INNOVATE WITH SECURITY

How PSD2 and Open Banking require banks to change their view on cyber security and redesign their security architecture to protect against fraud

accenture

TABLE OF CONTENTS

INTRODUCTION

The European Union's revised Payment Services Directive (PSD2) will open the way to a new era for payments in Europe. PSD2's core objectives include enhancing consumer protection against fraud and liability accountability across the payments ecosystem. Strong Customer Authentication (SCA)—along with secure communication—is key to achieving this goal.

By allowing customers' accounts to be accessed via application programming interfaces (APIs) or customer-facing interfaces, PSD2 enables entirely new types of payment service—namely third-party payment initiation provided by Payment Initiation Service Providers (PISPs), third-party account access provided by Account Information Service Providers (AISPs) and confirmation of funds provided by Card-issuing Payment Service Providers (CIPSPs).

On March 13, 2018, the final Regulatory Technical Standards (RTS) were published in the Official Journal of the European Union. Originally drafted by the European Banking Authority (EBA), it is set of minimum requirements with which all Payment Services Providers (PSPs)—including banks, acting as Account Servicing Payment Service Providers (ASPSPs)—will have to comply. Some notable aspects of the final RTS are summarized on page 4.

> "The security of electronic payments is fundamental in order to ensure the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud."
>
> — Payment Services Directive (PSD2), recital 95

LEGAL NOTICE

Accenture is a global provider of professional information technology solutions and services. Views and opinions expressed in this document are based on Accenture's knowledge and understanding of its area of business, markets and technology. The Information provided in this document does not purport to reproduce the exact requirements of the Payment Services Directive (PSD2), draft Regulatory Technical Standards (RTS), General Data Protection Regulation (GDPR) or any other legal or regulatory material and may not be read to constitute legal advice or legal interpretation of such requirements. The reader must rely on their legal and financial representatives to interpret the below information as well as the said requirements, rules of access to the regulated payment systems and underlying operational functions, as well as the precise manner of such access.

The RTS on strong customer authentication and secure communication is key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.

FROM THE FINAL RTS ON STRONG CUSTOMER AUTHENTICATION

- Banks must open their payments and core banking systems to third-party payment providers (TPPs) by providing interfaces (either dedicated state-of-the-art APIs, or a customer-facing interface for screen scraping).

- The APIs with the bank's underlying services (such as payment instruments and account information) must be granted to the TPPs under the same service level as they are granted to the bank's own services, such as online banking. The performance and availability requirements are currently defined by the API Evaluation Group of the ERPB.

- API standard needs to be based on recognized industry standard (available standard could be Berlin Group NextGenPSD2 or Open Banking UK).

- Authentication procedures will use two of three elements—knowledge (e.g., password), possession (e.g., multi-purpose device), inherence (e.g., behavioral biometrics).

- The channel, mobile application or device where the transaction information is displayed must be independent of the one used to initiate the payment.

- The authentication code generated needs to be specifically linked with the amount paid and the payment recipient. All information about the amount paid and the payment recipient must be passed on across all phases (generation, transmission and application) of the authentication, and must be shown to the payer.

- The RTS sets out exemptions from performing SCA and asking the user to enter authentication codes for every transaction. These exemptions for PISPs and AISPs will enhance convenience.

- A Mutual Authentication Mechanism between the TPP—be it a PISP, AISP, or CIPSP—and the ASPSP (bank): RTS proposes the use of Qualified Website Authentication Certificates (QWAC) and Qualified Electronics Seals (QSEAL) issued by Qualified Trust Service Providers (QTSPs) based on the eIDAS framework. Standards for these QTSP are being defined by ETSI to ensure the interoperability of all certifications.

- Bank-specific technical specification documents, developer portal, routines, tools and examples must be made available on the bank's website to be downloaded by anyone free of charge.

