WHITE PAPER

Descongestión y simplificación del cumplimiento de PSD2

por Akamai y Raidiam

RAIDIAM
TRUSTED IDENTITY SERVICES

Akamai

Tabla de contenido

Introducción

En la versión revisada de la directiva de servicios de pago (PSD2) y banca abierta, implementación en el Reino Unido de PSD2, se exige que las instituciones financieras abran su infraestructura de pagos para que los proveedores externos puedan acceder a los datos de las cuentas bancarias de sus clientes. Los organismos normativos están impulsando esta iniciativa para facilitar la innovación, la competencia y la eficiencia en los servicios financieros, al permitir a los proveedores externos proporcionar servicios de pago y de información de cuentas a los consumidores.

PSD2 es un requisito normativo, pero también ofrece a las instituciones financieras la oportunidad de obtener una ventaja competitiva, al ofrecer experiencias de usuario excelentes y servicios financieros centrados en el cliente. El cumplimiento de la directiva PSD2 conlleva nuevos desafíos técnicos, además de exigir controles de seguridad mejorados para garantizar que los datos confidenciales no corran peligro, se utilicen de forma incorrecta o se compartan con quien no se debe.

En este white paper, los responsables tecnológicos de grandes empresas pueden encontrar una descripción general de los requisitos de cumplimiento, los desafíos y las oportunidades de PSD2, así como un plan para optimizar las implementaciones.

Cómo pueden ayudarle Akamai y Raidiam

Las soluciones de Akamai ayudan a las instituciones financieras a cumplir con la directiva PSD2, al mejorar las experiencias de los clientes, la estabilidad de las aplicaciones y los controles de seguridad. Las empresas seleccionan las herramientas que mejor se adaptan a las necesidades de la organización. La solución se integra fácilmente con los entornos en la nube, locales e híbridos para reducir el coste total de propiedad.

Raidiam es una empresa especialista en gestión de identidades, que proporciona servicios de transformación digital centrados en la identidad de IoT y de los clientes. Fundada por los arquitectos que diseñaron la primera plataforma para abordar la banca abierta en el Reino Unido, así como por los principales actores en el desarrollo del estándar API apta para aplicaciones financieras (FAPI) de OpenID Foundation, Raidiam cuenta con una amplia experiencia en el examen de las trabas legales, las opciones técnicas y los desafíos organizativos relacionados con PSD2.

Versión revisada de la directiva de servicios de pago (PSD2)
Directiva de la Unión Europea que garantiza la seguridad de las transacciones de pago electrónico realizadas anteriormente solo por instituciones financieras.

Reglamento sobre identificación electrónica y servicios de confianza (eIDAS)
Estándar creado por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) para permitir interacciones electrónicas seguras y fluidas entre empresas, ciudadanos y autoridades públicas.

Proveedor externo (TPP)
Proveedor de servicios de información sobre cuentas (AISP) o proveedor de servicios de iniciación de pagos (PISP) autorizado para solicitar permiso de acceso a la información de la cuenta bancaria para proporcionar un servicio.

Nuevos desafíos y oportunidades

La directiva PSD2 no impone componentes tecnológicos específicos, lo que permite a las instituciones financieras evaluar y determinar la mejor estrategia posible para adaptarse a la normativa, y esto representa tanto un desafío como una oportunidad. Además, pasar de los silos de aplicaciones empresariales a una estrategia orientada al cliente influye en la implantación de la solución.

PSD2 conlleva desafíos tecnológicos y empresariales:

- Gestionar a los clientes de una forma que permita satisfacer sus expectativas en torno a la experiencia de usuario en los distintos productos.
- Diseñar una estrategia para aprovechar al máximo las oportunidades de negocio.
- Resolver los desafíos técnicos para responder, de manera rentable, a las necesidades de la empresa.

A medida que las instituciones financieras cumplen con la directiva, gestionan la complejidad y los costes de la solución global, surgen ventajas competitivas

- Crear mejores experiencias para los clientes.
- Conseguir la confianza del cliente al responder a sus necesidades.
- Ofrecer nuevos y atractivos productos y servicios financieros.

