# Visa Business News

23 de enero del 2025 | Global

# Visa Recomienda Usar el Modo de Uso Mejorado 'X' para el Bloque de Claves de MDK

**Resumen:** Para mejorar la seguridad de la generación de claves, Visa comenzará a eliminar gradualmente el soporte al modo de uso 'N' de bloque de claves de Clave Maestra de Derivación (MDK), anteriormente utilizado para la compatibilidad retrógrada. Los clientes deben planificar migrar al modo de uso 'X' más seguro para MDK.

Las MDK son claves criptográficas fundamentales que se utilizan para derivar otras claves, tales como una Clave Derivada Única (UDK), para operaciones criptográficas específicas y para ayudar a mejorar la seguridad general del sistema. Las claves MDK son uno de los muchos tipos de claves que se usan en criptografía de pagos para funciones como personalización de chip, personalización de claves únicas (como UDK), cifrado de PIN fuera de línea y verificación dinámica del Cardholder Verification Value 2 (CVV2).

Cada clave criptográfica, incluyendo MDK, está asociada con un modo de uso, que controla las operaciones permitidas para el bloque de claves. Una lista de modos de uso válidos se especifica en el documento ASC X9 TR 31-2018—Interoperable Secure Key Exchange Key Block Specification, disponible en la American National Stands Institute (ANSI) Webstore.

| De un Vistazo | | | |
|---|---|---|---|
| **Público** | | **Impacto** | |
| Emisores | | Acción recomendada | |
| Procesadores | | | |
| **Redes** | | **Impactos Especiales** | |
| Visa Network | ✓ | Procesamiento de Europa | ✓ |
| Interlink Network | ✓ | Afecta a los Comercios | |
| Plus Network | ✓ | Impacto Regulatorio | |
| V PAY | ✓ | Impacto de BER | |
| **Categoría** | | **Tipo de Artículo** | |
| Tarjetas con Chip | | Nuevo | |
| **Productos/Sistemas Impactados** | | | |
| V.I.P. System, todas las fuentes de fondos y tipos de transacciones | | | |

La especificación ASC X9 TR 31-2018 proporciona pautas integrales para la administración e intercambio seguros de claves criptográficas en servicios financieros. Abarca los formatos de bloques de claves y las prácticas de administración de claves y garantiza la interoperabilidad y el cumplimiento de los requisitos regulatorios y las normas de la industria. Al definir el modo de uso, ASC X9 TR 31-2018 garantiza que las claves se usen solamente para sus fines previstos, mejorando así la seguridad y reduciendo el riesgo de uso indebido.

## Modos de Uso Válidos

El modo de uso de una clave criptográfica define la operación que puede realizar la clave. Según ASC X9 TR 31-2018, los valores en la tabla a continuación son modos de uso válidos.

**Valores de Modo de Uso Definidos**

| Valor | Definición |
|---|---|
| 'B' | Cifrar y descifrar/proteger y desproteger |
| 'C' | Generar y verificar |
| 'D' | Descifrar/desproteger solamente |

Número de Identificación del Artículo: AI14824

| | |
|---|---|
| 'E' | Cifrar/proteger solamente |
| 'G' | Generar solamente |
| 'N' | Sin restricciones especiales |
| 'S' | Firma solamente |
| 'T' | Firmar y descifrar |
| 'V' | Verificar solamente |
| 'X' | Clave utilizada para derivar otra(s) clave(s) |
| 'Y' | Clave utilizada para crear variantes de clave |

## ¿Por qué Visa Soportó el Modo de Uso 'N' para MDK?

Las MDK se usan para derivar claves únicas a nivel de tarjeta. Por lo tanto, el modo de uso 'X' es el más apropiado para las MDK. Históricamente, Visa soportaba tanto el modo de uso 'X' como el modo de uso 'N' (genérico para compatibilidad retrógrada), lo que permitía a sus socios mantener operaciones existentes, proveedores de módulos de seguridad de hardware (HSM) y prácticas criptográficas sin cambios inmediatos. Sin embargo, para mejorar la seguridad, ahora es imperativo hacer la transición al modo de uso 'X', que se centra en procesos específicos de derivación de claves. El modo de uso 'X' garantiza que cada MDK se use para su fin previsto, proporcionando una seguridad más fuerte y cumplimiento con las normas criptográficas modernas.

## Eliminación Gradual del Soporte para el Modo de Uso 'N' para MDK y Cambio al Modo de Uso 'X'

Visa comenzará a trabajar para descontinuar el soporte al modo de uso 'N' de bloque de claves de MDK para la transmisión de claves (como se documenta en ASC X9 TR 31-2018) y comenzará a usar el modo de uso 'X'. Este cambio no afectará ninguna MDK existente en la que actualmente se esté usando el modo de uso 'N', incluyendo el Código de Autenticación de Mensaje (MAC) de MDK y el Cifrado de MDK (ENC). Visa recomienda encarecidamente que todas las nuevas MDK sean compartidas con el modo de uso 'X'. La fecha específica en que Visa eliminará gradualmente el modo de uso 'N' se comunicará más adelante.

## Impacto para los Clientes

Los clientes deben comenzar ahora a hacer sus propios planes para migrar al modo de uso 'X' de MDK. Visa recomienda a los clientes que se comuniquen primero con su proveedor de HSM para asegurar el soporte al modo de uso 'X' y, si no se soporta, que planifiquen actualizarse a un firmware más nuevo con el modo de uso 'X'.

Si, o cuando, el HSM del cliente soporta el modo de uso 'X' y el cliente aún no está usando el modo de uso 'X', Visa recomienda encarecidamente comenzar a usar el modo de uso 'X' para cualquier generación y transferencia de MDK. Es imperativo que esto se pruebe a fondo en entornos de prueba para evitar cualquier problema de producción durante el uso del modo de uso 'X'.

Los clientes que tengan preguntas sobre esta migración deben comunicarse con su representante de Visa.

## Información de Contacto

Visite Visa Support Hub para encontrar respuestas a sus preguntas y crear un caso si es necesario. De lo contrario:

**ALC, AP, ECMOA y Europa:** Cree un caso en Visa Support Hub.

**Canadá y EE. UU.:** Comuníquese con eSupport@visa.com.

---