DEFINING STRONG CUSTOMER AUTHENTICATION

As the RTS specifies, PSD2's SCA is based on two or more of three elements that are independent of one another. Alongside this authentication, PSD2 requires PSPs to have in place security measures to protect the confidentiality and the integrity of the payment service user's (PSU's) personalised security credentials when the payer:

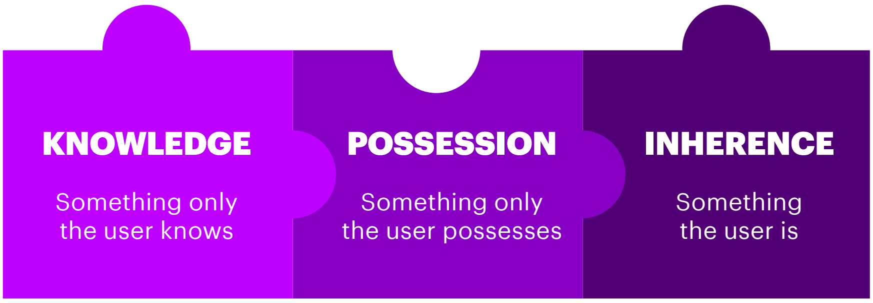
a) accesses its payment account online

b) initiates an electronic payment transaction

c) carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses.

With the initiation of electronic remote payments transactions, PSD2 again requires payment service providers to apply SCA, which must include elements that link the transaction dynamically to a specific amount and a specific payee.

Strong Customer Authentication means an authentication based on the use of two or more elements



KNOWLEDGE

Something only the user knows

POSSESSION

Something only the user possesses

INHERENCE

Something the user is

EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION

PSD2 allows for exemptions from having to apply SCA, based on the following criteria:

a) the level of risk involved in the service provided

b) the amount, specific payees and/or the recurrence of the transaction

c) the payments channel and use case used for the execution of the transaction

d) the duration of access to account information (up to 90 days without SCA)

PSD2 also introduces a liability shift, as providers who fail to authenticate a transaction appropriately will now be held liable for any resulting breaches. In cases where the payer's PSP does not require SCA, the payer will not be required to bear any financial losses unless the payer has acted fraudulently.

KEY QUESTION

Given the need for at least two out of three different elements to be used for customer authentication, have you decided what elements you will use, and how?

DIGITAL IDENTITY

CUSTOMER AUTHENTICATION

Even after publication of the final RTS, it remains unclear what the authentication technologies will ultimately look like. However, Accenture expects to see the adoption of a standardized, simple and user-driven authentication framework such as OAuth 2.0 and its extension OpenID Connect, which allows authentication and authorization without disclosing the user's credentials to TPPs.

In terms of practical implementation, it appears likely that most banks will decide to rely on the knowledge factor option such as a PIN, and then choose between possession and inherence as the second factor.

The RTS created some uncertainty regarding the second element, possession. The independence of channels plays a vital role in a multi-channel environment, especially in a mobile ecosystem of desktops, mobile devices and mobile applications. It is important that the authentication code is not transmitted through the same channel that the customer has used to initiate the authentication procedure.

Banks will focus on possession-based solutions using one device both for the initiation of the authentication procedure and the reception of the authentication code. Therefore, the technical separation of the different authentication elements within one device will play an important role, and should be considered by banks while reorganizing their authentication methods.

While a possession-focused solution would be—irrespective of the challenges—technologically strong, it may not provide the level of accuracy required. As a result, many banks are looking into inherence to address the second factor of authentication.