Cómo proporcionar acceso a terceros

PSD2 nos obliga a presentar formalmente a los proveedores terceros *sin contrato directo*, conocidos como proveedores externos, que representan una nueva clase de entidad en el sector de los servicios financieros. Aunque esto ya se venía dando de forma tácita desde hace años, los bancos han mantenido en gran medida el control de la relación con el cliente.

Los organismos reguladores y los grupos de defensa del consumidor que trabajan en el PSD2 pretenden ofrecer un entorno en el que terceros debidamente controlados puedan competir de forma justa entre sí y con la comunidad de servicios financieros establecida.

Identidad, consentimiento y autenticación

Al combinar las expectativas de los clientes con las responsabilidades organizativas que impone PSD2, surgen tres principios básicos:

- **Seguridad**: garantizar la protección de los datos y los acuerdos de confianza.
- **Identidad**: ofrecer a los clientes el control de sus datos.
- **Privacidad**: proteger los datos del cliente recopilados.

Figura 1: Tres principios básicos de PSD2

Identidad de cliente

La identidad desempeña un papel fundamental a la hora de ofrecer valor empresarial según PSD2. El objetivo de la identidad es proporcionar a los usuarios acceso, control y posibilidad de elección en cuanto se refiere a su información, cuentas y autorizaciones durante todo el proceso que contempla la directiva PSD2. Las soluciones de gestión de identidades y sus implementaciones correspondientes deben permitir a los clientes, también denominados usuarios de servicios de pago (PSU), tomar decisiones fundamentadas y disfrutar de una experiencia de usuario segura y sin problemas.

Una capacitación de identidades óptima se basa en los protocolos de Internet modernos OAuth2 y OpenID Connect. Janrain (ahora parte de Akamai) ha desarrollado estos estándares conjuntamente con OpenID Foundation. En configuraciones con alto grado de seguridad recientemente estandarizadas, estos protocolos son lo suficientemente sólidos como para la adopción de servicios financieros conforme a PSD2, por ejemplo. Mediante el uso de protocolos de Internet modernos, las credenciales de los clientes nunca se comparten, y el acceso de terceros se controla de forma estricta basándose en el consentimiento explícito del cliente.

Consentimiento y autorización

Si bien se considera que el consentimiento se gestiona de forma independiente y normalmente fuera de la solución de identidad, existe la posibilidad de consolidar las operaciones aprovechando una solución de metadatos más amplia que permite la recopilación del consentimiento y la autorización en el proceso de autenticación. Esto ofrece una serie de ventajas, entre las que se incluye la disponibilidad del consentimiento de los clientes en el flujo transaccional, así como para las solicitudes de autorización.

En PSD2, se requiere autorización explícita de consentimiento de PSU para:

- Compartir los datos de la cuenta de pago con un proveedor de servicios de información sobre cuentas (AISP).
- Permitir a un proveedor de servicios de iniciación de pagos (PISP) iniciar pagos desde cuentas de pago.
- Permitir que un emisor de instrumentos de pago basados en tarjetas (CBPII) envíe las solicitudes de confirmación de fondos a un proveedor de servicios de pago gestor de cuentas (ASPSP).

Proveedor de servicios de pago gestor de cuentas (ASPSP)
Normalmente, el banco de las cuentas.

Proveedor de servicios de información sobre cuentas (AISP)
Proveedor de servicios de agregación de cuentas.

Usuario de servicios de pago (PSU)
Usuario que da su consentimiento a un proveedor externo para que acceda a sus cuentas.

