, to be met in record time. Firstly, they must address the new requirements comprehensively and manage additional security risks and liabilities imposed by them. Secondly, they have to prepare for an entirely new business dynamic in a way that secures their business against disruption.

Under PSD2, financial services providers operating in SEPA countries must allow scores of third parties access to their customers' accounts if the latter have consented to it. Challenger banks, retailers, social media networks, telecommunications companies, and fintechs are lining up either to enter the market or expand their participation in it.

We hope to position our customers advantageously in the competitive race for market share in what is bound to become a highly fluid market for consumer financial goods and services. Audit proof, yes, but future proof too.

OUR PATH TO SUCCESS UNDER PSD2 CONSISTS OF THE FOLLOWING THREE STEPS:

STEP ONE
Meet immediate compliance objectives

STEP TWO
Provide a winning user experience

STEP THREE
Capitalize on the opportunity

The path to PSD2 success

STEP ONE

Meet immediate compliance objectives.

Invest in a proven, scalable, interoperable, and well-documented strong authentication solution that eases auditing and reporting to regulatory authorities.

As mandated under PSD2, the European Banking Authority's regulatory technical standards (RTS) on strong customer authentication and common and secure communication defines the enhanced security and authentication requirements that all relevant parties must use.[1]

Many practical questions remain, but independent analysts like the Payments Advisory Group have confirmed that Entersekt's patented solution meets all relevant articles in the RTS. [2] Our multi-factor, out-of-band authentication and app security product Transakt is engineered specifically for the heavily regulated financial sector and adheres to all major digital banking and payment security mandates globally. These include guidance from the European Banking Authority (EBA), German Federal Financial Supervisory Authority (BaFin), US FFIEC, and Monetary Authority of Singapore. Transakt is a FIDO® Certified U2F (universal second factor) authenticator. [3]

ENTERSEKT'S RTS SCORECARD

Download Entersekt's quick reference guide to making light work of the EBA's regulatory technical standards on strong customer authentication.

THE BASIC REQUIREMENTS EXPLAINED

What follows is a summary of the basic requirements set out in the RTS, together with Entersekt's approach to meeting them.

Strong customer authentication

Except in defined circumstances, strong customer authentication (SCA) is obligatory under PSD2 when a payer or proxy accesses payment accounts online, initiates an electronic payment transaction, or carries out any action through a remote channel that may imply a risk of fraud or other abuse.

An SCA procedure must use at least two of the following factors:

- **Knowledge** – something only the user knows (e.g. password, PIN, or identification number)
- **Ownership** – something the user possesses (e.g. token, smart card, mobile phone)
- **Inherence** – something the user is (e.g. a computer-readable biometric characteristic)

Entersekt's solution:
Transakt uses digital certificates to uniquely identify each registered mobile phone or tablet, transforming it into a trusted factor of possession.

These certificate are also used to generate authentication codes for every individual operation and to digitally sign them. In this way, the solution guarantees the authenticity of any digital transaction – that it was initiated and authenticated by the customer – and its integrity – that it has not been intercepted and modified by a third party in a man-in-the-middle or similar attack.

1 While PISPs and AISPs must ensure that strong customer authentication is applied appropriately, the cost of designing, implementing, and auditing the effectiveness of the authentication procedure falls on banks.

2 *Entersekt authentication under PSD2;* Payments Advisory Group

3 "FIDO® Certified Products"; FIDO Alliance

Independence of SCA elements

The transmission and use of authentication factors must ensure that they are independent of one other, so that a breach of one will not compromise the other. The channel, device or mobile app through which the authentication code is generated and received must be independent from the channel, device, or mobile app used for initiating the transaction.

Entersekt's solution:
Transakt's self-contained, NIST-compliant cryptographic stack and communications layer enables an isolated, end-to-end encrypted communications channel between the service provider and its customer's Transakt-secured mobile app. No third party, including Entersekt, can access these communications. All cryptographic material is securely stored, ensuring that neither the user nor the application developer can access it. Knowledge or inherence factors like PINs or biometrics are similarly protected.
See page 6 for detail on separation of elements on mobile.