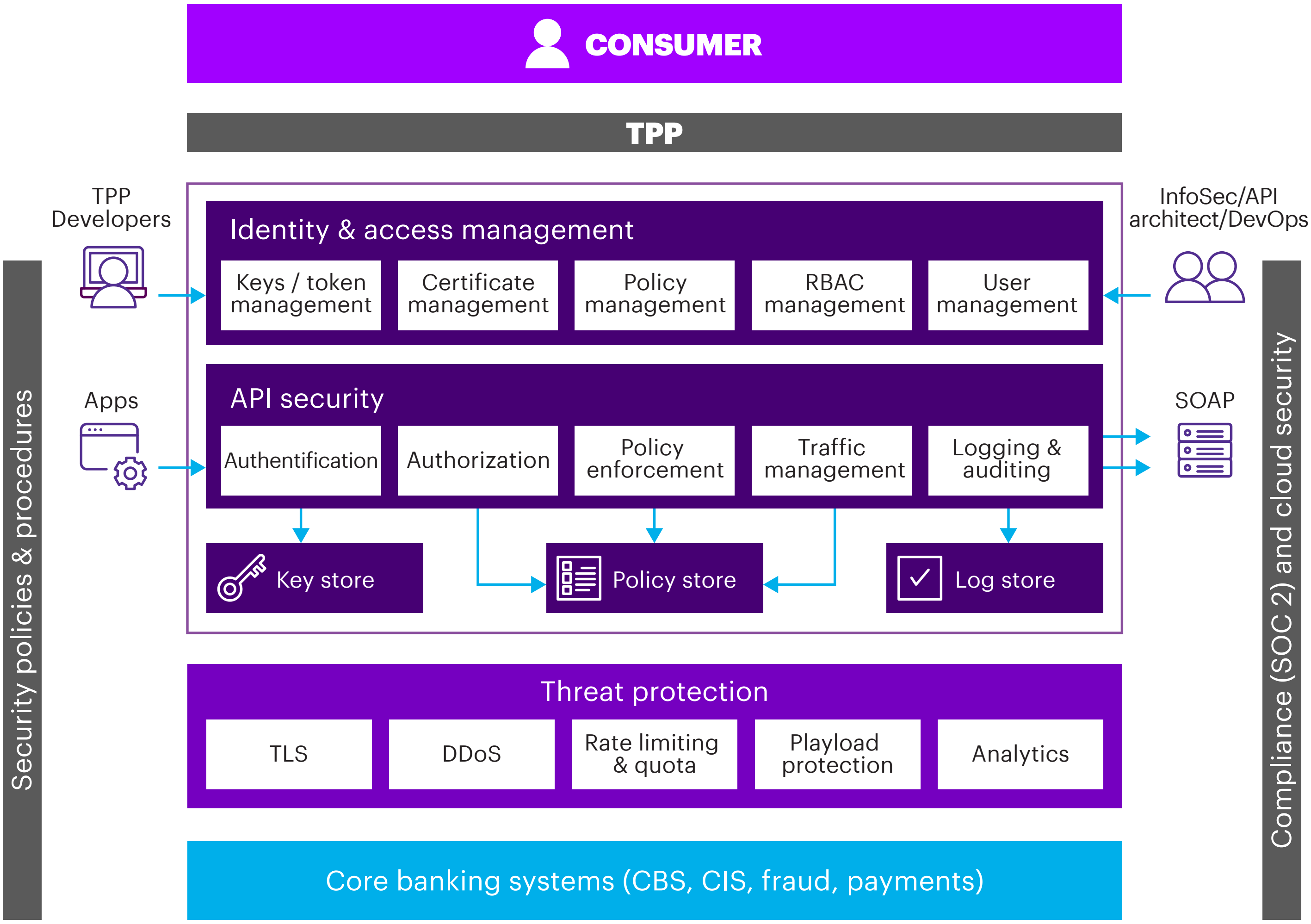
KEY QUESTION

Based on the available information in the latest RTS, OAuth 2.0/OpenID connect is likely to be the preferred authentication protocol. Even the latest API standards published by the Berlin Group or Open Banking UK propose OAuth 2.0. as a possible solution. The requirements on possession-based authentication methods have become stronger. Given this, is your organization ready for OAuth-based customer/TPP authentication and technically separated possession-based authentication methods?

CYBER SECURITY

The RTS allows "TPP-authenticated screen scraping" as an alternative and fallback solution to dedicated APIs. At the same time, it also paves the way to a state-of-the-art API-driven ecosystem. By providing their APIs to TPPs, banks open up a significantly greater attack surface to potential cyber adversaries, and can no longer hide critical applications behind perimeter firewalls.

However, banks that follow a sound architectural approach can mitigate these issues, by integrating security requirements with the fundamental business drivers and business cases. This helps to ensure that their security processes are adaptive and responsive to threats while also being tightly coupled to business impacts. Here is a high-level reference architecture for a bank's APIs:



API SECURITY AND MANAGEMENT

API security should be an integral part of API implementation—and achieving this requires a specific view of the API architecture. Historically, APIs have been considered as "trusted" B2B communication, meaning controls have not been enforced as strongly as in consumer-facing areas.

Instead, security controls similar to digital banking should to be applied to APIs, and a "do not trust" approach should be adopted to provide a stronger and resilient future for APIs. This security layer should address issues of:

- Access Control
- Threat Detection
- Confidentiality
- Integrity

Within this architecture, the design of APIs must take into account the need to protect against distributed denial of service (DDoS) attacks. Fortunately, this threat is also an opportunity. Since creating systems with open APIs represents a "greenfield" development for many organizations, it provides a one-off window of opportunity to do things right from start, by blocking attacks high up the stack and protecting the intelligence located on lower layers.