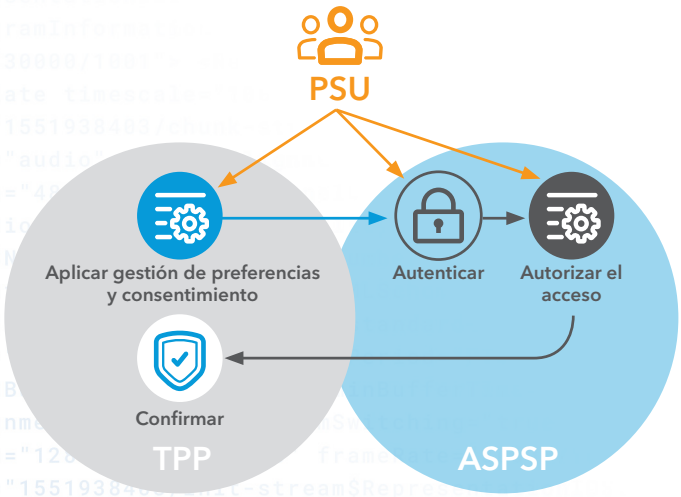

Figura 2: Flujo de autorización

Por ejemplo, si el proveedor externo inicia la solicitud de autorización, el PSU se debe dirigir al ASPSP para que la autorice. Una vez que esto ocurra, el PSU se debe redirigir de nuevo al proveedor externo para completar la transacción. La autorización se almacena en el token, que debe validarse para cada llamada a la API.

En la gestión general de autorizaciones, un PSU debería ser capaz de:

- Revocar el consentimiento.
- Activar o desactivar temporalmente el acceso a todos los datos o a datos específicos.

Autenticación reforzada del cliente

Parte de las nuevas reglas de PSD2 es un requisito denominado Autenticación reforzada del cliente (SCA). La SCA establece estándares para todas las partes, ya sea un banco o una interfaz de servicios financieros externa, para ofrecer una autenticación coherente a los clientes. La SCA también fomenta un acceso más seguro al cliente y ayuda a reducir el fraude debido a procesos de autenticación débiles.

A menos que estemos ante una excepción, las reglas de SCA se aplican cuando un pagador:

- Inicia una transacción de pago electrónico.
- Accede a una cuenta de pago online.
- Realiza cualquier acción de forma remota que pueda suponer un riesgo de fraude en los pagos.

Todos los grupos de clientes deben poder usar las soluciones de SCA, lo que puede suponer proporcionar varios métodos de autenticación diferentes, incluidos los destinados a las personas que no poseen un smartphone. Además, la implantación de SCA no debería suponer ninguna incomodidad innecesaria durante el proceso que sigue el cliente ni ofrecer malas experiencias. Implantar un procedimiento en el que se tiene en cuenta el contexto a la hora de gestionar la autenticación, la autorización y el consentimiento permite una mejor experiencia de usuario.

Control de API

La directiva PSD2 y las normas técnicas de regulación (NTR) exigen a las instituciones financieras que faciliten interfaces de comunicación seguras. Según los estándares, las interfaces "deben ofrecer, en todo momento, el mismo nivel de disponibilidad y rendimiento", sin obstaculizar la prestación de los servicios financieros por parte de los proveedores externos. Existe un consenso generalizado en el sector que afirma que las API son la mejor tecnología posible para cumplir estos requisitos.

La **solución de puerta de enlace de API de Akamai** admite tres tipos de API:

- API privadas dentro de la institución financiera
- API de partner entre la institución financiera y el proveedor externo
- API abiertas a disposición de todos los proveedores externos de confianza

Normas técnicas de regulación (NTR)
Estándares detallados sobre la autenticación reforzada del cliente, así como la comunicación común y segura.

Autenticación reforzada del cliente (SCA)
Requisito de PSD2 para aumentar la seguridad de los pagos electrónicos mediante la autenticación multifactorial.

Las instituciones que actúan como ASPSP ofrecen terminales de API únicos o múltiples para que los usen los proveedores externos en función de la ubicación geográfica, la disponibilidad y la aplicación. Cada API espera que se incluya un token de acceso OAuth con cada llamada a la API. Los ASPSP emiten tokens de acceso para proporcionar una interacción limitada al proveedor externo, incluidas las solicitudes de consentimiento.

