Security Solutions for PSD2 Compliance and Risk Mitigation

Four ways payment service providers mitigate risk with the Akamai Intelligent Edge Platform™

Gerd Giese, Manager Enterprise Security Architects, Akamai
Dr. Anna Schmits, EMEA Data Protection Officer, Akamai
Elmar Witte, Product Marketing Manager Security, Akamai
# Table of Contents

WHAT IS PSD2?

FOUR WAYS AKAMAI HELPS WITH PSD2 COMPLIANCE
   - Access Control and Governance for APIs
   - API Protection Against Attacks
   - Common and Secure Communication
   - Avoid Screen Scraping

CONCLUSION
The new EU Directive on Payment Services, PSD2, allows any certified service provider to perform payment transactions. Its main goals are to reinforce consumer protection and improve the security of Internet payments and account access. Akamai’s security services will help minimize the risks associated with these electronic data transactions.

— Dr. Anna Schmits, EMEA Data Protection Officer, Akamai

**What is PSD2?**

PSD2, the revised Payment Services Directive by the EU (EU 2015/2366), ensures the security of electronic payment transactions that were formerly performed only by financial institutions such as banks, and can now be executed by any financial service provider. The main goal of PSD2 is to increase competition within the financial industry by granting third-party financial service providers access to customers’ banking data. Opening access to the data is expected to spur the creation of new financial services for consumers and secure banking data within the EU and the European Economic Area (EEA).

PSD2 requires financial institutions such as banks to grant access to the account data of their customers to Third Party Providers (TPPs), so the TPPs can offer financial and information services to the bank’s customers, such as a single view of all accounts of an individual across multiple financial companies.

Access is based on an open standard for communication — public APIs — to enable the TPPs to easily communicate with financial institutions when providing their services, as shown in Figure 1.
Financial institutions are required to ensure that effective access controls are in place to protect the communication between TPPs, the institution, and its customers. Furthermore, financial institutions also need to secure customers’ bank account details. These requirements are set in a document, called Regulatory Technical Standards (RTS), as follows:

- The communication model is based on dedicated communication interfaces.
- The communication must allow TPPs to access the customers’ account data as needed. This communication channel must enable financial institutions and TPPs to identify each other and communicate securely at all times. (Note: Banks are considering APIs for the implementation of this interface.)
- Screen scraping is prohibited. TPPs must identify themselves and must not pose as the customer by using the customer’s security credentials. The TPP may only access data explicitly authorized by the customer.
- Banks become Identity Holders responsible for controlling the data and ensuring secure connections.
• No TPP must be discriminated against; every TPP legitimately requesting access to a customer’s bank account data must be provided with access via the implemented communication mechanism. Third Party Providers (TPPs) act between a bank and its customers.

### Four Ways Akamai Helps with PSD2 Compliance

The requirement under PSD2 to offer an open communication interface to TPPs increases the security risks to financial institutions. First, the interfaces must ensure secure messaging between the TPPs and the institution at all times. Second, even legitimate communication by TPPs could reach a level of interaction that impacts the bank’s production systems, much like a cyberattack. Therefore, banks are required by PSD2 to put in place advanced security controls for the open interfaces to mitigate the risks.

The Akamai Intelligent Edge Platform serves as a conduit for communication between TPPs and the financial institution. Akamai security services protect the institution’s APIs from unauthorized access and ensure only authenticated access requests are processed.

