accenture

Strategy | Consulting | Digital | Technology | Operations

Accenture Payment Services &
Accenture Technology Advisory

PSD2 & Open Banking

Security and Fraud Impacts on Banks

Are You Ready?

High performance. Delivered.

Table of Contents

Legal Notice


TOUCH TO UNLOCK

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 payment ecosystem. Strong customer authentication – along with secure communication – is key to achieving this goal.

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

In August 2016, the European Banking Authority (EBA) published a consultation paper with a first draft of the Regulatory Technical Standards (RTS), a 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 EBA's draft RTS are summarised below.

> "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*

From the EBA's draft RTS:

- Authentication procedures will use the three elements – knowledge, possession, inherence.
- "Dynamic linking" and channel independency: the channel, mobile application or device where the transaction information is displayed must be independent of the one used to initiate the payment
- Mutual Authentication Mechanism between TTP (PISP, AISP) and ASPSP (bank): the EBA proposes the use of Website Certificates issued by qualified Trust Service Providers (TSPs) based on the eIDAS framework. The EBA says there will be a qualified TSP designated under eIDAS not before October 2018.
- The RTS sets out exemptions from performing SCA and asking the user to enter Authentication Codes for every transaction. These exemptions for PISPs, AISPs and PSPs will enhance convenience for users.
- Security standards will be in compliance with ISO 27001.
- Banks must open up their payments and core banking systems to TPPs using ISO20022 or other industry standard.
- Bank-specific technical specification documents, routines, tools and examples must be made available on the bank's website to be downloaded by anyone free of charge.
- The APIs with the bank's underlying services (payment instruments, account information) must be granted to the TTPs under the same SLAs as granted to the bank's own services, such as online banking.

Defining strong customer authentication

As the RTS specifies, PSD2's "strong customer authentication" 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 payment transactions, PSD2 again requires payment service providers to apply strong customer authentication, which must include elements that dynamically link the transaction to a specific amount and a specific payee.

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

Exemptions from strong customer authentication

PSD2 allows for exemptions from having to apply strong customer authentication, based on the following criteria:

a) the level of risk involved in the service provided

b) the amount and/or the recurrence of the transaction

c) the payment channel used for the execution of the transaction.

PSD2 also introduces a **liability shift**, as the 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 strong customer authentication, the payer will not be required to bear any financial losses unless the payer has acted fraudulently. In cases where the **payee** – or the payee's PSP – fails to accept strong customer authentication, it will be required to refund the financial loss caused to the payer's PSP.

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 the release of the EBA's draft RTS, it remains unclear what the authentication technologies will ultimately look like. However, Accenture expects to see the adoption of a standardised, simple and user-driven authentication framework such as OAuth 2.0 and its extension OpenID Connect, which allows authentication and authorisation 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 draft 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 reorganising 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.