Muchas API se desarrollan en silos según las necesidades del departamento y no siempre se crean al mismo nivel que otras API similares en la empresa. Una puerta de enlace de API proporciona las funciones de gestión necesarias para unificar los requisitos relevantes en todas las API, como la autenticación, la limitación de velocidad, el registro y el almacenamiento en caché.

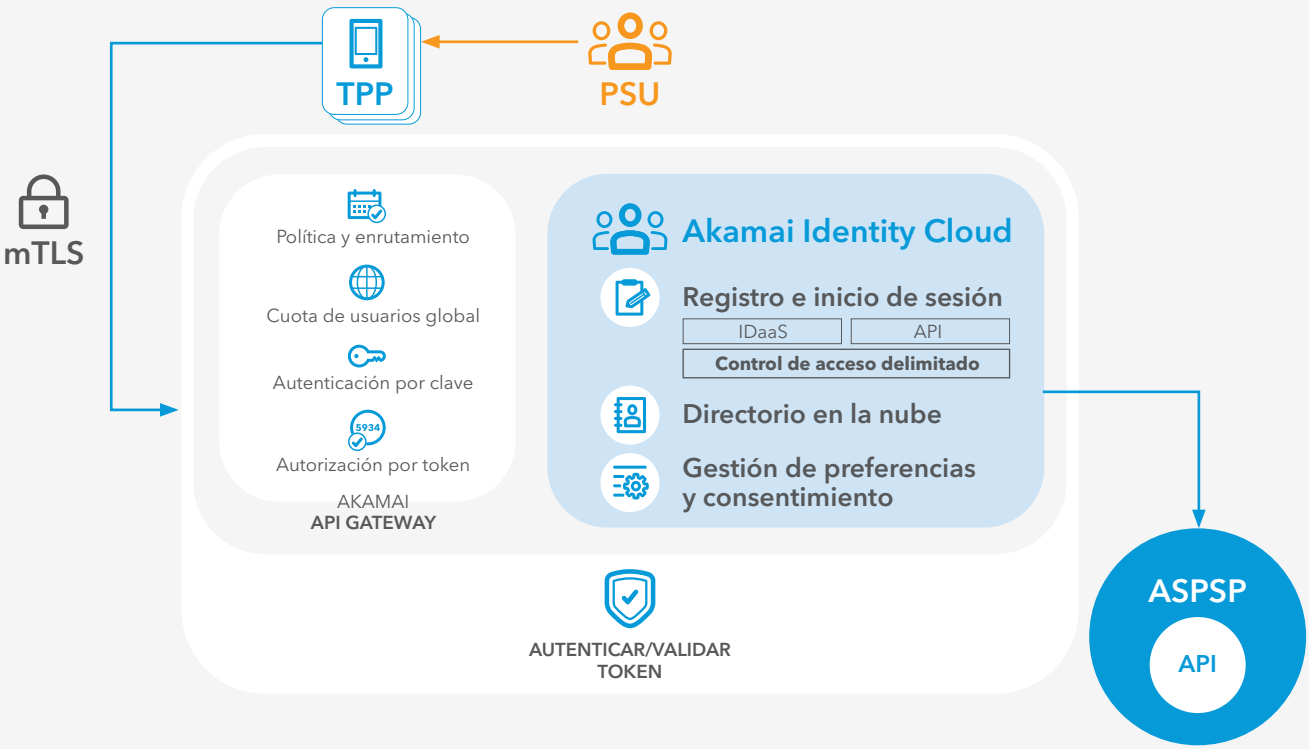

Figura 3: Una puerta de enlace de API gestiona la validación del token

Una solución de puerta de enlace de API ofrece la oportunidad de descongestionar la tarea de validación, inspección y aplicación de tokens de acceso OAuth 2.0, con la consecuente protección de las transacciones para las API en Akamai Intelligent Edge Platform. A medida que aumentan los volúmenes de solicitudes de API y cada una de las solicitudes exige autenticación según PSD2, la regulación de la validación de tokens puede volverse impredecible, lo que dificulta el control de los costes de infraestructura en la nube o local. El control del acceso en el borde de Internet garantiza una estrategia sostenible con la API como elemento principal.

