3D Secure 2.0

cashless 3.0

Administre la autentificación del titular de la tarjeta durante el proceso de e-commerce y m-commerce

tas group
an owl company

Una solución para servidores de control de acceso que implementa el nuevo protocolo de autentificación EMVCo 3-D Secure 2.0, en línea con los requerimientos PSD2. Este protocolo amplía su alcance desde el e-commerce (comercio electrónico) hasta el m-commerce (comercio electrónico a través de dispositivos móviles); además está diseñado para proporcionar una experiencia segura y satisfactoria para el cliente durante el proceso de pago. Los emisores podrán verificar la identidad del titular de la tarjeta durante los procesos de compra on-line, con total capacidad para:

- Control del registro del titular de la tarjeta
- Determinar si código PAN está registrado en la VbV / programa de control de identidad del emisor
- Determinar la autentificación del titular de la tarjeta
- Calcular el CAVV/AAV y enviar un mensaje de verificación al comercio-tienda

Completado con funciones de administración basadas en parámetros, funcionalidades de reporte y características que permiten la migración de protocolos previos, esta solución se puede integrar fácilmente con cualquier otro software de procesamiento de tarjetas y es totalmente compatible con PCI-3DS.

Características

CI 3D Secure 2.0, parte de **cashless 3.0**, tiene una estructura modular que permite a emisores y procesadores trabajar con procesos de autentificación basados en las especificaciones 3-D Secure 2.0 de una manera flexible y altamente configurable.

Módulo de registro

- Verifica la identidad del titular de la tarjeta (basado en la información de pre-inscripción)
- Permite al titular de la tarjeta definir un método de autentificación
- Utiliza distintos métodos de registro, incluidos:
  - Registro en la página web del emisor
  - El titular de la tarjeta accede a la página web de registro del emisor, facilita los detalles de la tarjeta y los datos requeridos, crea un mensaje de seguridad personal y su contraseña

CI 3D Secure Data Security

- Encripta el PAN antes de almacenarlo en una base de datos segregada y devolver un token. El PAN se muestra en un formato enmascarado
- El mismo procedimiento de token se usa para la información de identificación personal del titular de la tarjeta
- Proporciona características seguras de autentificación
- Proporciona información de seguimiento para auditoria
- La arquitectura prevé que la información del titular de la tarjeta no se almacene dentro de la conocida como Demilitarized Zone (DMZ)
- Posibilita la implementación en un estructura compatible con PCI-3DS

Módulo de reporte

- Genera informes sobre las actividades de registro y transacciones de pago autentificado, facilitando la monitorización de operaciones y gestión de incidencias o discrepacias.
  Los informes pueden incluir:
  - Estadísticas de transacciones autentificadas con éxito, operaciones fallidas, volumetrías y tiempos y número de intentos de registro exitosos y fallidos
  - Información sobre operaciones individuales fallidas o exitosas

Módulo de autentificación

- Permite al emisor verificar la identidad del titular de la tarjeta al finalizar una compra online
- Admite Strong Customer Authentication (SCA) y SCA Exemption, favoreciendo un proceso de pago sin fricciones
- Favorece una autentificación segura a través de un código de usuario único y de múltiples factores de autentificación (MFA) tanto para acceso administrativo como para la autentificación del usuario durante el proceso de pago
- Opciones SCA que incluyen:
  - Autentificación biométrica – la mejor manera de verificar la identidad de un titular de tarjeta
  - OTP vía SMS – el método de recuperación más común para la autentificación biométrica
  - OTP token (basada en el tiempo) – es necesario poseer un token
  - OTP CAP/DPA – es necesario tener un PCR (Personal Card Reader – lector de tarjetas) y de la aplicación correspondiente en el chip EMV
  - OTP vía IVR – es necesario que el usuario tenga unos auriculares, eso permite al banco registrar a los clientes que ya tienen credenciales de banca en casa (Home Banking)
- Gestiona las claves AAV/CAVV proporcionando evidencias de los resultados de la autentificación de pagos durante los procesos de compra online

Consola de Autentificación

- Permite una fácil gestión de la configuración parametrizable
- Permite la configuración y mantenimiento de los titulares de tarjetas, emisores, servidores de interoperatividad
- Determina el control de acceso a través de la gestión de roles

SDK para aplicaciones móviles

- Adecuado para dispositivos iOS y Android

Las funcionalidades cl 3D-Secure están también disponibles como SaaS a través de nuestro TAS Group Data Centres