Authentication and Authorization

Authenticate licensed TPPs using the TPP certificate issued by a QTSP under PSD2 and check against revocation list. In addition to this, maintain a list of licensed TPPs gathered from the EBA Register

Content Based Attacks

Protect against different types of content-based attacks such as malformed XML threats, malformed JSON threats, and malicious script injection threats

Data Encryption

Use transport layer encryption such as TLS to secure the communication. Any sensitive message in the API needs to be protected using message/field level encryption

Identity Tracking

User info and/or TPP ID should be logged for Identity tracking using policies within the flow

Message Validation

Use Data Masking policies for hiding sensitive data when logged. A "validation before consumption" principle should be used to safeguard APIs

Traffic Management

Use traffic management policies to prevent infrastructure getting overwhelmed. Implement throttling and rate limiting on the number of requests allowed for a TPP in a given time period

ADAPTING TO THE GENERAL DATA PROTECTION REGULATION (GDPR)

With the introduction of EU's new General Data Protection Regulation (GDPR), the risk landscape will change significantly. This shift will include new requirements around accountability, documentation, privacy reviews and design, as well as the imposition of very high fines for non-compliance.

These changes are coming in at a time when many banks already face issues such as limited understanding of the data across their organizations, an increasing volume and magnitude of cyber-attacks, and public concerns over the privacy of personal data. These issues will be impacted and in some cases amplified by GDPR regulation and moves to harmonize data protection and privacy across all the EU and EEA along with the EU-US Privacy Shield.

Again, this wave of regulation—combined with the move to open up banking APIs under PSD2—presents a great one-off "greenfield" opportunity to design APIs that are built from the ground up to maximize privacy and security. So banks should take a number of principles into account when designing APIs. These include:

EMBED PRIVACY INTO DESIGN

Not as an add-on, but as an inherent part of any IT system.

BE PROACTIVE, NOT REACTIVE; PREVENTATIVE, NOT REMEDIAL

Aim to anticipate and prevent privacy-invasive events before they happen, not to handle them afterwards.

HAVE MAXIMUM PRIVACY AS THE DEFAULT SETTING

Protecting all kinds of personal data.

FULL FUNCTIONALITY: POSITIVE-SUM, NOT ZERO-SUM

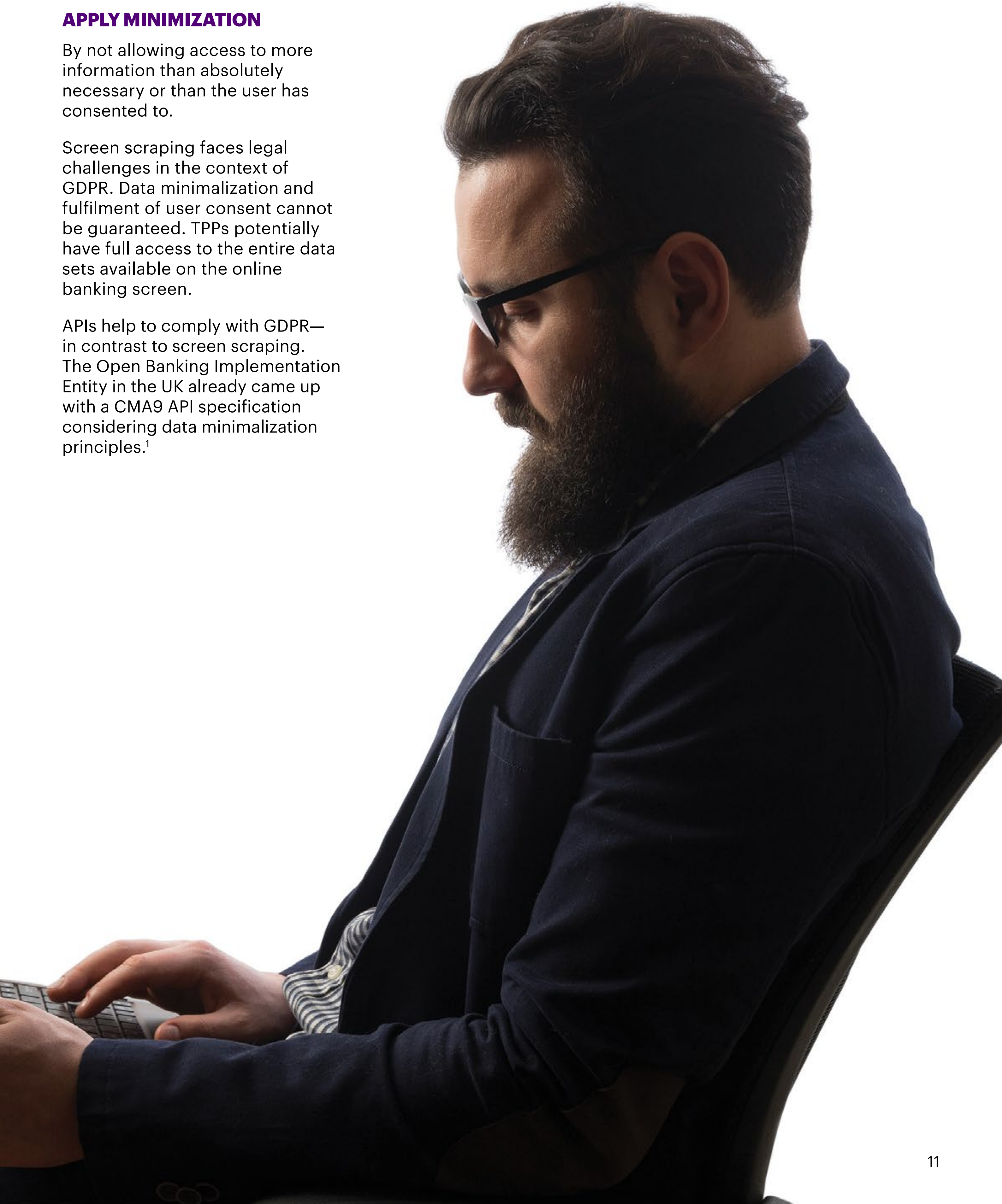
Avoid unnecessary trade-offs like privacy versus security.