TLS mutua

La identificación de terceros según el estándar PSD2 y de banca abierta requiere el uso del Reglamento sobre identificación electrónica y servicios de confianza (eIDAS), una estrategia definida por la UE para que las empresas presenten su identidad de forma irrefutable. Los certificados utilizados los proporciona un proveedor externo al ASPSP mediante el protocolo de seguridad de la capa de transporte (TLS). Hay una serie de comprobaciones que ASPSP debe realizar:

- El estado del certificado eIDAS con el proveedor de certificados eIDAS.
- El estado del proveedor de certificados de eIDAS con el organismo nacional competente.
- El nivel de autorización de PSD2 de la empresa con el organismo nacional competente.

Los servicios de Akamai Edge pueden gestionar la terminación y validación de TLS mutua (mTLS), lo que ahorra a las instituciones financieras la necesidad de implantar, manejar y mantener esa complejidad.

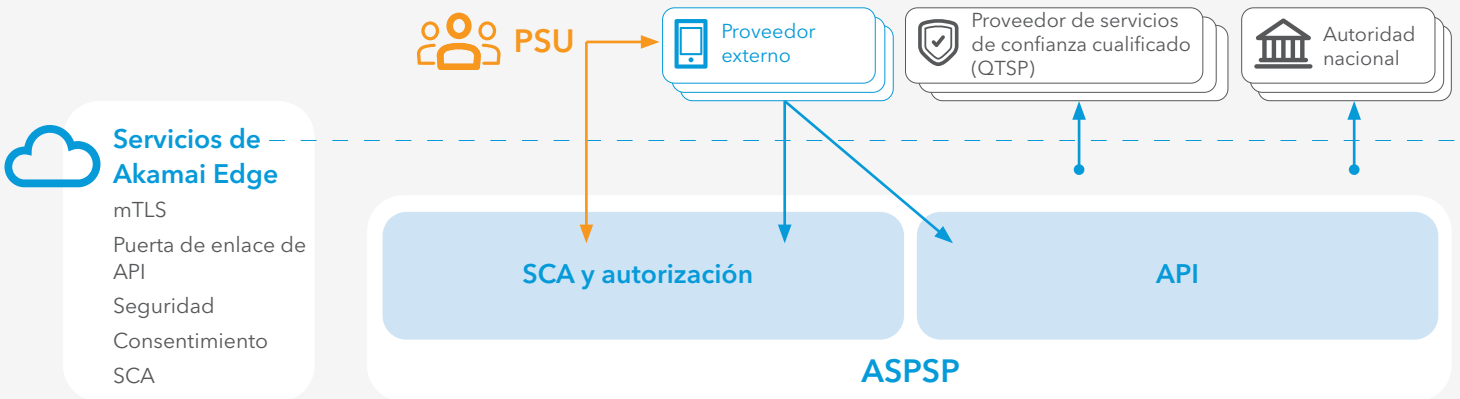

Figura 4: Akamai descongestiona la terminación y validación de mTLS

Modelo de madurez PSD2

Debido a la complejidad y a la naturaleza dinámica de las normativas, así como a las diferentes estrategias de tecnología y plataforma para lograr el cumplimiento y generar valor, una estrategia PSD2 óptima debe ser flexible para adaptarse a los cambios a lo largo del tiempo. El modelo de madurez PSD2 tiene cinco etapas: en cada una se proporcionan ventajas exclusivas a la organización y se tiene en cuenta cómo el cliente pasará de una etapa a la siguiente.

1. No existente

Al comenzar la transición hacia el cumplimiento de PSD2, las organizaciones normalmente se encuentran en una fase de investigación, o bien pertenecen a un sector adyacente que se ve afectado por PSD2, como el comercio de retail. Muchas organizaciones en esta etapa han adoptado un enfoque de "esperar y ver", buscando las mejores prácticas y los estándares del sector, así como el apoyo de los reguladores para contar con más tiempo para adaptarse.

