WHITE PAPER

Offloading and Simplifying PSD2 Compliance

by Akamai and Raidiam

RAIDIAM
TRUSTED IDENTITY SERVICES

Akamai

Table of Contents

Introduction

The revised Payment Services Directive (PSD2) and Open Banking, the UK implementation of PSD2, require financial institutions to open their payment infrastructure, granting third-party provider (TPP) access to their customers' bank account data. Regulatory bodies are driving this initiative to facilitate innovation, competition, and efficiency in financial services by enabling TPPs to provide payment and account information services to consumers.

PSD2 is a regulatory requirement, but it also offers financial institutions an opportunity to gain competitive advantage by delivering superior user experiences and customer-focused financial services. Compliance with PSD2 introduces new technical challenges and requires enhanced security controls to ensure sensitive data is not compromised, misused, or shared improperly.

This white paper provides technology leaders of larger enterprises with an overview of PSD2 compliance requirements, challenges, and opportunities, as well as a roadmap to optimize implementations.

How Akamai and Raidiam Help

Akamai solutions help financial institutions comply with PSD2 by enhancing customer experiences, application stability, and security controls. Enterprises select the tools that best fit the organization's needs, and the solution is easily integrated with cloud, on-premises, and hybrid environments for low total cost of ownership.

Raidiam is an identity specialist that provides digital transformation services focused on customer and IoT identity. Founded by the leading architects who conceived the first platform to address Open Banking in the United Kingdom as well as key players in developing the OpenID Foundation Financial Grade API (FAPI) standard, Raidiam has deep experience in navigating the legal hurdles, organizational challenges, and technical options for PSD2.

Revised Payment Services Directive (PSD2)
A directive by the European Union that ensures the security of electronic payment transactions that were formerly performed only by financial institutions

Electronic Identification, Authentication and Trust Services (eIDAS)
A standard created by European Telecommunications Standards Institute to enable secure and seamless electronic interactions between businesses, citizens, and public authorities

Third-Party Provider (TPP)
An account information service provider (AISP) or payment initiation service provider (PISP) authorized to ask permission to access bank account information to provide a service

New Challenges and Opportunities

The PSD2 does not mandate specific technology components, allowing financial institutions to evaluate and determine the best approach to achieving compliance – both a challenge and an opportunity. In addition, the shift from enterprise application silos to a customer-first approach influences solution deployment.

PSD2 poses technology and business challenges:

- Managing customers in a way that meets user experience expectations across products
- Building a strategy to make the most of business opportunities
- Solving technical challenges cost-effectively while supporting business needs

As financial institutions comply with the directive, managing the complexity and costs of the overall solution, competitive advantages emerge:

- Creating better customer experiences
- Establishing customer trust by meeting their needs
- Offering compelling new financial products and services

Providing Access to Third Parties

PSD2 requires the formal introduction of third-party providers *with no direct contract*, known as TPPs, a new class of entity in the financial services sector. While this has been going on tacitly for a number of years, banks have largely remained in control of the customer relationship.

PSD2 customer advocacy groups and regulators aim to provide an environment where appropriately controlled third parties can compete fairly with one another and the established financial services community.

Identity, Consent, and Authentication

Combining customer expectations and organizational responsibilities under PSD2, three core tenets emerge:

- **Security** – making sure that data and trust agreements are protected
- **Identity** – enabling customers to have control over their data
- **Privacy** – protecting the customer data collected

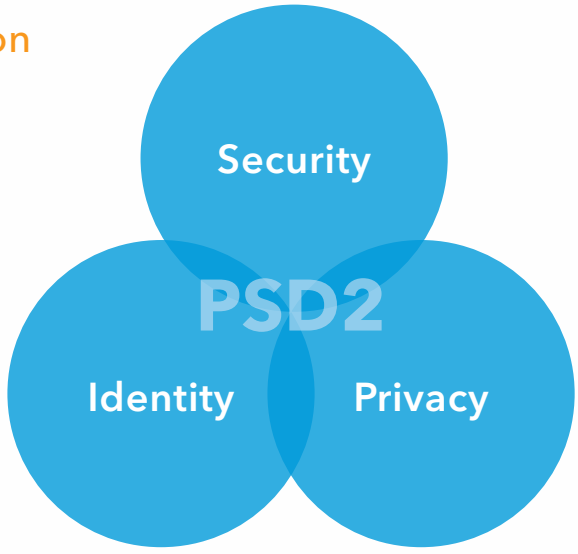

Figure 1: Three core tenets of PSD2

Customer Identity

Identity plays a crucial role in delivering business value under PSD2. The goal of identity is to give users access, control, and choice over their information, accounts, and authorizations throughout the user journey enabled under PSD2. Appropriate identity solutions and implementations should allow customers, also referred to as the payment services user (PSU), to make informed decisions while enjoying a secure, low-friction user experience.