Dynamic linking

The transmission and use of authentication factors must ensure that they are independent of one other, so that a breach of one will not compromise the other. The channel, device or mobile app through which the authentication code is generated and received must be independent from the channel, device, or mobile app used for initiating the transaction.

Entersekt's solution:
Authentication prompts are delivered to the user over the out-of-band channel that Transakt enables. Only the service provider and user know the nature of the encrypted request, which includes all the details required in the RTS.

Associate the user with their credentials, devices, and software

Authentication solutions must have the ability to securely associate the customer with their personalized security credentials, their authentication device(s), and any software that they use in the authentication process.

Entersekt's solution:
Once a Transakt-secured app is installed on a mobile device, it generates a pseudonymous digital certificate, uniquely identifying it. This certificate is only linked to the customer by the service provider at registration, so only they are party to the relationship between device and customer. If the device is stolen, lost, or replaced, the provider simply unlinks the certificate from the user, rendering the app unusable

Monitor access to user accounts

Authentication solutions must include monitoring and real-time risk assessment in order to protect users from unauthorized operations resulting from lost or stolen security credentials. The system should flag suspicious activity, including abnormal spending, atypical device or software usage, device- or software-based vulnerabilities, and malware infection.

Entersekt's solution:
Transakt's layered mobile and server-side detection and prevention procedures mean it is invulnerable to malware, SIM-swap fraud, and brute force attacks. It serves backend risk engines with device and application data, including device type, operating system version, and geographic location. Includes also app tamper awareness and advanced detection of rooting, jailbreaking, or similar mobile operating system security bypass hacks.

Is separation of **SCA elements possible on mobile?**

The RTS states that a transaction and corresponding authentication can be conducted using the same device if all authentication factors are adequately separated on it. This has proved controversial during consultation with industry stakeholders. What seems at first a perfect encapsulation of a basic principle of SCA – that the breach of one factor of authentication should not compromise any other – very often presents problems when applied to mobile.

Excerpt: Regulatory Technical Standards [4]

Chapter 2:

Security Measures for the Application of Strong Customer Authentication

Article 9: Independence of the elements

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.
2. Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.
3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:
    (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;
    (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;
    (c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

Commenting on the draft RTS, Klarna, a prominent Stockholm-based payments provider, raised widely shared concerns about requirements in Article 9 as it was then phrased:

> With regards to the independence of the authentication requirements we do find it problematic that data delivered to a device has the requirement for independence in the SCA elements as they thereby mutually exclude each other. In the example given the mobile device (the possession element) makes the code (the knowledge element) sent to the mobile device insufficient. [5]

Indeed, Article 9 appears to negate the use of SMS one-time passwords (OTPs) [6]. OTPs are delivered to mobile devices over open mobile networks, where they can be intercepted and altered and are largely unprotected on the device. Worse, OTPs are entered into the same potentially compromised mobile browsers or apps through which transactions are initiated, failing the RTS's requirements for the separation of elements.

4 "Regulatory technical standards on strong customer authentication and secure communication under PSD2"; EBA

5 "Discussion on RTS on strong customer authentication and secure communication under PSD2"; Klarna AB

6 This is not the only aspect of the RTS that calls into question the utility of SMS OTPs. Another is that they are shared secrets, to which the bank and mobile carrier have access in addition to the user.

Multinational consulting firm Deloitte stated the problem in broader terms:

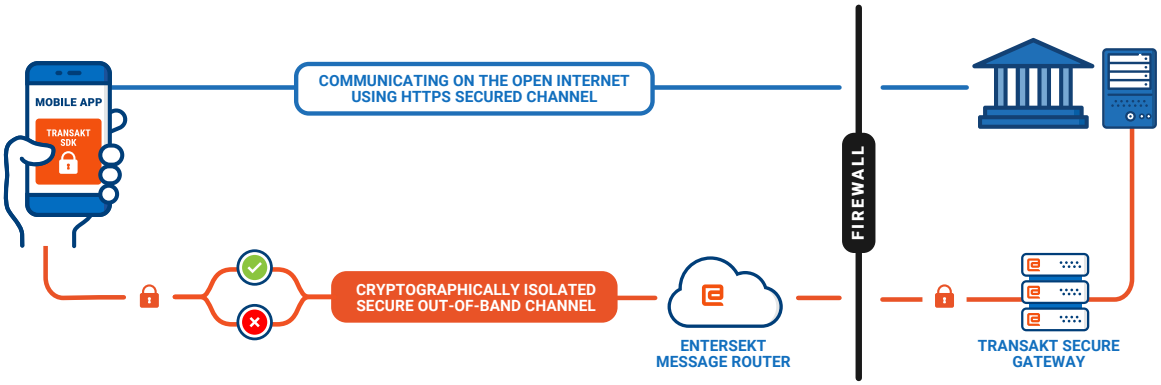
Importantly, the RTS requires PSPs to ensure the independence of all the elements used in the SCA procedure and the channel, device or mobile app through which the authentication code is generated and received to be "independent or segregated" from the channel, device or mobile app used for initiating the electronic payment transaction.