2. Ad hoc

Las organizaciones que se encuentran en esta etapa ya están aplicando un nivel de cumplimiento, que suele ser una serie de sistemas y procesos basados en soluciones existentes y, en muchos casos, propios. Existen silos de identidad conocidos y controlados, con poca o ninguna integración entre sí y los sistemas (por ejemplo, varias estrategias de SCA). Las organizaciones en esta etapa suelen cumplir con la normativa de forma total o parcial.

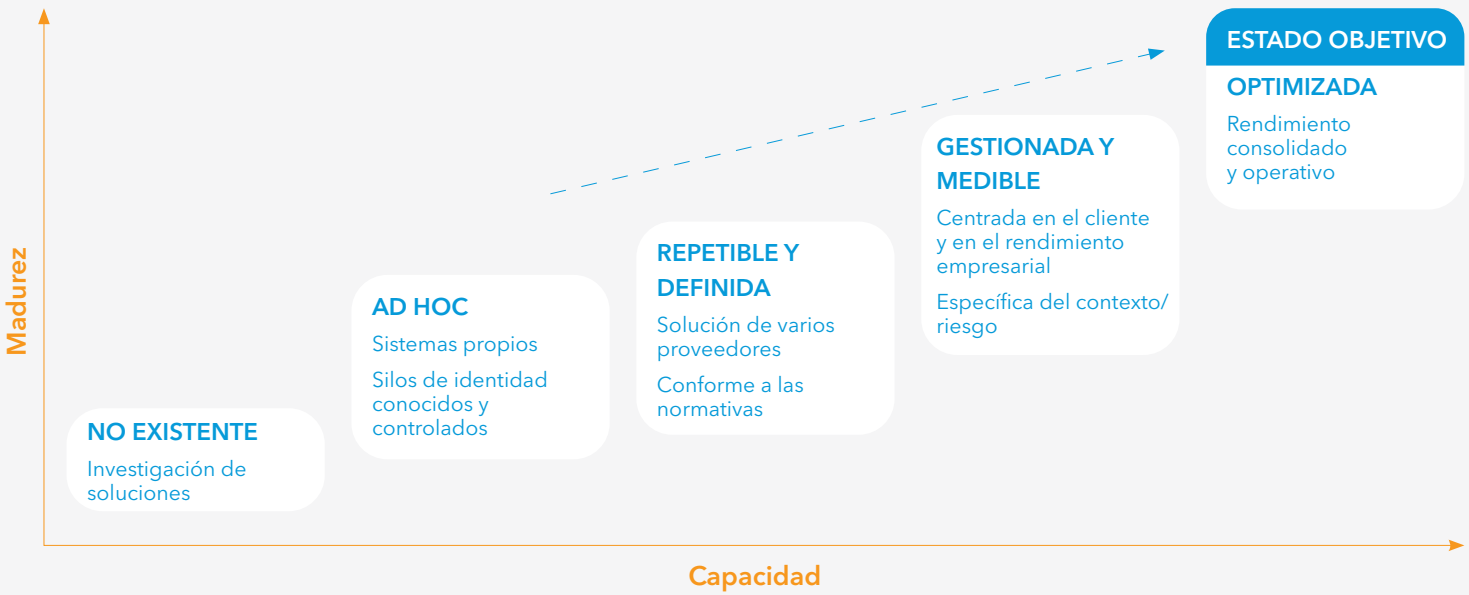

Figura 5: Cinco etapas de madurez de PSD2

3. Repetible y definida

El objetivo de esta etapa es sentar las bases para unas integraciones más sólidas con sistemas que permitan ofrecer valor empresarial, lo que incluye contar con una sólida plataforma de gestión de identidades de clientes, API que puedan unificar datos de clientes de fuentes internas y externas, así como una SCA basada en políticas.