Identity enablement is best built on modern Internet protocols OAuth2 and OpenID Connect. These standards were co-developed by Janrain (now part of Akamai) with the OpenID Foundation. With recently standardized high assurance configurations, these protocols are robust enough for financial services use cases such as PSD2. Using modern Internet protocols, customer credentials are never shared, and third-party access is tightly controlled based on explicit customer consent.

Consent and Authorization

While consent is considered to be independently managed and typically outside of the identity solution, there is an opportunity for consolidation, and leveraging a broader metadata solution that has consent and authorization collection in the authentication journey. This offers a number of benefits, including making customers' consent available in the transactional flow, as well as for authorization requests.

Under PSD2, explicit PSU consent authorization is required to:

- Share payment account data with an account information service provider (AISP)
- Allow a payment initiation service provider (PISP) to initiate payments from payment accounts
- Enable a Card-Based Payment Instrument Issuer (CBPII) to submit Confirmation of Funds requests to an ASPSP

Account Servicing Payment Service Provider (ASPSP)
Typically, the bank holding the accounts

Account Information Service Provider (AISP)
A provider of account aggregation services

Payment Services User (PSU)
The user providing consent to a TPP to access its accounts

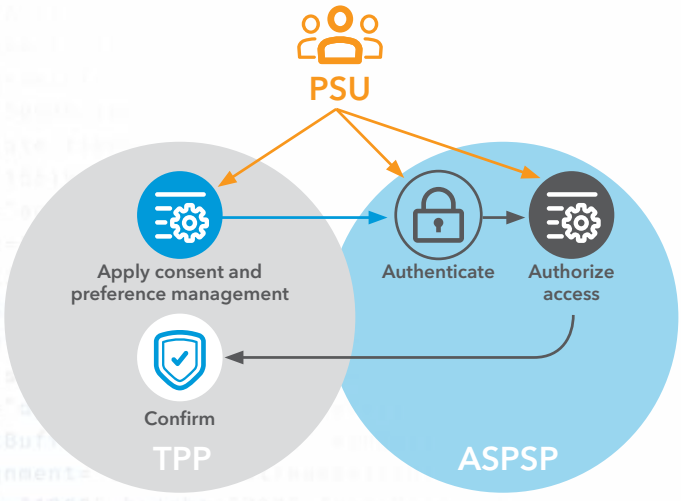

Figure 2: Authorization flow

For example, if the authorization request is initiated by the TPP, then the PSU should be directed to the ASPSP to authorize. Once that happens, the PSU should be redirected back to the TPP to complete the transaction. The authorization is stored in the token, which should be validated against every API call.

In general authorization management, a PSU should be able to:

- Revoke consent
- Temporarily enable or disable access to all or specific data

Strong Customer Authentication

Part of the new PSD2 rules is a requirement referred to as Strong Customer Authentication (SCA). SCA sets standards for all parties – whether a first-party bank or third-party financial service interface – to deliver consistent authentication to customers. SCA also promotes more secure customer access and helps reduce fraud due to weak authentication processes.

Unless an exception applies, SCA rules pertain when a payer:

- Initiates an electronic payment transaction
- Accesses a payment account online
- Carries out any action remotely that may imply a risk of payment fraud

SCA solutions must work for all groups of customers, which may mean providing several different methods of authentication, including for those who do not own a smartphone. In addition, SCA implementation shouldn't unnecessarily disrupt the customer journey or deliver poor experiences. Implementing context-aware user journeys for authentication, authorization, and consent management provides a better user experience.

API Governance

PSD2 and the Regulatory Technical Standards (RTS) require financial institutions to make secure communication interfaces available. According to the standards, the interfaces "should offer at all times the same level of availability and performance" without creating obstacles to the provision of financial services by the TPPs. There is a general industry consensus that APIs are the best technology to deliver on these requirements.

Regulatory Technical Standards (RTS)
Detailed standards on strong customer authentication as well as common and secure communication.

Strong Customer Authentication (SCA)
PSD2 requirement to increase the security of electronic payments by using multi-factor authentication

The **Akamai API gateway solution** supports three types of APIs:

- Private APIs within the financial institution
- Partner APIs between the financial institution and an external TPP
- Open APIs available to all trusted TPPs

Institutions that act as ASPSPs will offer either single or multiple API endpoints for use by the TPPs dependent on geography, availability, and application. Each API will expect an OAuth access token to be presented with every API call. Access tokens are issued by the ASPSP to provide limited interaction to the TPP, including consent claims.