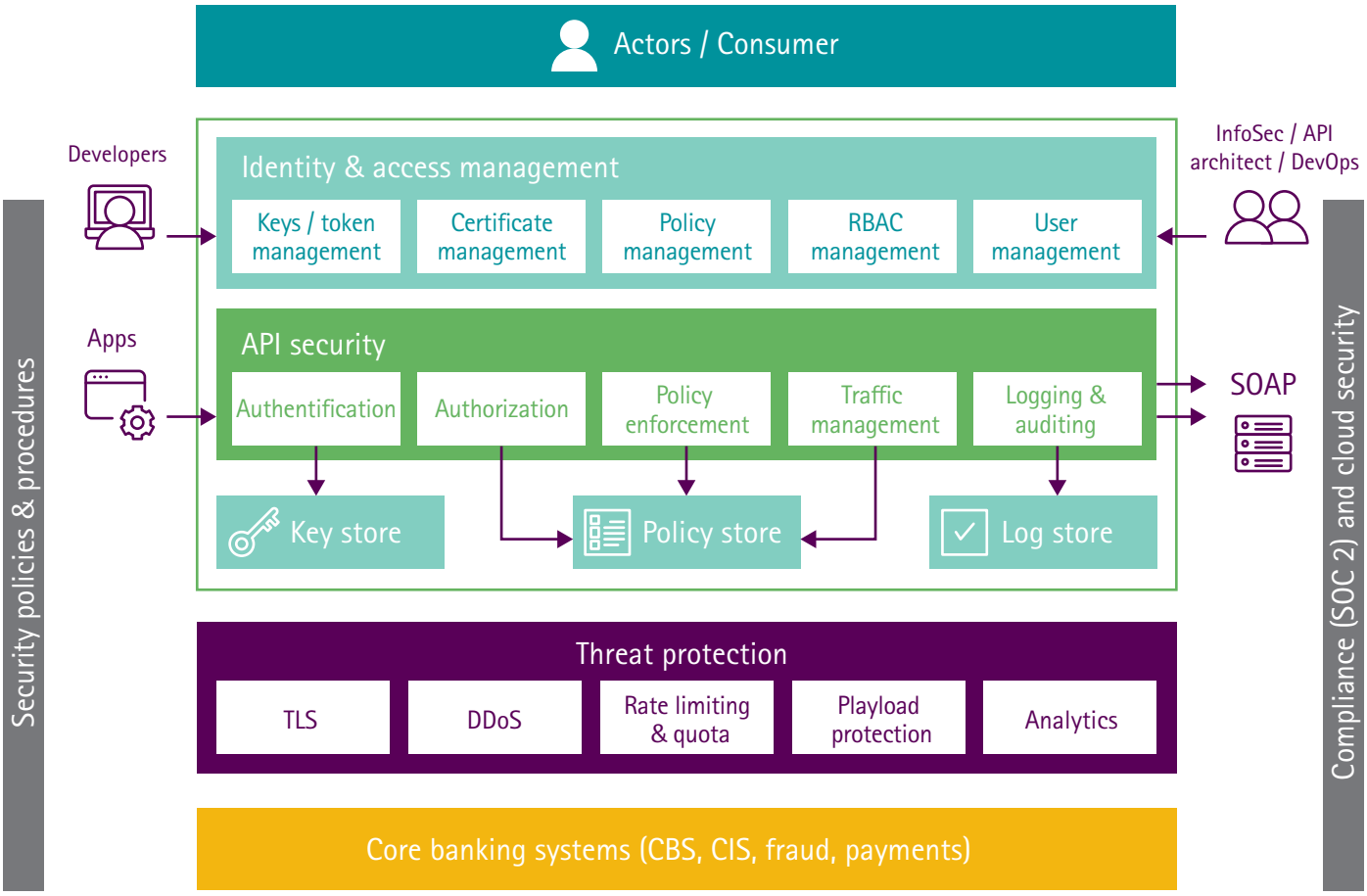
Key Question

Based on the available information in the draft RTS, OAuth 2.0/ OpenID connect is likely to be the preferred authentication protocol. The requirements on possession-based authentication methods have become stronger. Given this, is your organisation ready for OAuth-based customer/TPP authentication and technically separated possession-based authentication methods?


Off
On

Cyber Security

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 organisations, 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	Use API Keys for app authentication at a minimum and restrict access for apps to their allowed resources. Leverage basic authentication using an "authorization" header for user authentication if present
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 app 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 an app 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) regulation, 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 organisations, 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 forthcoming GDPR regulation by mid-2018, and moves to harmonize data protection and privacy across all the EU and EEA, along with the EU-US Privacy Shield.

Information Commissioner's Office (ICO) has now confirmed that the UK will be implementing the General Data Protection Regulation (GDPR).

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 ground up to maximise 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.

Maintain visibility and transparency

Any IT system should operate according to the initially stated promise, by maintaining the transparency of its components and operations.

Show respect for user privacy

By offering strong inherent privacy and appropriate notice.

Action-based availability

Only expose information upon users' consent in order to enable a specific action

Graceful degradation, not collapse

A system should continue to operate at the best of its capabilities despite the fact that a given piece of functionality may be missing.