Figure 2 summarizes the security and authentication duties of each of the three parties:

<table>
<thead>
<tr>
<th></th>
<th>Financial Institution</th>
<th>Akamai</th>
<th>Third Party Provider (TPP)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>Exposes its APIs in accordance with PSD2.</td>
<td>Offloads the financial institution’s infrastructure and protects APIs exposed by a financial institution to TPPs through contracted services. This service can include many protections, including but not limited to protection from DDoS attacks, application layer attacks, bots, and traffic from unauthorized parties.</td>
<td>Provides financial services to end users.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Uses the TPP’s certificate to authenticate the TPP and grants or declines the TPP access to its APIs and the financial data of its customers.</td>
<td>Acts as a safe conduit between the TPP and a financial institution, and — after technical validation — forwards the TPP’s certificate along with its request to the financial institution for verification.</td>
<td>Confirms its identity by presenting a certificate signed by a Trust Provider designated for a given market.</td>
</tr>
</tbody>
</table>

**Figure 2:** Each of the three parties has a role in security and authentication.
When Akamai protects the PSD2 APIs of a financial institution, TPPs connect to Akamai edge servers to access the financial institution’s APIs.

The TPP will send a request asking for an API of a specific financial institution. Both the TPP and Akamai will present their certificates, signed by a PSD2 Trust Provider designated for a specific market, for authentication and to encrypt the connection. The TPP uses its own certificate, and Akamai uses the certificate issued to Akamai to use on behalf of the financial institution.

At this point, the behavior of the Akamai Intelligent Edge Platform will depend on a configuration agreed upon with the financial institution, with the following options available:

**Option 1: Only Akamai validates the full certificate**

Akamai can verify the TPP’s certificate and check the following:

a. Whether the certificate is issued by a designated Trust Provider and is valid in the context of the specific market and customer

b. Whether the certificate has been revoked by the Trust Provider – if the certificate is not valid, the connection can be dropped without involving the financial institution

If the certificate is valid, the request will be processed by Akamai security services. These services can make sure that the request is not malicious and does not exceed other safety parameters, such as rate controls. After a successful check, the request is forwarded to the financial institution along with fragments of the certificate. This information allows the financial institution to check mandatory fields of the certificate for compliance (e.g., as a

---

**Figure 3:** The data exchange process between a TPP, Akamai, and a financial institution using Akamai API protection with PSD2/Open Banking-compliant certificates
minimum, a Distinguished Name check is required in the UK Open Banking implementation of the PSD2), check optional fields as desired, and respond to the TPP’s request.

Option 2: Akamai and the financial institution each validate the full certificate
Akamai can perform all the checks and protections listed in Option 1 and then forward the confirmed request along with the full certificate to the financial institution. This second approach allows the financial institution to validate the certificate before responding to the request.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better offloads the financial institution’s infrastructure and still offers compliance with mandatory standards.</td>
<td>Adds additional certificate validation by the financial institution, which adds overhead but might be required by the financial institution.</td>
</tr>
</tbody>
</table>

**Figure 4:** The behavior of the Akamai Intelligent Edge Platform will depend on a configuration agreed upon with the financial institution

**ACCESS CONTROL AND GOVERNANCE FOR APIS**
PSD2 and the Regulatory Technical Standards (RTS) require financial institutions to make available secure communication interfaces. The interfaces “should offer at all times the same level of availability and performance” without creating obstacles to the provision of the financial services by the TPPs.

**Akamai API Gateway** is a service for API access control and governance that is deployed on Akamai’s Intelligent Edge Platform. Every edge server becomes an API Gateway located close to the producer or consumer of the data. API Gateway ensures the availability of the financial institution’s APIs, and maximizes the scalability and reliability of the underlying authentication, authorization, and control of requests to be performed by the financial institution.

The API Gateway service is backed by the 100% uptime service level agreement (SLA) of the Akamai Intelligent Edge Platform and supports the Regulatory Technical Standards that require the availability and stability of an institution’s PSD2 interface.

API Gateway 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
Akamai serves as an OAuth 2.0 provider, securing transactions for APIs through the edge platform. API Gateway provides full API key lifecycle management and authenticates requests using these API keys. It can also validate JSON Web Tokens (JWT), an open standard (RFC 7519) that defines a compact and self-contained way to transmit information securely between parties as a JSON object.