Many APIs are developed in silos according to the department need, and not always built to the same level as similar APIs across the business. An API gateway provides the management features to unify the requirements that are relevant across all APIs such as authentication, rate-limiting, logging, and caching.

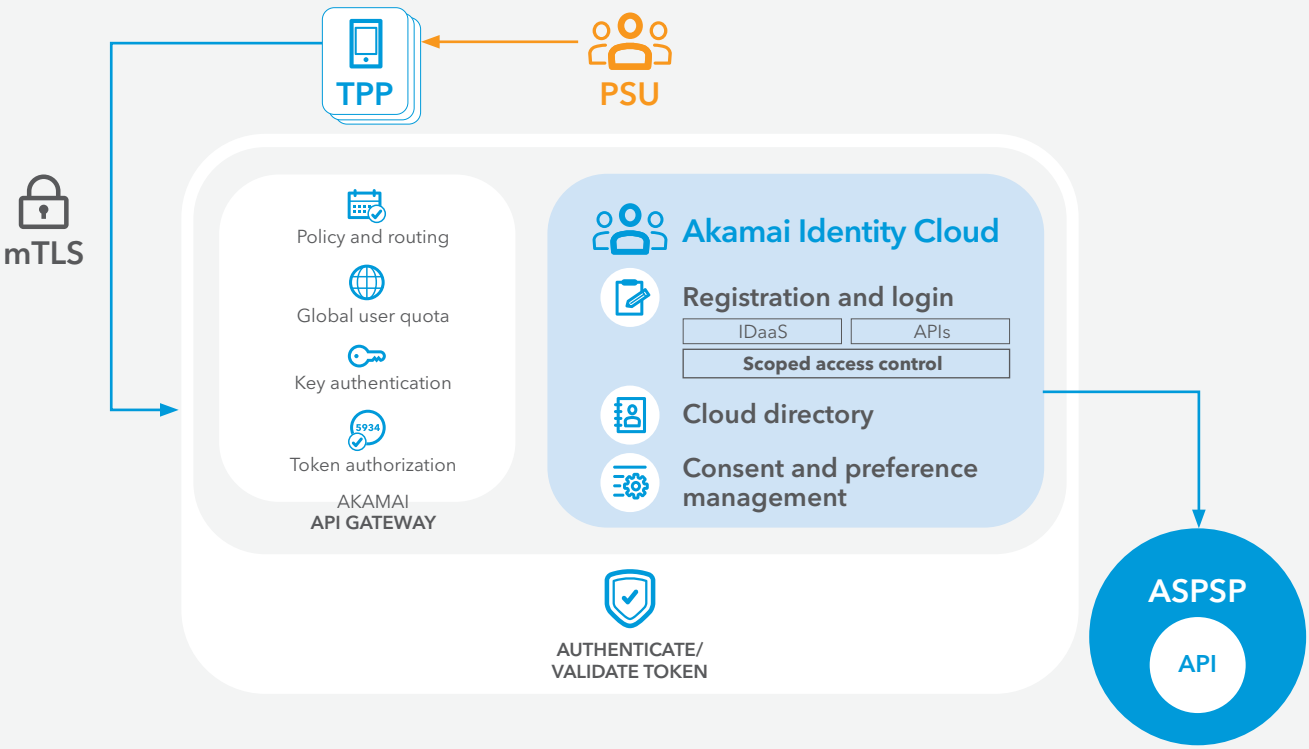

Figure 3: An API gateway manages token validation

An API gateway solution provides the opportunity to offload the task of the token validation, inspection, and enforcement of OAuth 2.0 access tokens – securing transactions for APIs through the Akamai Intelligent Edge Platform. As API request volumes go up, and each request requires authentication under PSD2, token validation throttling can become unpredictable, making it difficult to control cloud or on-premises infrastructure costs. Controlling access at the edge ensures a sustainable API-first strategy.

Mutual TLS

Identification of the third parties under PSD2 and Open Banking requires the use of electronic identification, authentication, and trust services (eIDAS), an EU-defined approach for companies to irrefutably present their identity. The certificates used are provided by a TPP to the ASPSP using the Transport Layer Security (TLS) protocol. There are a number of checks that will need to be done by the ASPSP:

- The status of the eIDAS certificate with the eIDAS certificate provider
- The status of the eIDAS certificate provider with the correct national body
- PSD2 authorization level of the company with the correct national body

Akamai Edge Services can manage the mutual TLS (mTLS) termination and validation, saving financial institutions from the challenges of implementing, operating, and maintaining that complexity.