Apply minimisation

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

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 unauthorised 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

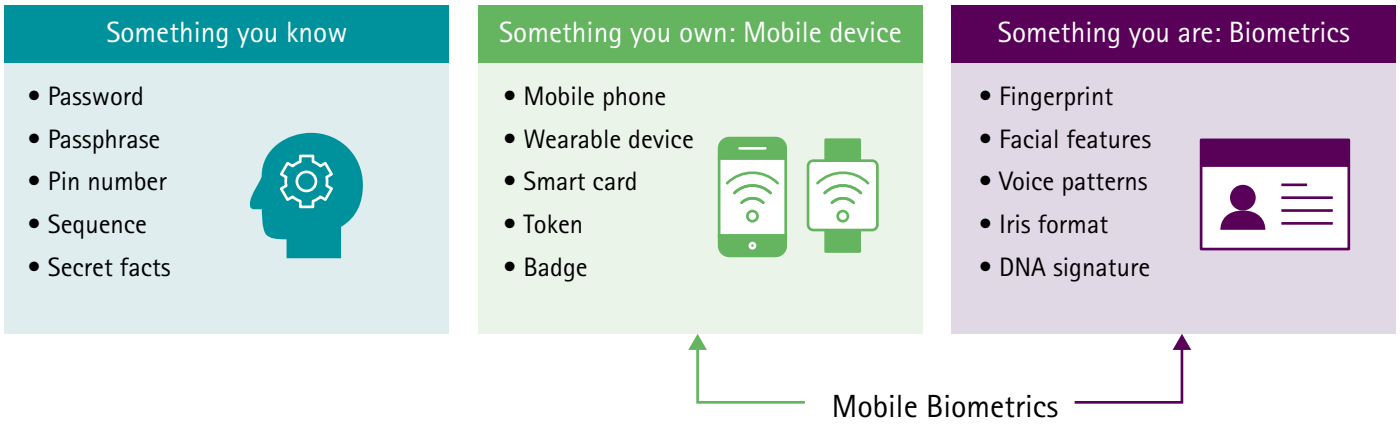
Using inherence as the second factor caters to both the security requirements and user experience priorities of PSPs. A form of inherence already in widespread use is biometric authentication, which is consumer-friendly, works in real-time, is easy to implement, and addresses the PSD2 requirement for 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 behavioural profiling. By assessing the customer's location and behaviour against their usual patterns, banks can gain a clearer view of the risks and the level of authentication required. And because behavioural profiling runs in the background, it is invisible to users and does not impinge on the customer journey.

Behavioural 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 organisation have a pluggable and adaptive authentication capability to support new and upcoming innovation in authentication technologies and techniques?



Conclusion

As the introduction of PSD2 approaches, 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-centred security mindset to an active cyber security stance – thus positioning security as a positive enabler of the "Everyday Bank" at the heart of its customers' daily lives. This enablement will be seen in all three of the Everyday Bank's key roles, as access facilitator, advice provider and value aggregator. 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 draws near, now is the time to start.

Bank as Advice Provider

Provide specific buying suggestions, based on deep customer knowledge and purchasing algorithms

Security as an enabler

Secure & digital identities enabling accurate, trusted & continuous analytics and 360°customer view creation

Bank as Access Facilitator

Support the customer in "everyday/everywhere" buying processes (shopping, access to daily services)