Akamai’s API Gateway provides quota enforcement that limits request counts for individual API keys on a global basis. The quota ensures that API consumption is kept in check, as required under the RTS. API policies can be defined on a per-endpoint basis, while real-time analytics provide insight into API traffic, errors, and consumption trends. This service enables financial institutions to perform the required authentication.

![Diagram of Akamai Intelligent Edge Platform](image)

**Figure 5:** Akamai Intelligent Edge Platform delivers, governs, and secures APIs with the API Gateway

### API PROTECTION AGAINST ATTACKS

Akamai’s web application security solutions secure both APIs and web applications. These industry-leading web application firewalls provide broad protection against the most sophisticated API, web application, and distributed denial-of-service (DDoS) attacks. The solutions are deployed on the Akamai Intelligent Edge Platform and are architected as a reverse proxy to automatically drop all network-layer DDoS attacks.

PSD2 APIs are protected via control mechanisms, and the firewall rules are designed and updated regularly by Akamai’s global threat research team. Real-time analytics and reporting...
tools are provided in a web management interface to support day-to-day operations and deep forensic analysis of threats. Easy integration with local security information and event management (SIEM) platforms can enable further forensics analysis. This security solution allows financial institutions and TPPs to trace all events relevant to the API usage as required by RTS.

**Figure 6:** API protection is part of Akamai web application security solutions

### COMMON AND SECURE COMMUNICATION

SSL/TLS security standards, the building blocks of the HTTPS protocol, provide high-quality secure communication, which is required by PSD2 and RTS. HTTPS enables authentication and encryption of online transactions from the end user to the financial institution and back, securing infrastructure, private keys, and connections along the way.

Akamai’s Secure CDN solution provides industry-leading security and reliability, certificate options with complete lifecycle management, and easy-to-use tools, systems, and expertise. This solution runs on the Akamai Intelligent Edge Platform, so it is fully fault-tolerant, resilient, and backed by a 100% uptime SLA.

### AVOID SCREEN SCRAPING

Akamai can assist the financial institution in avoiding screen scraping activities with the use of its bot management solution\(^3\) which can identify automated traffic targeted at a web service.

Leveraging different analysis technologies, Akamai can distinguish machine-automated from human-generated traffic. Bot response methods enable comprehensive traffic management to differentiate good bots from bad bots. Responses can go from simple blocking to serving the bot with alternate content or modified information, so TPP requests can be allowed through while preventing or redirecting activities by other types of bots.
Conclusion

The revised Payment Services Directive (PSD2) aims to better protect consumers when they pay online, promote the development of innovative online and mobile payments, and make European payment services safer.

PSD2 requires financial institutions to open their payment infrastructure and grant TTPs access to their customers’ bank account data to enable them to provide payment and information services to consumers.

It is a regulatory compliance requirement and a security technology challenge, due to the responsibility of the financial institution to provide secure communication interfaces and to take measures to protect those interfaces and their customer accounts against threats. Akamai can support your financial institution in complying with PSD2 in many ways while also enhancing your organization’s overall security posture.

Protection Against Phishing

PSD2 also aims to “limit the risks relating to phishing and other fraudulent activities” (PSD2 Directive (EU) 2015/2366). In this case, as part of the Zero Trust Principle, Akamai’s solution to protect against advanced threats can control all outgoing Internet requests and compare them, through a DNS resolution, with its Cloud Security Intelligence (CSI) database, to identify if the domain, URL, or payload being requested is malicious or safe.

The Akamai CSI threat intelligence database leverages Akamai’s comprehensive views of DNS and IP traffic to deliver up-to-the-minute protection against phishing, malware, ransomware, and DNS data exfiltration.
Enhancing Security Posture by SIEM Integration

Integration with a SIEM that can process all information from the Akamai Intelligent Edge Platform to the customer's data center can further enhance visibility.

THIS WHITE PAPER REFERS TO:


SOURCES
1 European Commission Fact Sheet: Payment Services Directive (PSD2) - Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments
2 Kona Site Defender and Web Application Protector
3 Bot Management