

DOCUMENTACIÓN TÉCNICA

Integración AddCard Tokenization

FECHA: 2026/01/12

VERSIÓN #: 01

REVISIÓN #: 00



Indice

INTEGRACIÓN ADDCARD / TOKENIZATION	2
1. Descripción general	2
2. Alcance de la integración	2
3. Requisitos previos.....	2
4. Flujo funcional de tokenización.....	3
5. Funcionalidades soportadas.....	3
6. Seguridad y cumplimiento	4
7. Configuración básica	4
8. Manejo de respuestas	4
9. Referencia – PCI / NO PCI	5
10.1 Escenario PCI	5
10.2 Escenario NO PCI.....	6
Notas obligatorias de implementación.....	7
Conclusión.....	7



INTEGRACIÓN ADDCARD / TOKENIZATION

1. Descripción general

La integración **AddCard / Tokenization** permite a los comercios **registrar y almacenar tarjetas de forma segura** mediante la generación de un **token**, evitando que el comercio manipule o almacene directamente datos sensibles de la tarjeta.

El token generado puede utilizarse posteriormente para realizar pagos, pagos recurrentes o cobros en segundo plano, manteniendo altos estándares de seguridad y reduciendo el alcance de cumplimiento PCI.

2. Alcance de la integración

Esta integración permite al comercio:

- Registrar tarjetas de clientes de forma segura
- Generar tokens de tarjeta no reversibles
- Ejecutar pagos utilizando tokens
- Implementar pagos recurrentes o suscripciones
- Realizar cobros sin interacción del usuario
- Reducir el alcance de cumplimiento PCI

3. Requisitos previos

Antes de iniciar la integración AddCard / Tokenization, el comercio debe contar con:

- Credenciales activas:
 - **AppCode**
 - **AppKey**
- Ambiente habilitado:
 - Sandbox / Test

- Producción
- Dominio o aplicación registrada
- Certificado SSL (HTTPS)
- Backend capaz de almacenar tokens de forma segura

4. Flujo funcional de tokenización

1. El cliente inicia el proceso de registro de tarjeta.
2. Los datos de la tarjeta se capturan mediante un componente seguro (SDK, formulario JavaScript).
3. Nuvei valida la tarjeta y ejecuta controles de seguridad.
4. Se genera un **token único** asociado a la tarjeta.
5. El token es retornado al backend del comercio.
6. El comercio almacena el token para usos posteriores.
7. Los pagos futuros se ejecutan utilizando el token, sin requerir el PAN.

5. Funcionalidades soportadas

La integración AddCard / Tokenization permite:

- Tokenización de tarjetas de crédito y débito
- Pagos con token
- Pagos recurrentes
- Suscripciones
- Pagos iniciados por el comercio
- Integración con flujos:
 - 3DS 2.x (según adquirente y tipo de transacción)
- Integración con motores antifraude

6. Seguridad y cumplimiento

- El PAN **nunca es almacenado** por el comercio (NO PCI)
- Token no reversible y cifrado
- Comunicación segura **TLS 1.2 o superior**
- Reducción significativa del alcance PCI
- Cumplimiento típico:
 - **PCI DSS SAQ-A** (dependiendo del flujo implementado)

El comercio es responsable de **proteger el token** como información sensible.

7. Configuración básica

Parámetros comunes requeridos para AddCard / Tokenization:

- **AppCode**
- **AppKey**
- **Customer ID**
- **Card holder data** (capturado de forma segura)
- **Environment** (test / prod)
- URLs de:
 - Callback
 - Webhook
 - TermURL (si aplica 3DS)

8. Manejo de respuestas

La operación de tokenización retorna estados claros:

- **Success** → token generado correctamente
- **FAILURE** → tarjeta rechazada



- **Pending / Challenge** → autenticación adicional requerida
- **Error** → error técnico o de validación

Para pagos con token:

- El resultado final del pago debe validarse siempre vía **webhook**
- El token **no garantiza aprobación**, solo habilita el cobro

Consideraciones importantes

- El token es **único por tarjeta y comercio**
- El token puede invalidarse por:
 - Expiración de la tarjeta
 - Políticas del adquirente
- El comercio debe implementar:
 - Control de tokens activos
 - Manejo de errores por tarjeta expirada o inválida

9. Referencia – PCI / NO PCI

9.1 Escenario PCI

Para comercios que **CUENTAN con certificación PCI DSS**, se permite el consumo directo de los endpoints API.

Endpoints AddCard / Tokenization

- Add Card:
<https://developers.paymentez.com/api/#payment-methods-cards-add-a-card>
- Listar tarjetas:
<https://developers.paymentez.com/api/#payment-methods-cards-get-all-cards>
- Eliminar tarjeta:
<https://developers.paymentez.com/api/#payment-methods-cards-delete-a-card>

- Débito con token:
<https://developers.paymentez.com/api/#payment-methods-cards-debit-with-token>
- Refund (**obligatorio**):
<https://developers.paymentez.com/api/#payment-methods-cards-refund>
- Webhook / Callback (**obligatorio**):
<https://developers.paymentez.com/api/#webhook>
- Verify (**obligatorio para Diners / 3DS**):
<https://developers.paymentez.com/api/#payment-methods-cards-verify>

9.2 Escenario NO PCI

Para comercios que **NO cuentan con certificación PCI DSS**, es obligatorio usar componentes seguros (JavaScript o SDK).

Endpoints permitidos

- Add Card (JavaScript seguro):
<https://developers.paymentez.com/docs/payments/#javascript>
- Listar tarjetas:
<https://developers.paymentez.com/api/#payment-methods-cards-get-all-cards>
- Eliminar tarjeta:
<https://developers.paymentez.com/api/#payment-methods-cards-delete-a-card>
- Débito con token:
<https://developers.paymentez.com/api/#payment-methods-cards-debit-with-token>
- Refund (**obligatorio**):
<https://developers.paymentez.com/api/#payment-methods-cards-refund>
- Webhook / Callback (**obligatorio**):
<https://developers.paymentez.com/api/#webhook>
- Verify (**obligatorio para Diners / 3DS**):
<https://developers.paymentez.com/api/#payment-methods-cards-verify>

Notas obligatorias de implementación

- Todos los comercios **deben implementar Refund**, por requerimiento de los Bancos.
- Es obligatorio enviar un **correo de confirmación de pago** al cliente, incluyendo:
 - Detalle de la compra
 - transaction_id (DF)
 - authorization_code
- Una transacción **Aprobada** se valida con:
 - status = "success"
 - status_detail = "3"
- El comercio **debe implementar callback/webhook** para validación del estado final.
- Si los puntos descritos **no están implementados**, el comercio **no podrá avanzar** en su integración.

Conclusión

La integración **AddCard / Tokenization** permite a los comercios implementar **pagos recurrentes, suscripciones y cobros posteriores** de forma segura, sin exponer datos sensibles, cumpliendo con los requerimientos bancarios y reduciendo el alcance PCI.