> This will pose challenges both technically and commercially. Technically, PSPs will need to ensure two different applications/channels are used to separately initiate payments and generate authentication elements (for example by requiring users to install the relevant bank "app" on their phone or carry a token generating key). Commercially the challenge will be to do so with as little inconvenience to the user as possible, as cheaply as possible, but better than competitors. [7]

This set of challenges is met by Transakt on all counts, whether integrated into a mobile payments or banking app.

Transakt enables PSD2-compliant transacting and authentication on one mobile app.

Transakt's self-contained, NIST-compliant cryptographic stack and communications layer enables an isolated, end-to-end encrypted communications channel between a mobile device and the service provider's mobile app server. This channel avoids the open Internet and unsecured mobile networks for authentication purposes. No third party, including Entersekt, can access these communications.



In the diagram above, we show the distinct channels Transakt enables between the mobile phone and service provider. The blue channel at the top is used to initiate a transaction; the orange channel below it, to authenticate the transaction. These channels and the means by which Transakt securely stores related cryptographic key material together enable transactions to be initiated and authenticated completely out of band using the same mobile app.

7 "PSD2 RTS on authentication and communication"; Stephen Ley, Steven Bailey, Valeria Gallo; Deloitte LLP

STEP TWO

Provide a **winning user experience.**

Empower your customers to transact anywhere, anytime, enhancing your relationship with each new interaction.

Bureaucrats regulate, businesses innovate, but it is ultimately consumers who determine which self-service technologies prevail. We know from decades of progress in digital service provision that people invariably opt for pared down, intuitive experiences that save time and avoid uncertainty. Winning solutions keep users informed, engaged, and in no doubt of what to expect next. Every interaction is designed to foster a sense of control.

With PSD2, consumers can expect a flood of new authentication prompts from a wide range of sources, both legitimate and fraudulent. That they will take a more active role in securing their money and personal data through SCA is no longer a matter for debate. They will. The real question is how financial institutions, payment providers, and data aggregators can make the process easier for them.

Many organizations have warned that PSD2's SCA requirements will slow channel adoption and damage the payments ecosystem. Visa reported that 61 percent of consumers it surveyed would abandon online purchases if additional steps were introduced at checkout.[8] Ecommerce Europe, a trade body, said "mandating SCA as identified by the EBA [...] is likely to slow investments in innovation, prevent competition and ultimately offer worse online payment fraud protection to consumers." [9] Mastercard worried that "an intended fraud prevention technique, if not implemented correctly, could rapidly become a business prevention technique." [10]

It is entirely possible to boost channel adoption with a low-friction, predictable means of approving payments and third-party access to accounts in real time. Entersekt has seen how well-engineered authentication can boost trust in brands and channels, improve customer loyalty, lower costs, and not only increase revenue but its sources.

What can **3-D Secure teach us?**

European consumers are already familiar with SCA, the application of which became mandatory for many sensitive digital transactions after the passing into law by SEPA states of the EBA's "Guidelines on the security of internet payments" of 2014.[11] The majority of online shoppers in the Benelux countries, Italy, Switzerland, and the United Kingdom now secure their card-not-present purchases using 3-D Secure, which was widely adopted as a result of the guidelines.