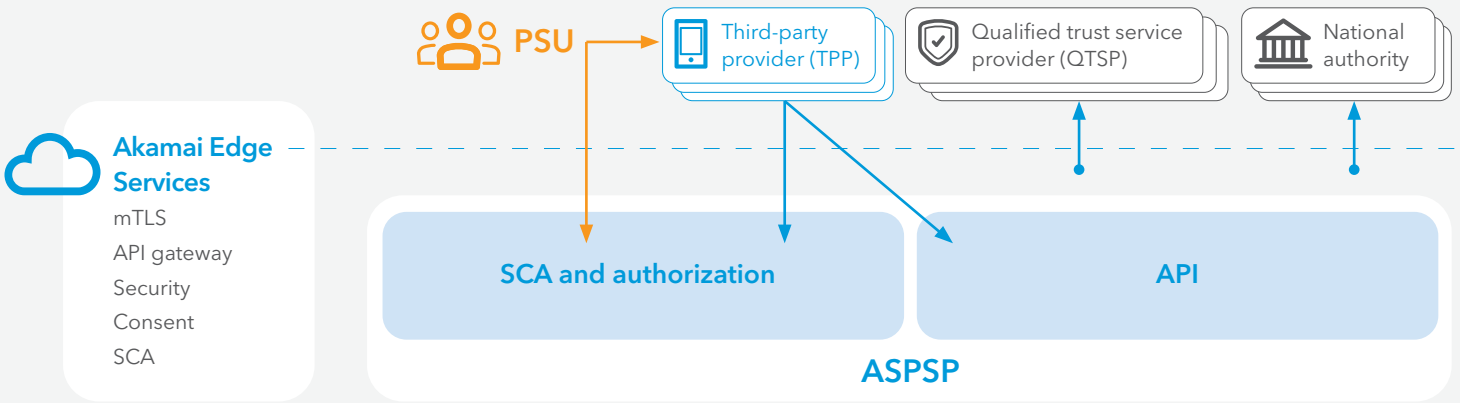

Figure 4: Akamai offloads mTLS termination and validation

PSD2 Maturity Model

With the complexity and dynamic nature of regulations, as well as the different technology and platform approaches to achieving compliance and driving value, a successful PSD2 strategy needs to be flexible to accommodate changes over time. The PSD2 maturity model has five stages – each provides unique benefits to the organization and considers how the customer will transition from one stage to the next.

1. Nonexistent

At the beginning of the PSD2 journey, organizations are typically in a research phase, or in an adjacent industry that's impacted by PSD2, such as retail commerce. Many organizations at this stage have adopted a "wait-and-see" approach, looking for industry best practices, standards, and support from the regulators on additional time to meet compliance.

2. Ad-hoc

Organizations at this stage have a level of compliance in place, typically a number of systems and processes built around existing and, in many cases, proprietary solutions. Known and controlled identity silos are in place with little or no integration between those silos and systems (for example, multiple approaches to SCA). Organizations at this stage are typically compliant or partially compliant.