APPLY MINIMIZATION

By not allowing access to more information than absolutely necessary or than the user has consented to.

Screen scraping faces legal challenges in the context of GDPR. Data minimalization and fulfilment of user consent cannot be guaranteed. TPPs potentially have full access to the entire data sets available on the online banking screen.

APIs help to comply with GDPR—in contrast to screen scraping. The Open Banking Implementation Entity in the UK already came up with a CMA9 API specification considering data minimalization principles.[1]



FRAUD AND FINANCIAL CRIME

As banks implement APIs and open their infrastructure to TPPs under PSD2, this could create a whole range of opportunities for fraudsters—at a time when banks have already lost significant amounts to fraud, and are engaged in an arms race to stay ahead of ever more sophisticated cyber-criminals.

With PSD2, the rules of the security game are changing fundamentally. Banks' current systems rely on customers interacting with them direct, meaning banks themselves possess all the information needed to establish whether a transaction is fraudulent. Under PSD2, many customers may no longer log on to their banks' digital banking websites at all, reducing the amount of relevant data available to the banks.

Against this background, providing a secure infrastructure to TPPs will be a major challenge for banks. To prevent fraud in real time, most banks use packaged software whose fraud scoring models are trained over a period of 18 to 24 months. So after PSD2 introduces new transactions through TPPs, it will take around two years for the banks to generate scores reflecting the transaction risk.

In the interim, banks' fraud analytics departments will need to perform proactive transaction monitoring and develop their own rules to prevent frauds. Under PSD2, banks can block third-party access to accounts if they have the evidence that the activity is unauthorized or fraudulent. This is a capability they may well need to exercise once PSD2 comes in.

KEY QUESTION

Does your enterprise suffer from fraud silos? Have you considered the impacts on fraud engines in the new environment where ecommerce transactions might come to digital channels for risk-scoring without any ecommerce history? Are you considering an integrated fraud layer?