8 "Europe's online shoppers faced with inconvenience and disruption"; Peter Bayley; Visa Europe

9 *Recommendations for improving European online payments regulation;* Clever Advice;

10 "Ensuring a good customer outcome from Strong Customer Authentication"; Jason Lane; Mastercard

11 "Guidelines on the security of internet payments"; European Banking Authority

Merchants continue to resist 3-D Secure bitterly in more lightly regulated jurisdictions. The concern is that it introduces unnecessary friction during the critical last stage of the checkout process, increasing shopping cart abandonment. [12]Even in Europe, where it is by now a fact of life, consumers find most implementations frustratingly time consuming and cumbersome.

3-D Secure, which provided a mass market mechanism for SCA of the kind PSD2 requires, offers lessons on squaring usability with security.

When shoppers forget their 3-D Secure static password or find the process of entering an OTP too clumsy, they abandon their carts. Those less familiar with the process are often confused or apprehensive about the sudden redirect to an unsophisticated authentication screen with strange new logos. A pause in the transaction provides room for second thoughts.

These are issues for anyone shopping on a computer, but the frustration people experience securing payments at the desktop is multiplied when attempting the same actions on a mobile device's smaller screen and touchpad. That's a problem for service providers that have not optimized authentication for the mobile phone, and one that will grow more serious under PSD2. Most digital exchanges that European consumers will have with financial institutions and third parties after PSD2 will be conducted on the mobile phone.

Mobile-optimized SCA.

The ideal SCA solution exploits mobile's popularity and convenience to deliver an intuitive, one-touch user experience while meeting the strictest security standards anywhere in the world. Entersekt pioneered phone-as-as-token, push-based authentication. Our card-not-present authentication solution, fully accredited by Visa, Mastercard, and American Express, simplified the 3-D Secure authentication process significantly, enabling a simple one-touch response with no requirement to remember personal credentials and passwords or retype OTPs.

Our approach to RTS-compliant SCA is similarly transformative. We push authentication requests bearing all necessary details to consumers' mobile phones or tablets in real time. All they have to do is touch "Accept" or "Reject" to authorize or stop transaction or access requests immediately.

12 3-D Secure's negative impact on conversion rates has been demonstrated in many countries, but the effect is not universal. In a 2014 study, "Optimizing payments to increase revenues", Adyen, a payment systems provider, found a conversion *uplift* in a third of the countries it assessed, including the United Kingdom, where the average checkout rate climbed nearly three percent. It ascribed the rise to superior implementations, greater consumer awareness, and an increased sense of security.

CASE STUDY

SCA usability driving channel growth

This European card issuer began rolling out Entersekt's mobile-based payments enablement solution in 2016. Its primary goal was to improve the 3-D Secure user experience.

Within five months, it almost eliminated card-not-present fraud, but it is arguably the solution's beneficial effect on channel adoption that made the biggest impact:

- The number of digital payments processed climbed 29 percent
- The total transaction value increased by over 15 percent

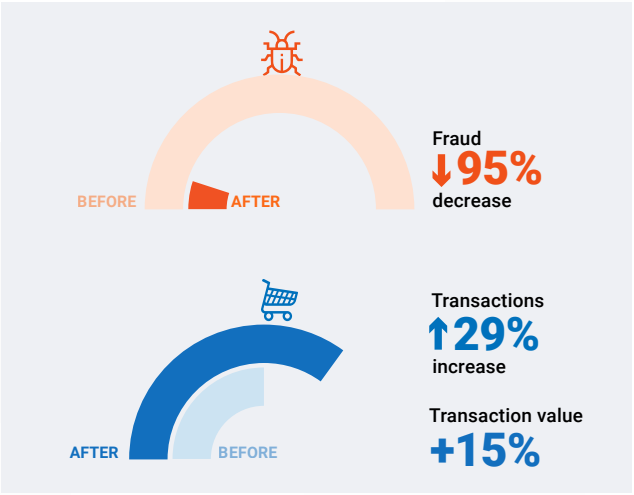


Illustration source: Adaptation of customer's own chart

When you can uniquely identify the customer-held mobile device with a digital certificate and can ensure that only the owner can access sensitive communications to it, you have the most reliable authentication factor – possession – covered, and with zero effort needed from your customer. The second factor can be a biometric or simple PIN capture. This combination achieves not only the strong security mandated by the RTS but a low-friction user experience primed for a mobile-first world.