La sustitución de sistemas propios y dispares en varios entornos de TI requiere una estrategia bien definida sobre cómo la organización va a crear valor a partir de una plataforma integrada. En esta etapa, el cumplimiento de normativas implica una estrategia de varios proveedores, ya sea mediante la sustitución o ampliación de los sistemas propios. Además, las soluciones presentan una implementación muy personalizada para facilitar la integración. Las organizaciones en esta etapa suelen cumplir con la normativa, pero con una elevada sobrecarga operativa.

4. Gestionada y medible

El objetivo de esta etapa es crear mejores experiencias para el cliente. Con una plataforma universal de identidad del cliente implantada, la transición a la siguiente etapa comienza cuando los gestores empresariales encuentran métodos para aprovechar las soluciones para algo más que casos de uso basados en el cumplimiento. En esta etapa, la inversión se centra más en el cliente y en el rendimiento empresarial, adaptando el proceso en función del contexto y el riesgo.

5. Optimizada

El objetivo de esta etapa es impulsar el valor estratégico tanto para la organización como para sus clientes. Por lo general, las organizaciones en esta etapa buscan mejorar y dejar atrás soluciones concretas, y consolidarse con proveedores que puedan ofrecer una solución de mejores prácticas para reducir la complejidad y los costes operativos relacionados con la identidad del cliente, mTLS y la seguridad de las API.

Conclusión

Al evaluar una estrategia de cumplimiento de PSD2, las empresas deben intentar alcanzar cinco objetivos empresariales clave:

1. Cumplir los requisitos normativos.
2. Ofrecer la mejor experiencia posible al cliente.
3. Crear una ventaja competitiva.
4. Garantizar los controles de seguridad necesarios.
5. Ofrecer una solución técnica rentable y operativa.

El uso de la tecnología y los servicios de Akamai puede optimizar la implantación de estándares de PSD2 y de banca abierta para lograr un cumplimiento sostenible, mejorar la experiencia del cliente, reducir la complejidad operativa y disminuir los costes. Akamai ofrece experiencias digitales seguras a las empresas más grandes del mundo, incluidos los 10 bancos europeos más importantes. Akamai Intelligent Edge Platform llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad.

Raidiam acelera la entrega de soluciones conformes a PSD2 con una estrategia que permite avanzar en el nivel de madurez. La empresa también permite la entrega ágil de soluciones de API y web más generales para afrontar los desafíos asociados al acceso a dichos servicios. Raidiam ofrece un servicio de proxy gestionado para controlar la terminación de TLS mutua y validación de certificados de PSD2, además de proporcionar servicios de aplicaciones e infraestructura gestionados para soluciones empresa a empresa (B2B) y empresa a cliente (B2C).

Las instituciones financieras que afrontan la banca abierta y PSD2 como una oportunidad para redefinir el recorrido del usuario y consolidar los entornos de TI aprovecharán las ventajas que presenta esta nueva directiva. Para obtener más información, visite akamai.com/psd2.

Información adicional

- White paper de Akamai: Soluciones de seguridad para cumplir la directiva PSD2 y mitigar riesgos
- Normativas sobre servicios de pago de 2017
- Directrices para la experiencia del cliente en banca abierta

Autores:
Mark Haine, partner fundador de Raidiam Services Ltd (raidiam.com)
Mayur Upadhyaya, director sénior de Identity Cloud, Akamai (akamai.com)

RAIDIAM
TRUSTED IDENTITY SERVICES

Raidiam es una empresa especialista en gestión de identidades, que proporciona servicios de transformación digital centrados en la identidad de IoT y de los clientes. Fundada por los arquitectos que diseñaron la primera plataforma para abordar la banca abierta en el Reino Unido, así como por los principales actores en el desarrollo del estándar API apta para aplicaciones financieras (FAPI) de OpenID Foundation, Raidiam cuenta con una amplia experiencia en el examen de las trabas legales, las opciones técnicas y los desafíos organizativos relacionados con PSD2. Al hacerlo, Raidiam proporciona servicios optimizados para satisfacer y superar los desafíos normativos de los clientes según PSD2, como la validación de los certificados digitales eIDAS.

Akamai

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com y blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en diciembre de 2019.