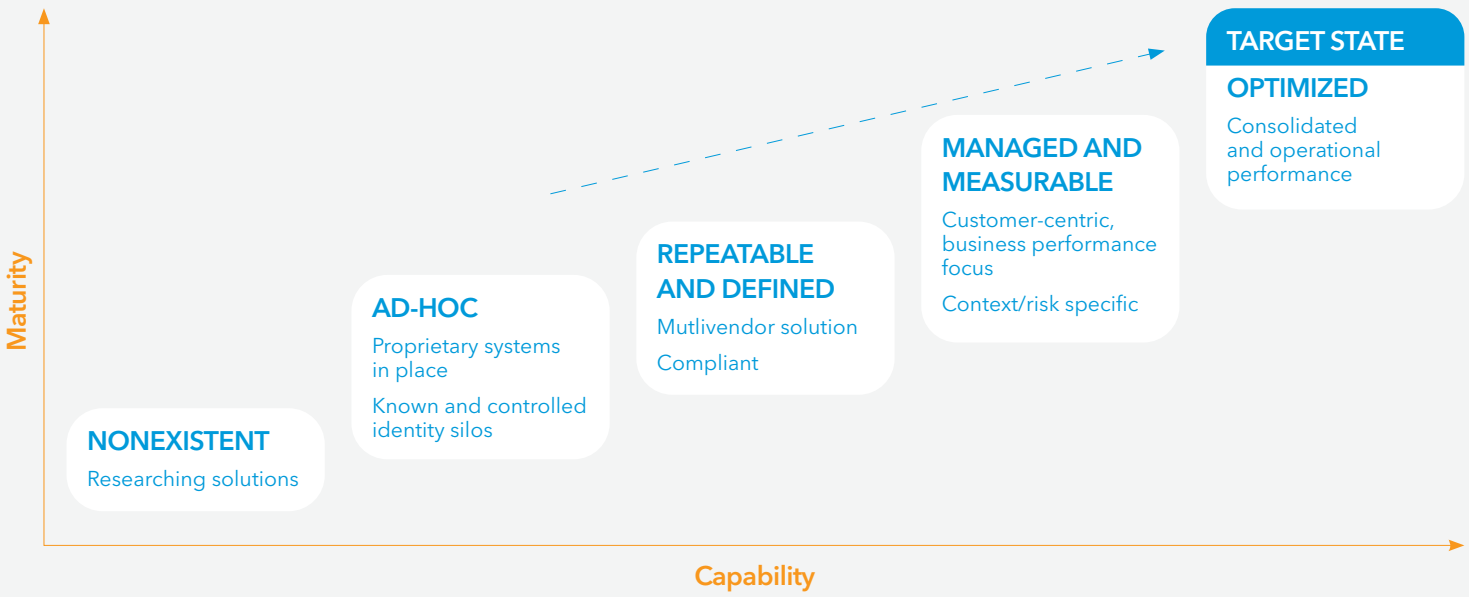

Figure 5: Five stages of PSD2 maturity

3. Repeatable and defined

The focus of this stage is to lay the foundation for deeper integrations with systems that can better deliver business value. This includes having a robust customer identity management platform, APIs that can pull together customer data from internal and external sources, and policy-based SCA.

Replacing homegrown, disparate systems across multiple IT landscapes requires a clear strategy of how the organization will create value from an integrated platform. At this stage, compliance involves a multi-vendor approach, either replacing or augmenting homegrown systems, and solutions have a high degree of custom implementation for integration. Organizations at this stage are typically compliant, but with high operational overhead.

4. Managed and measurable

The focus at this stage is to create better customer experiences. With a universal customer identity platform in place, the transition to the next stage begins when business leaders find ways to tap solutions for more than compliance-based use cases. At this stage, the investment becomes more customer centric and focused on business performance, changing customer journeys based on context and risk.

5. Optimized

The focus at this stage is to drive strategic value for both the organization and its customers. Typically, organizations at this stage are looking to optimize away from point solutions, and consolidate with vendors that can offer a best-practice solution to reduce complexity and operational costs for customer identity, mTLS, and API security.

Conclusion

When evaluating an approach to PSD2 compliance, enterprises should seek to achieve five key business goals:

1. Meeting regulatory requirements
2. Providing the best possible customer experience
3. Building a competitive advantage
4. Ensuring necessary security controls
5. Delivering an operational and cost-effective technical solution

Using Akamai technology and services can streamline implementation of PSD2 and Open Banking standards for sustainable compliance, improved customer experience, reduced operational complexity, and lower costs. Akamai secures and delivers digital experiences for the world's largest companies, including all of the top 10 European banks. The Akamai Intelligent Edge Platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure.

Raidiam accelerates delivery of PSD2-compliant solutions and moves customer solutions further up the maturity scale. The company also supports the agile delivery of more general web and API solutions to handle the challenges associated with access to those services. Raidiam offers a managed proxy service to deal with PSD2 mutual TLS termination and certificate validation, and provides managed application and infrastructure services for B2B and B2C solutions.

Financial institutions that approach PSD2 Open Banking as an opportunity to redefine the user journey and consolidate IT environments will capitalize on the benefits this new directive presents. For more information, visit akamai.com/psd2.

Additional Information

- Akamai White Paper: Security Solutions for PSD2 Compliance and Risk Mitigation
- The Payment Services Regulations 2017
- Open Banking Customer Experience Guidelines

Authors:
Mark Haine, Founding Partner, Raidiam Services Ltd (raidiam.com)
Mayur Upadhyaya, Senior Director, Identity Cloud, Akamai (akamai.com)

RAIDIAM
TRUSTED IDENTITY SERVICES

Raidiam is an identity specialist that provides digital transformation services focused on customer and IoT identity. Founded by the leading architects who conceived the first platform to address Open Banking in the United Kingdom as well as key players in developing the OpenID Foundation Financial Grade API (FAPI) standard, Raidiam has deep experience in navigating the legal hurdles, organizational challenges, and technical options for PSD2. In doing so Raidiam provides optimized services to meet and mature customers' regulatory challenges under PSD2 such as the validation of eIDAS digital certificates.

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 12/19.