What, after all, could be simpler or more direct – touching a button in a simple user interface on a secured device you carry with you everywhere?

Real-time push	One-touch action	Seamless transaction signing	Mobile optimized	Consistent for all channels
				

The Transakt user experience

STEP THREE

Capitalize on the opportunity.

Act now to become the trusted keeper of consumers' digital assets and change your strategic position relative to third-party payment service providers.

Couched in terms of consumer choice and protection, PSD2 is a systemic response to accelerating technological innovation, the enabling nature of the Internet and mobile phone in particular. It represents one more stage in the continuing evolution of payments – and is not the last one any of us will experience either.

Once it comes into force, work will begin on annual updates and its eventual replacement by PSD3 in five years' time. The RTS will be superceded by stricter regulations – many of which will be inspired by trends in other parts of the world or will aim to address the varying experiences of SEPA member states as they grappled with the practicalities of PSD2, GDPR, and more. [13]

Entersekt understands how to navigate this changing landscape. Pioneers in user-friendly phone-as-a-token authentication, our products are mature and widely deployed. We have deep experience of implementations in Europe, which is complemented by our global outlook on emerging trends, both in regulation and digital fraud.

Successful **adaptation requires flexibility.**

Flexibility is an essential feature of any PSD2-compliant authentication solution. Banks and other service providers should invest in technology that will adjust to future revisions of the RTS: new security controls applied to a wider set of use cases.

Transakt covers most authentication use cases. It provides a converged authentication experience of online banking, mobile banking, e-commerce, call center interactions, staff access, and more. It covers the entire user authentication lifecycle, including enrollment, maintenance, account recovery, off-boarding, and the introduction of new service channels.

Some service providers may need to offer additional authentication options to their customers. To save costs and speed time to market, they should consider solutions built on widely adopted industry standards like those of the FIDO Alliance, which has developed an open authentication protocol aimed at supplanting reliance on passwords. As a FIDO® Certified U2F authenticator, Transakt interoperates with over 350 other FIDO products. Once an enterprise implements one FIDO-compliant solution, it can roll others out without additional development. [14]

13 It is frequently suggested that PSD2 and the European Union's General Data Protection Regulation (GDPR) pull in opposite directions, the former mandating open access to consumer data, the latter seeking to protect it to a greater extent than ever before. In actual fact, these two sets of regulation, likely to be adopted into law within months of each other, dovetail well, at least in their aims. Both seek to give consumers control of their data, with GDPR providing the legal framework for the concept of informed customer consent. The practical and technical interplay of PSD2 and GDPR is, on the other hand, unresolved.

14 *FIDO & PSD2:* FIDO Alliance

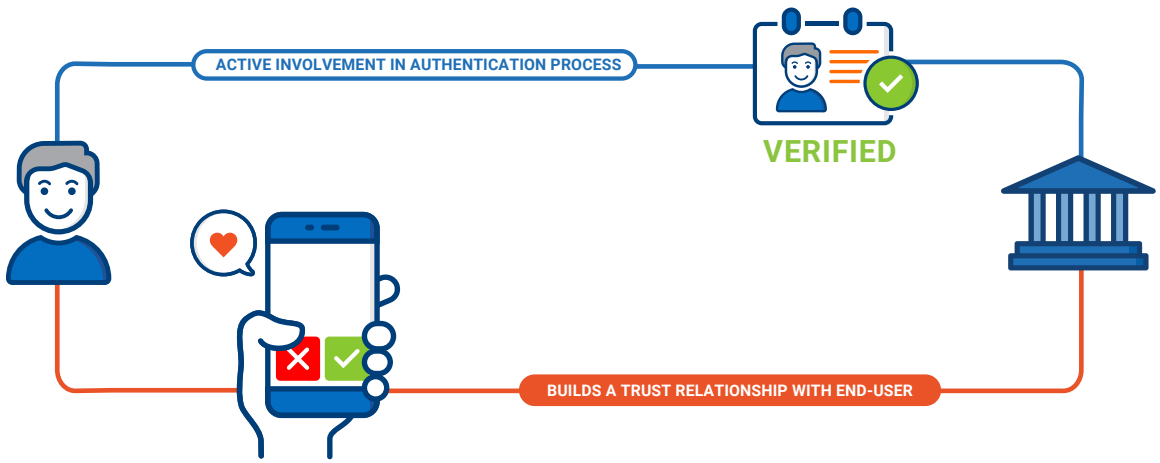
The future is **built on trust.**

"People need banking, not banks," say many of the fintech companies. They have a point, but what people need more than banking is trust. With so many new payment platforms and financial service providers entering the consumer market, where do people go to secure their identity, personal data, and accounts with confidence?