Security as an enabler

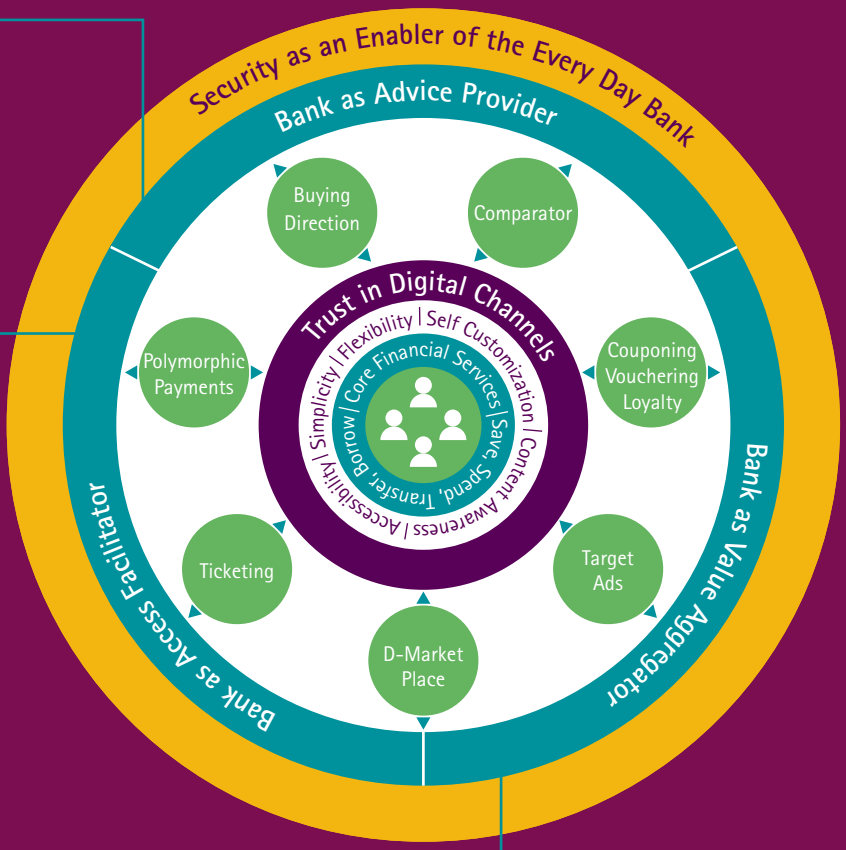
Reducing fraud & threat surface while increasing confidence of compliance increases customer faith, retention & loyalty leads to enhanced effectiveness of customer-centric business operations

Bank as Value Aggregator

Assembly components (financial and non-financial, own and third parties) to create an integrated solution for "real world" customer needs

Security as an enabler

Trusted & secure behavioural intelligence allowing for real-time management & accuracy of customer interaction




Password

NOTE

1. https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/

AUTHORS

Hakan Eroglu
Senior Manager,
ASG Digital Payments & API Lead
hakan.eroglu@accenture.com

Gagan Bhatia
Manager,
FS Technology Advisory Cyber Security Lead
gagan.bhatia@accenture.com

Anshuman Bhardwaj
Senior Manager,
Fraud & Authentication Lead
anshuman.bhardwaj@accenture.com

Andrew McFarlane
Senior Manager,
European PSD2 Lead
andrew.g.mcfarlane@accenture.com

CO-AUTHORS

Jeremy Light
Managing Director,
Accenture Payment Services, EALA
jeremy.light@accenture.com

Yousaf Mir
Managing Director ,
UK&I FS Technology Advisory
yousaf.mir@accenture.com

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

ABOUT ACCENTURE PAYMENTS

Accenture Payments offerings help bank and nonbank payment service providers and processors improve business strategy, technology and operational efficiency, covering retail payments, corporate payments and transaction banking, card payments, digital payments and innovation, compliance and operations. Accenture has more than 4,500 professionals dedicated to helping payment service providers and processors set strategy, reposition for the digital economy (including deploying open APIs, cloud services, real-time and distributed ledger technology and working with FinTechs), develop new mobile and digital services, maintain payments as a revenue-generator, reduce costs and improve productivity, meet new regulatory requirements, and simplify and integrate their payments systems and operations. Accenture has helped some of the world's top payment service providers and processors turn their payment operations into high performing-businesses. To learn more, visit www.accenture.com/payments.

FINANCIAL SERVICES TECHNOLOGY ADVISORY PRACTICE

As Consulting Practitioners in Technology Advisory we advise our clients on the current shifts in technology in Financial Services, and bring the capability to enable them to transform; from Cognitive Computing to Cyber Resilience, from Application Rationalisation to Crypto Currencies, from Software Defined Networks to DevOps Enablement. Alongside other areas in Accenture, Technology Advisory can offer the full delivery lifecycle from; advising on FS strategy and trends to delivering large transformation projects. Each advisor has specific skills and experience that will enable our clients to overcome challenges. We drive cross-FS thinking on the latest technology trends and we are the go-to practice for the latest thinking on the CIO, CTO and CDO agenda.

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 specialized 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 384,000 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.

16-4304