OPTIONS FOR INHERENCE: BIOMETRIC AND BEHAVIOURAL PROFILING

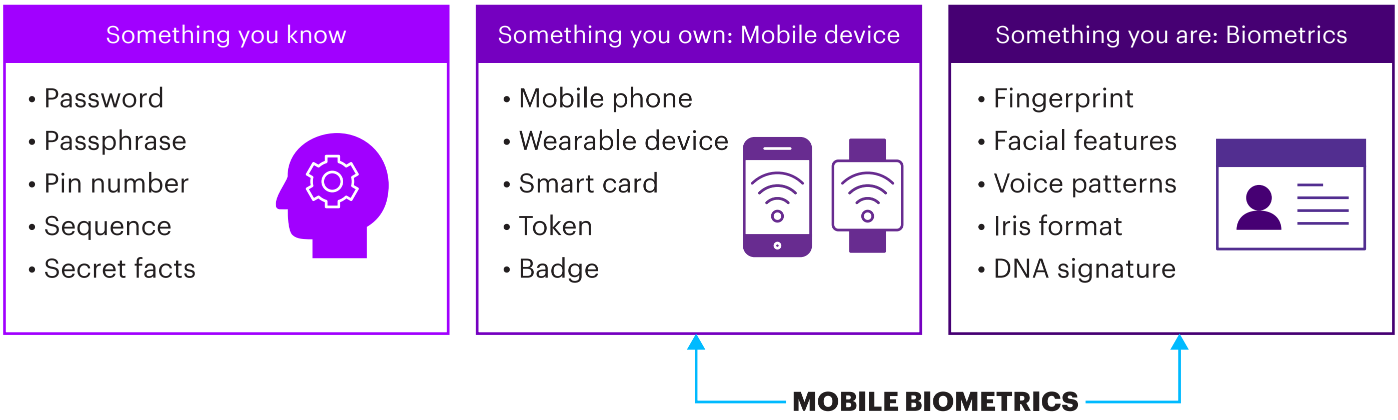
Using inherence as the second factor caters to both the security requirements and user experience priorities of PSPs. A form of inherence already in widespread use is biometric authentication, which is consumer-friendly, works in real-time, is easy to implement, and addresses the PSD2 requirement for more accurate validation. All of this makes identity fraud less likely, and explains why biometric technologies are moving into end-user mobile devices, usually combined with passwords.

Another important subset of inherence is behavioral profiling. By assessing the customer's location and behavior against their usual patterns, banks can gain a clearer view of the risks and the level of authentication required. And because behavioral profiling runs in the background, it is invisible to users and does not impinge on the customer journey.

Behavioral profiling is a comparatively new mechanism that is currently on the path to maturity. At this stage it would be better suited to being used as an augmentation to strengthen fraud controls rather than acting as the authentication mechanism itself.

KEY QUESTION

Does your organization have a pluggable and adaptive authentication capability to support new and upcoming innovation in authentication technologies and techniques?



Something you know

- Password
- Passphrase
- Pin number
- Sequence
- Secret facts

Something you own: Mobile device

- Mobile phone
- Wearable device
- Smart card
- Token
- Badge

Something you are: Biometrics

- Fingerprint
- Facial features
- Voice patterns
- Iris format
- DNA signature

MOBILE BIOMETRICS

CONCLUSION

As the PSD2 RTS needs to be implemented by September 14, 2019, it is imperative for all players in the evolving payments ecosystem—not least banks—to have a specific PSD2 security strategy. The good news is the greenfield opportunity that PSD2 brings to embed security up-front in the new systems and APIs, thus turning security into a business asset.

Achieving this requires a shift from a compliance-centered security mindset to an active cyber security stance. Doing so positions security as an enabler of the Future-Ready Bank where cyber security capabilities and behaviors make it as difficult as possible for hackers, keeping customer data and trust secure. To undertake this journey successfully, banks will need their security teams to adapt continually to keep pace with evolving business objectives. As the PSD2 era is here, now is the time to start.

NOTE

1. https://www.openbanking.org.uk/

AUTHORS

Hakan Eroglu
Senior Manager
European Open Banking Lead
hakan.eroglu@accenture.com

Andrew McFarlane
Senior Manager
Global Open Banking Lead
andrew.g.mcfarlane@accenture.com

CONTRIBUTOR

Dr. Martin Bentele
Managing Director
ASGR Payments Practice Lead
martin.bentele@accenture.com

ABOUT ACCENTURE PAYMENTS

Accenture Payments helps banks, payments providers and other players transform their payments systems and operations to grow and win in the digital economy. We offer unmatched capabilities, scale and experience of Accenture to address the end-to-end needs of payments stakeholders—from the boardroom and C-suite to the back office. Our services support every phase of the payments value chain, and can help reduce costs and improve value outcomes. Our more than 4,300 payments advisors and payments systems integration specialists bring together strategy, business function consulting, digital technology and delivery execution know-how to help keep our clients on the leading edge of payments. To learn more, visit www.accenture.com/payments.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

www.accenture.com/banking

Accenture Banking

@bankinginsights

Accenture Banking blog