Banks have long maintained this function, which gives them an enormous advantage over non-traditional market entrants post-PSD2, but their lead is slipping. A 2016 survey by PwC's strategy consultancy Strategy& found that the majority of Europeans (88 percent) already used third-party digital payment services, and that they rated their security extremely highly. Eighty-two percent were certain that PayPal, Amazon, and other alternative payment providers transferred money as safely as their banks did. [15] While banks held a large lead in the provision of banking apps, consumers were less convinced about their security. Only 32 percent used banking apps, with 34 percent of those who did not use them expressing unmet security concerns.

Figures like these neatly encapsulate the pitfalls and opportunities of open banking, especially for incumbents. Banks could lose their grasp on the primary customer relationship to third-party competitors and become so-called "dumb pipes".

On the other hand, if they respond to PSD2 with ambition and long-term vision, they could become providers of attested information services and a central cogs in the value chain of payment initiation and account information delivery.



Once established as the trusted keeper of their customers' digital assets, banks could become disrupting forces themselves. They may expand value-added services beyond their traditional remit and engage their customers several times daily, in all sorts of new ways, but with a secured mobile app at the core of the relationship.

15 *Catalyst or threat: The strategic implications of PSD2 for Europe's banks;* Jörg Sandrock, Alexandra Firnges; Strategy&

Transakt can deliver on that vision. So much more than a means of checking compliance boxes, it provides a security platform on which to build all manner of innovative new products, with no concerns about fraud.

CASE STUDY

Mobile enablement powers Capitec Bank's growth

South African retail bank Capitec has long held mobile at the center of its ambitious growth strategy. It wanted to enable all services on the channel, aiming to boost customer convenience and drive down costs with a highly secure and user-friendly offering. It turned to Entersekt in early 2012 after larger authentication vendors proved too rigid and uninspiring when it came to mobile innovation.

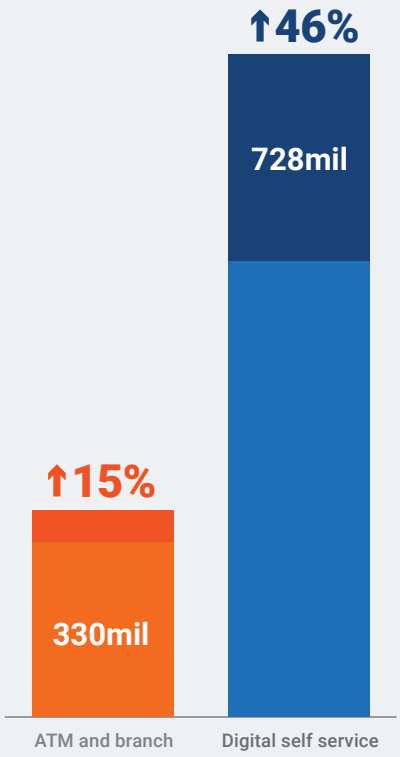
Capitec credits Entersekt's technology for increasing customer confidence in the mobile channel, contributing to a significant increase in the number and value of digital transactions.

The results are impressive:

- Market share grew from 2 percent in 2007 to 25 percent in 2017
- Client base doubled since 2012 to 9.3 million
- Remote banking transactions increased by 46 percent ear-on-year to early 2017
- No fraud on digital channels
- Capitec named Best Retail Bank in the world by Lafferty Group for the last two years, beating 99 other banks in 32 countries

Transaction growth

Year-on-year to February 2017



Source: Capitec presentation at Gartner Symposium/ITxpo 2017, Barcelona, Spain

Contact us at **info@entersekt.com** or **entersekt.com** to explore how we can help you achieve success in this area – and others!

/Entersekt @Entersekt /Entersekt